6480 Via Del Oro
San Jose 95119
California USA
+1 800-998-2408

Customer Release Notes

ExtremeWireless™ Convergence Software

Software Version 9.21.18.0009
July 14, 2017

INTRODUCTION:

This document provides specific information for this version of software for the ExtremeWireless™ Convergence Software.

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

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

Firmware Specification:

Status	Version No.	Type	Release Date
Current Version	9.21.18.0009	Maintenance Release	July 14, 2017
Previous Version	9.21.17.0006	Maintenance Release	April 28, 2017
Previous Version	9.21.16.0013	Maintenance Release	February 16, 2017
Previous Version	9.21.15.0006	Maintenance Release	December 12, 2016
Previous Version	9.21.14.0005	Maintenance Release	November 4, 2016
Previous Version	9.21.13.0005	Maintenance Release	October 3, 2016
Previous Version	9.21.12.0005	Maintenance Release	August 25, 2016
Previous Version	9.21.11.0004	Maintenance Release	July 22, 2016
Previous Version	9.21.10.0005	Maintenance Release	June 20, 2016
Previous Version	9.21.09.0004	Maintenance Release	May 13, 2016
Previous Version	9.21.08.0013	Maintenance Release	April 8, 2016
Previous Version	9.21.07.0007	Maintenance Release	February 26, 2016
Previous Version	9.21.06.0006	Maintenance Release	January 22, 2016
Previous Version	9.21.05.0007	Maintenance Release	December 4, 2015
Previous Version	9.21.04.0007	Maintenance Release	October 30, 2015
Previous Version	9.21.03.0010	Maintenance Release	September 25, 2015
Previous Version	9.21.02.0014	Maintenance Release	August 14, 2015
Previous Version	9.21.01.0179	Feature Release	June 26, 2015
Previous Version	9.15.07.0008	Maintenance Release	June 5, 2015
Previous Version	9.15.06.0010	Maintenance Release	May 8, 2015
Previous Version	9.15.05.0007	Maintenance Release	March 27, 2015
Previous Version	9.15.04.0011	Maintenance Release	February 27, 2015
Previous Version	9.15.03.0005	Maintenance Release	January 23, 2015

Status	Version No.	Type	Release Date
Previous Version	9.15.02.0009	Maintenance Release	December 15, 2014
Previous Version	9.15.01.0121	Feature Release	November 17, 2014
Previous Version	9.12.04.0003	Maintenance Release	October 09, 2014
Previous Version	9.12.03.0009	Maintenance Release	September 12, 2014
Previous Version	9.12.02.0006	Maintenance Release	July 25, 2014
Previous Version	9.12.01.0067	Feature Release	June 26, 2014

SUPPORTED CONTROLLERS AND ACCESS POINTS

This ExtremeWireless™ Convergence Software version supports the following controllers and access points:

Product	Image
ExtremeWireless Controller C4110	AC-MV-09.21.18.0009-1.gxe
ExtremeWireless Controller C5110	AC-MV-09.21.18.0009-1.txe
ExtremeWireless Controller C5210	AC-MV-09.21.18.0009-1.rue
ExtremeWireless Controller C25	AC-MV-09.21.18.0009-1.pfe
ExtremeWireless Controller C35	AC-MV-09.21.18.0009-1.cwe
ExtremeWireless Virtual Appliance V2110 VMware	AC-MV-09.21.18.0009-1.bge
ExtremeWireless Virtual Appliance V2110 MS Hyper-V	AC-MV-09.21.18.0009-1.ize
Wireless AP3801i – internal antenna model only	AP3801-09.21.18.0009.img
Wireless AP3805	AP3805-09.21.18.0009.img
Wireless AP3865	AP3825-09.21.18.0009.img
Wireless AP3825	AP3825-09.21.18.0009.img
Wireless AP3715	AP3715-09.21.18.0009.img
Wireless AP3710	AP3710-09.21.18.0009.img
Wireless AP3705	AP3705-09.21.18.0009.img
Wireless AP3765	W78XC-2-09.21.18.0009.img
Wireless AP3767	
Wireless AP3605	AP3600-09.21.18.0009.img
Wireless AP3610	
Wireless AP3620	
Wireless AP3630 (thin mode)	
Wireless AP3640 (thin mode)	
Wireless Outdoor AP3660	
Wireless AP2605	AP200-09.21.18.0009.img

Wireless AP2610	
Wireless AP2620	
Wireless AP2630 (thin mode)	
Wireless AP2640 (thin mode)	
Wireless Outdoor AP2650	AP2650-09.21.18.0009.img
Wireless Outdoor AP2660	
Wireless AP4102 (thin mode)	*AP4102-09.21.05.0007.img (End of SW Support)*

INSTALLATION INFORMATION

Note: **Extreme Networks strongly recommends that you create a rescue image (do a backup operation) before upgrading your controller as described in the Maintenance Guide.**

Note: The minimum system software version is 08.32.01 to upgrade to this software version.

Note: A new installation wizard has been added to the CLI in V9.21. The CLI installation wizard will automatically run when the administrator logs into the CLI for the first time, and after a factory reset in the same manner as the GUI installation wizard. Details about the CLI installation wizard can be found in chapter 1 of the CLI user guide.

Note: Before connecting the V9.21 wireless controller to Netsight version 6.2 or earlier, please ensure that you have done one of the following: completed the GUI installation wizard, completed the CLI installation wizard, or started the GUI installation wizard and then exited it and selected to not run the installation wizard again.

Note: Legacy Wireless QoS support will be phased out in V9.21. A newly created Wireless Service and the existing Wireless Services with legacy Wireless QoS disabled will not have the option to enable Legacy Wireless QoS support from GUI or CLI. However, V9.21 does permit existing WLAN Services to grandfather in the already enabled legacy Wireless QoS support. This will give the user the option to disable legacy Wireless QoS support in GUI and CLI. The user won't be able to re-enable legacy Wireless QoS after it is disabled and configuration is saved. The GUI/CLI will display a warning before the user saves the configuration that switches the legacy Wireless QoS support to disable.

Note*:* If Policy Manager is being used for controller's configuration, before upgrading to the firmware version 8.32.01.035 the administrator must change the controller internal VLAN ID from the default value 1 to any other arbitrary value between 2 and 4094 or else a conflict with Policy Manager's default VLAN ID 1 will occur.

Note: It is possible that some client devices will not handle frames properly when the L2 MAC is unicast and the L3 IP address is multicast in which case the "Multicast to Unicast Delivery" option should be disabled.

Note: The V2110 is supported on ESXi version 5.1 and 5.5. For best performance and lowest latency the MMU and CPU should support hardware virtualization such as the Intel EP-T & VT-x or AMD AMD-V & RTI. Release 9.12.01 introduces V2110 support for most of the VMware vSphere advanced features. The following advanced features are supported on vSphere 5.5:

- vSphere High Availability (HA). Release 9.12.01 adds support for vSphere application level HA monitoring. This provides protection comparable to that offered by the hardware watchdog timer on the hardware wireless controllers.
- vSphere vMotion. vMotion involves moving a running virtual machine (VM) from one host to another within a cluster with minimal or no service interruption.
- vSphere Dynamic Resource Scheduling (DRS) and Dynamic Power Management (DPM). These features monitor host utilization and use vMotion to migrate VMs to different hosts based on power management and resource utilization goals.
- Storage vMotion. Storage vMotion allows the administrator to move a VM's disks to different host servers while the VM is running.
- Cold migration – The V2110 supports cold migration subject to the requirement that the V2110 is migrated in a shutdown state not in a suspended state.
- Distributed Virtual Switches (DVS). A DVS is a virtual switch that spans multiple physical hosts. VMs migrated between hosts sharing a DVS retain their network point of presence and addresses. Customers who expect to vMotion V2110s frequently should deploy DVSs if possible.
- The V2110 has supported the virtual serial port and virtual serial port concentrator features since its first release. This support continues in release 9.21.01. VMware requires the customer to purchase licenses in order to use this feature.

The release 9.21.01 V2110 does not support the vSphere Fault Tolerance feature. This feature is only available to VMs that require only one virtual core. This is a VMware restriction.

Note: The controllers communicate amongst themselves using a secure protocol. Among other things, this protocol is used to share between controllers the data required for high availability. They also use this protocol to communicate with NetSight Wireless Manager. The protocol requires the use of a shared secret for mutual authentication of the end-points.

By default, the controllers and NetSight Wireless Manager use a well-known factory default shared secret. This makes it easy to get up and running. However, it is not as secure as some sites require.

The controllers and NetSight Wireless Manager allow the administrator to change the shared secret used by the secure protocol. In fact, the controllers and Wireless Manager can use a different shared secret for each individual end-point to which they connect with the protocol.

To configure the shared secret for a connection on the controller, open the "Secure Connections" page of the "Wireless Controller" GUI module. You can enter on this page the IP address of the other end of the secure protocol tunnel and the shared secret to use.

Be sure to configure the same-shared secret onto the devices at each end of the connection. Otherwise, the two controllers or controller and NetSight Wireless Manager will not be able to communicate. In this case, features like availability will fail.

Note that changes to secure connection share secret would come into effect only when a new connection is being established.

Please refer to the NetSight Wireless Manager 5.1 or higher User Guide for a description of how to configure the shared secret on a Wireless Manager.

Note: Upgrading Virtual Appliance V2110 VMware to the current release

You only need to install the ".ova" file when you first install the V2110 VMware. All subsequent upgrades can be performed using the standard controller upgrade procedure to apply a ".bge" file to the V2110 VMware.
For more information about installing the V2110 VMware refer to the "ExtremeWireless V2110 Virtual Appliance Installation Guide VMware platform".
For more information about upgrading the V2110 VMware refer to the "ExtremeWireless Software Maintenance Guide".

Note: Upgrading V2110 Virtual Appliance V2110 MS Hyper-V to the current release.

You only need to install the ".zip" file when you first install the V2110 Hyper-V. All subsequent upgrades can be performed using the standard controller upgrade procedure to apply a ".ize" file to the V2110 Hyper-V.
For more information about installing the V2110 MS Hyper-V refer to the "ExtremeWireless V2110 Virtual Appliance Installation Guide MS Hyper-V platform".
For more information about upgrading the V2110 MS Hyper-V refer to the "ExtremeWireless Software Maintenance Guide".

Note: When the DHCP lease time is long the VNS is configured such that the DHCP IP address changes upon authentication, i.e. topology changes, some clients may not renew their IP address in an "acceptable" time to the authenticated/new IP address. In these instances, the DHCP lease time for the un-authenticated topology should be reduced. Alternatively, manually renew the DHCP leasing again.

Note: During Site configuration use the following precautionary measures:
1. The following features will not function when the AP-Controller link is broken, so do not use them in a Site Configuration:
  Tunneled/routed topologies
  Radius accounting
  Captive Portal (will be addressed in a future release).
2. Software implementation will affect the packet-processing rate; therefore do not use more than 32 filter rules within an AP filter.
3. Do not configure session availability.

Note: Please add filter rule "In Filter:dest, Out Filter:src, 0.0.0.0/0, port:BootP(67), Protocol:UDP, allow" in non-authenticated policy for captive portal WLAN Service if you intend to allow wireless clients to get an IP address through DHCP.

Note: If the filters used by controllers are managed by Policy Manager (PM), PM should include the DHCP allow rule in the policies where that is appropriate. If PM has not done this then it will need to explicitly add the rule to policies that are pushed to the controller and that need to support DHCP.

Note: IP Broadcast Multicast traffic will apply catch-all role action. If users would like to allow specific multicast, broadcast, and subnet broadcast traffic with the deny-all catch-all filter rule for global default policy, they need to explicitly add specific multicast, broadcast and subnet broadcast rules one by one to allow that traffic.

Note: Turning on "Radar" feature and assigning an AP to "in-service" scan profile will increase CPU usage.

Note: If using Sites Mode it is recommended to reboot an AP when moving between different sites.

Note: \, ', " characters are not supported in WLAN/VNS fields.

Note: In case of upgrade to V9.21, if an existing VNS has WMM disabled only legacy clients will be serviced until WMM is enabled.

Note: The dual Ethernet ports on APs should only be configured on the same subnet.

Note: During the first upgrade from pre-v9.01 to V9.21 all filtering rule will fail the Policy Manager verification. The newly upgraded controller will require a policy enforcement from Policy Manager to fix it. After this, any additional verification and enforcement will be always handled normally. Upgrades from v9.01 or later version will not have this problem.

Note: The lowest supported version for a mobility tunnel paired controller is V8.01. If a controller running an older version connects to a controller running V9.01, the results can be unpredictable.

Note: The "Bypass multicast/broadcast" option has been removed from GUI/CLI. NO filter rules are automatically generated. If the administrator needs to bypass multicast/broadcast, they should create their own filter rules to cover this case.

Note: Newly configured as well as modified Remotable WLAN Services require VNS assignments, both on the home controller and on the foreign controller. Otherwise, just like regular Wlan service, it will NOT be allowed to push to an AP, until the vns is defined.

Note: Deployment and configuration advice for AP2660

Since versions 8.21, there is a configuration change in order to enforce compliance of the controller.
This was created as a restriction for "Professional Installation" configurations.
To configure the WS-AP2660 for a single or double connected to a Left or Right radio connection, both the Left or Right antenna options should be populated with "Professional Antenna Installation". Also, both Left or Right diversity options need to be set in the Advanced Radio section. If both Left and Right connections are used, then diversity should be set to "Best".
For example, if an antenna is connected to R1 A connection (Radio 1, Left), both R1 Left and R2 Left should be populated. The configuration would be like this:
R1 Left - Professional installation
R1 Right - No antenna
R2 Left - Professional installation
R2 Right - No antenna
Tx Diversity – Left for both radios
Rx Diversity – Left for both radios

Note: RBT-4102/ AP4102 reached End of Software Support in Dec 2015.
Last build is AP4102-09.21.05.0007.img

Note: The release 9.21.10.0005 is the Minimum Firmware version for AP3801i (Rev 5F) and AP3805i/e (Rev 5K) manufactured after April 2016.

NETWORK MANAGEMENT SOFTWARE SUPPORT:

Network Management Suite (NMS)	Version No.
Extreme Networks NetSight and Wireless Manager	6.3 or higher
Extreme Networks NetSight Wireless Advanced Services	4.4
Extreme Networks NAC	6.3 or higher

EXTREME NETWORKS WIRELESS V8 TO V9 REQUESTS FOR NEW LICENSE KEYS

A new activation license key needs to be requested whenever the Wireless Controller software is upgraded from one major version to another (e.g. version 8 to version 9). Old activation keys will not carry over in the upgrade process, but feature licenses (incremental AP licenses, etc.) are carried over on the same controller.

If a new activation license key is not installed, the controller will operate without a license for 7 days after an upgrade to the next major release. After that time has elapsed, some controller functionality is disabled until the new activation key is installed.

To request a new V9 license key:

Log into your Extreme Networks Extranet account (https://extranet.extremenetworks.com/).

1. *Select the Product Licensing (https://extranet.extremenetworks.com/mysupport/licensing) link*
2. *Select the ' ExtremeWireless Upgrade Licenses' option from the list of tasks on the right-hand side of the page.*
3. *Fill in the simple form: Upgrade Version: <select "V9"> Contract Number: <type your service contract number> MAC Address: <type the dash-delimited MAC Address of your ExtremeWireless controller>*
4. *Click the 'Submit' button.*
5. *Once the form has been submitted, it will be reviewed by Order Management to confirm the contract is valid for a version 9 upgrade.*
6. *Upon approval the user will be notified via email, and given an Entitlement ID that must be redeemed though the user's Extranet account (follow the emailed instructions).*
7. *Once the Entitlement is redeemed, an activation key will be emailed to the user (or directly copied by the user).*
8. *Configure the activation key into the ExtremeWireless Controller.*

If you experience any issues with this process, please contact GTAC for assistance.

NEW FEATURES, SOFTWARE CHANGES, AND ENHANCEMENTS

Changes in 9.21.18.0009	
wns0016947	Addressed antenna port assignment logic on AP3805 for non-populated port configurations.
wns0017368	Improved stability for Load Balance Groups when many clients are within the same group.
wns0017500	
wns0018004	Improved 11k stability during background scan when Radar is detected
wns0018025	Corrected out of range exception on controller where creating a new topology would Assign a VLAN ID greater than 4096.
wns0018062	Addressed Potential Vulnerability of Controller in CVE-2016-10229.

Changes in 9.21.17.0006	
wns0017126	Enhanced logic in Background Scan and Quiet IE functions for 802.11k to better handle effect of devices in Power Save Mode
wns0017620	Corrected logical error for AP37xx (both radios) and AP38xx (2.4GHz radio) when triggered it does not always restart the Rx path after the queues have been drained which results in the radio getting stuck
wns0017729	Resolved 'AP Performance Report by Radio' columns sorting incorrectly
wns0017814	Resolved reconfiguration push issue in Sites Mode when modifying RADIUS configuration
wns0017874	Improved garbage collection logic to better free-up resources associated with disconnected clients
wns0017968	Addressed the RFC3580 support for RADIUS Access-Request Called-Station-Id to use format BSSID:SSID.
wns0017969	Resolved CLI command "show stats ap" to output correct data.
wns0017970	Corrected adding of MAC address to blacklist in GUI.
wns0017354	Enhanced logic in RADAR scanning for a DFS hit within a 40MHz channel to scan for threats on secondary channel. Also RADAR scanning will check for either 20MHz or 40MHz when set 'Auto'.

Changes in 9.21.16.0013	
wns0016122	Corrected issue with re-use of DFS channels for AP3600 series APS, which could cause AP from not re-considering previously marked DFS channel and therefore radio appearing non-operational.
wns0016280	Enhanced power save mode logic, to account for large discrepancies in timestamps which can occur in high-noise environments, to improve client wake-up from Power Save Mode.
wns0016397	Corrected logic with channel selection of DFS channels to consider alternate DFS channel for operation after a DFS event (radar). In some countries only DFS band is available for outdoor operation.
wns0016897	Corrected issue with configuration of Band Preference/Load Control for Sites deployments.
wns0017030	Improved memory footprint for AP3705 by removing un-necessary in-memory functions and reduced size flow table size to 2048 entries, to avoid possible memory exhaustion conditions.
wns0017125	Enforced inclusion of local reference address for NAS-IP-Address when doing local RADIUS authentication in Sites mode.
wns0017187	Corrected issue with propagation of AP tunnel state to peer Controller in High-Availability (HA), which could cause APs to fail in establishment of backup tunnel.

Changes in 9.21.16.0013	
wns0017218	Corrected issue with importing of MAC Blacklists, by improving serialization logic to better handle special characters in MAC listings.
wns0017279	Improved compatibility with Ascom Phones for power management frames when aggregation enabled.
wns0017291	Improved logic for handling of malformed small frames to protect from possible memory corruption leading to platform instability.

Changes in 9.21.15.0006	
wns0014750	Adjusted client association management logic to improve buffer management for disconnecting devices.
wns0016281	Improved AP discovery methods to improve resilience of AP registration operations.
wns0016386	Improved stability on Controller when integrating NAC and leveraging Change-of-Authorization (CoA)
wns0016413	Improved reliability of 4-way handshake in congested environments which could affect sensitive clients
wns0016466	Relaxed restrictions on multicast/broadcast queue management and optimized algorithm to minimize drops.
wns0016498 wns0016863	Improved performance with Chromebooks on AP3700 (both radios) and AP3800 (2.4GHz only) where clients entering power save mode would not receive aggregated packets.
wns0016666	Addressed Multiple Potential Vulnerabilities for AP in CVE-2016-7406, CVE-2016-7407, CVE-2016-7408, CVE-2016-7409
wns0016906	Addressed Potential Vulnerability of AP/Controller in CVE-2016-5195
wns0016964	Corrected logic for timer handling to address possible connectivity issues for AP3600 operational for long-periods of time

Changes in 9.21.14.0005	
wns0014331	Addressed protection mode logic to improve compatibility with Motorola Scanner connecting to 2.4Ghz radio
wns0015807	Improved packet processing logic for core assignment to address possible instability during high-rate flows on wave2 Access points.
wns0016298	Addressed race condition in client disassociating during a failover event that could corrupt session tables.
wns0016450	Improved stability for look up on missing rates

Enhancements in 9.21.14.0005
wns0016457 Added country support for Serbia for AP3825i/e

Changes in 9.21.13.0005	
wns0012835	Corrected issue with IP address learning that could affect connectivity for non-chatty clients
wns0016146	Corrected issue with Configuration Management initialization that could result in ExtremeWireless(TM) appliance instability
wns0016154	Corrected GUI issue with reporting of Client associated statistics for an AP
wns0016159	Improved logic for client de-authentication that could affect stability during generation of 802.11k Neighborhood reports.

Changes in 9.21.13.0005	
wns0016226	Improved configuration import logic to prompt user to re-enter corrupted Radius Secret values instead of halting import process.

Enhancements in 9.21.13.0005
wns0016066 Added Country Support for Uruguay for AP3825i/e
wns0016067 Adjusted Power settings for Macau to leverage 200mw allowance in 2.4 GHz (B/G/N) for AP Update AP38xx and AP39xx models

Changes in 9.21.12.0005	
wns0012074 wns0015461	Updated V2110 network device drivers to improve stability and host interoperability
wns0014842	Addressed possible vulnerability for CVE-2016-2108 - Negative 0
wns0015687	Relaxed timestamp validation for Fast Failover user registrations to allow for time drift from the AP
wns0015691	Improved Statistics framework to better handle long user statistics data sets that could cause web UI to become un-responsive

Enhancements in 9.21.12.0005
wns0015593 Enhanced Guest account management interface to support multi-edit for Account lifetime

Changes in 9.21.11.0004	
wns0012728	Improved logic in Radar surveillance component to address false-positive 'Spoof AP' for APs configured with suppressed SSIDs.
wns0012777	Additional optimizations of the background scanning algorithm to improve stability of AP38xx
wns0014382	Updated packet buffer handler to address message corruption for secure tunnel connections
wns0014589	Corrected user guide to correct description of CSV fields that carry user session lifetime.
wns0015206	Addressed possible instability for AP3800 series devices in handling of client connectivity management features (Steering, Balance, Probe Suppression)
wns0015240	Adjusted validation logic for derived key maximum key length for 802.11r (Fast Transition) configuration. Misconfiguration could cause AP38xx series radio to not initialize correctly.
wns0015352	Adjusted parsing logic of RADIUS attributes to avoid stripping of domain name information for Captive Portal Authentication.
wns0015409 wns0015436	Adjusted AP38xx radio logic handling to protect against aggressive client behavior of frequent changes in Power-Save mode for mixed client environments.

Changes in 9.21.10.0005	
wns0012777	Optimized background scanning algorithm to improve stability of AP38xx
wns0014085	Added support of topology groups in the exception filters for internal captive portal
wns0014729	Addressed Radius client recovery after target Server IP configuration changes
wns0014899	Fixed timer for Inter-AP Protocol to reduce the number of multicast transmissions for Auto Channel Selection exchanges
wns0015157	Updated configuration handler for hostname to remove leading and trailing ‘space’ characters. Space characters are not supported in Hostname definition and can cause configuration backup/restore to fail.

Enhancements in 9.21.10.0005
wns0015084 Add country support for Morocco to the AP3825i
wns0015085 Add country support for Argentina to the AP3805i/e and AP3865e
wns0015086 Add country support for Pakistan to the AP3805i/e and AP3825i/e
wns0015087 Updated Pakistan and Mexico to the latest regulations on all tables
wns0014488 For AP3705i, delayed booting up until flash clean-up is finished (up to 5 minutes). Improved resilience on recovery from hard-power reset/interruption

Changes in 9.21.09.0004	
wns0014333	Fix prevents AP radios from permanently stopping service after a wlan-service was removed
wns0014390 wns0014686	Improved memory allocation management to better handle high utilization loads
wns0014412	When client session is not there and the NAC sends a COA Request to the controller, the controller now sends a response of COA NAK with Error-Cause of 503 (session context not found)
wns0014484	SNMP traps are now sent to IPv6 trap receivers with IPv6 addresses

Enhancements in 9.21.09.0004
wns0014654 Add country support for Bosnia Herzegovina to AP3801i
wns0014655 Add country support for Bosnia Herzegovina to AP3805i/e
wns0014657 Add country support for Bosnia Herzegovina to AP3825i/e
wns0014658 Add country support for Bosnia Herzegovina to AP3825i/e-1
wns0014659 Add country support for Bosnia Herzegovina to AP3865e
wns0014486 Corrected missing channels for Malaysia on HT40 table for AP3805i

Changes in 9.21.08.0013	
wns0013329	Implemented improved recovery strategy triggered by resource impairment detection
wns0013918	Corrected user-name of radius accounting-request packets
wns0013916	Resolved NAC policy change authentication timeout after a client access re-direct
wns0014080	Fixed B@AP multicast filters configuration in sites mode
wns0014358	Updated probe suppression algorithm to use Atheros usage pattern
wns0014371	Changed probe suppression to block 802.11 auth requests
wns0014389	Corrected non-offload radio low level reset during group rekey
wns0014416	Fixed channel plan pop-up when adjusting large number of APs in multi-edit

Enhancements in 9.21.08.0013
wns0014251 Added support for AP3825i-1 and AP3825e-1 models
wns0013757 Added country support for Indonesia to AP3801i, AP3805i/e and AP3825i/e
wns0014457 Added country support for Brunei to AP3805i and AP3865e
wns0014458 Added country support for Vietnam to AP3805i, AP3825i, and AP3825i-1
wns0014459 Added country support for Malaysia to AP3805i, AP3825e, AP3825e-1, and AP3865e

Changes in 9.21.07.0007	
wns0012733	Improved discarding of received corrupted packets to protect frame sequences

Changes in 9.21.07.0007	
wns0013005	Ensure that LLDP frames are sent untagged independently of management interface VLAN assignment
wns0013228	Improved memory management protection for handling of EAP and RADIUS accounting transactions.
wns0013711	Improved Garbage collection for MU DeAuth packet detected in RX data path after a period of time and if the encryption key is missing
wns0013847	Corrected issue with handling of wrap-around for very long-running timers
wns0013859	Resolved issue where AP could get stuck in scanning mode until it is rebooted
wns0013942	Corrected ipv6 address parsing when added via the CLI
wns0014009	Resolved 802.1X authentication client connection issues
wns0014075	Fixed controller configuration check routine for overlapping subnets on different interfaces, this use case is not supported
wns0014153	Improved handling of Fast Transition state for 802.11r
wns0014185	Fixed duplicate L2 updates when new client associated to AP which caused invalid MAC addresses on the AP switch port

Enhancements in 9.21.07.0007
wns0012697 "Current Tx Power Level" changed to "N/A" for all Guardian AP’s since it is variable based on the channel and sending countermeasures if threat detected
wns0013892 Added additional support for Korea for AP3805i/e and AP3825i/e by adding channels 120, 124, 128

Changes in 9.21.06.0006	
wns0012007	Bypass filtering functions if no filter rules defined
wns0012717	Implemented routine to cleanup node list for clients that only send 802.11 auth frames but don’t actually associate
wns0012910	Resolved issue caused when Global Radius Accounting configuration state change
wns0012997	Restricted transmission of Ethernet pause frames on the AP3805i
wns0013329	Implemented improved recovery strategy triggered by resource impairment detection
wns0013414	Addressed possible resource leak while handling clients in power save mode
wns0013502	Corrected radius accounting state machine relevant to start messages when interval set to 0
wns0013505	Fixed issue when controller didn’t send Siemens-SSID RADIUS value for a fast-failover event
wns0013574	Corrected length of configured IPv6 address for management interface functions
wns0013620	Resolved iStat device not staying connected with WPA2-PSK authentication

Enhancements in 9.21.06.0006
wns0012660_Fixed coordination of Area roaming information elements for authentication transactions when both MBA and 802.1x enabled.
wns0013652_Added Country Support for Philippines to AP3825ie
wns0013761 Updated AP3865e power settings to comply with latest Industry Canada (IC) Regulations. Removed band 1 for all antennas with the exception of the WS-ANT-5DIPN. Change band 1 channels 36-48 power to meet 50mW limit and Indoor Only for WS-ANT-5DIPN.
wns0013712 Addressed possible exposure to OpenSSH keyboard-interactive authentication (CVE-2015-5600)

Changes in 9.21.05.0007	
wns0012633	Dynamic Channel Selection default set to Monitor Mode correcting channel utilization statistic reporting
wns0012723	Reserved more space for WASSP header for AMSDU frames
wns0012852	Removed the “Export_drm / Import_drm” from CLI
wns0012876	Corrected acknowledgement aggregation when MU is in power save state for 2.4 GHz radio on AP38xx
wns0013031	Resolved binding key synchronization for AP backup tunnels
wns0013188	Fixed null pointer check when retrieving AP trace
wns0013262	Corrected RADIUS interim accounting statistics updates while in B@AP topology
wns0013327	Corrected source of RADIUS Accounting Called-Station-Id value
wns0013328	Fixed the logic of the probe suppression dissociation feature of the AP
wns0013414	Resolve power save client resources leak

Enhancements in 9.21.05.0007
wns0013208 Added country support for Thailand to the AP3801i

Changes in 9.21.04.0007	
wns0011674	Improved compatibility for Hyper-V 32 bit support for V2110-H
wns0012881 wns0012178 wns0012838	Improved data structure protection for high-utilization situations on AP36xx
wns0012494	Corrected issue with Client management on APs if 5 GHz tried to re-associate to 2.4 GHz
wns0012770	Corrected issue with setting Power Save mode for roaming clients
wns0012723	Enhanced validation of sufficient packet descriptor space before transmissions
wns0012802	Reworded Warning message for WDS PSK configuration to emphasize minimum length recommendation of 24 characters.
wns0012897	Corrected issue with attempted assignment of filter rules to Legacy AP models that do not support filtering.
wns0012900	Corrected issue with possible race condition in packet de-queueing
wns0012939	Removed inadvertent Radius Accounting message for roaming clients when Interim reporting disabled
wns0012982	Corrected issue preventing enforcement of more than 43 rules when configured via Policy Manager

Enhancements in 9.21.04.0007
wns0011774 Added support for Taiwan in ROW domain for AP3805i, AP3805e and AP3801i
wns0013028 Added support for AP3801i in the Philippines
wns0011852 Improved automatic cleanup of CLI temporary artifacts
wns0012295 Enhanced exporting of AP inventory report to include BSSID to SSID assignment mapping
wns0012669 Enhanced CLI command set to provide ability to specify higher level security settings for inter-system message bus (Langley)

Changes in 9.21.03.0010	
wns0012027	Improved packet description handling for VLAN tagged on AP3765

Changes in 9.21.03.0010	
wns0012455	Improved support for 802.11r capable mobile devices
wns0012570 wns0012819	Addressed issue with WEP cache cleanup for AP3600
wns0012665	Improved cleanup of stale flows for users roaming across HA controllers.
wns0012707	Corrected enforcement of segment upper range for DHCP assignments.
wns0012713	Corrected issue with default minimum base rate configuration for 802.11b mode
wns0012720	Improved protection for handling of short EAP frame
wns0012734	Enforced use of 4-addr format for multicast distribution in Mesh network for improved Mesh network membership.
wns0012743	Ensure duplication of broadcast packets to all services if APs configured with multiple MESH WLAN services
wns0012745	Corrected issue with policy assignment of default VLAN for users of APs in Sites mode
wns0012879	Corrected encoding of Message-Authenticator in Radius Access Request

Enhancements in 9.21.03.0010
wns0011022 Added country support in Brazil for the AP3865e
wns0012791 Added country support in China for the AP3865e
wns0012795 Added country support in Korea for AP3805i and AP3805e models
wns0012796 Added country support in Brazil for the AP3805i and AP3805e models
wns0012836 Added country support in Ecuador for the AP3805ie, AP3825ie, and AP3865e
wns0012837 Added country support in Uganda for the AP3825i
wns0012863 Added country support in Chile for the AP3805i, AP3805e and AP3865e
wns0012895 Added country support in Costa Rica for the AP3825i
wns0012896 Added country support in Malaysia for the AP3825i
wns0012203 Expanded Access Point Maintenance mode to include all AP models

Changes in 9.21.02.0014	
wns0012309	Corrected issue with blacklist not restoring when AP is restored to home controller following a failover situation
wns0012406	Corrected issue with preservation of Internal Captive Portal settings after upgrade.
wns0012628	Corrected issue with generation of Tech support reports
wns0012646	Addressed possible vulnerability to cross-site scripting
wns0012662	Resolved EWC not saving and using a new shared secret after changing
wns0012665	Fixed roaming of client station back to home controller in HA mode
wns0012694	Resolved AP crash in WDS site config due to excessive logging messages
wns0012705	Resolved NetSight/Purview 6.3 not showing the TCP network and application response time
wns0012719	Corrected the base license and capacity license for C35 wireless appliance to match the datasheet
wns0012659	Improved the security by sending cookies with secure attributes via HTTPs only

Enhancements in 9.21.02.0014
wns0011775 Added country support for Japan for AP3805i/e
wns0011873 Added country support for Jamaica for AP3825i/e

Enhancements in 9.21.02.0014
wns0011874 Added country support for Jamaica for AP3805i/e
wns0012688 Added country support for Dominica for AP3825i/e
wns0012689 Added country support for Mexico on AP3805i/e
wns0012690 Tables updated for AP3865e to reflect latest approved power settings for Mexico in the 5GHz band
wns0012691 Remove country support for Japan on AP3801i
wns0012696 Added country support for Serbia for AP3805i/e
wns0012729 Added country support for Ukraine for AP3805i/e

Enhancements in 9.21.01.0179
Hardware
Introducing support for the ExtremeWireless ™ Wireless AP3801i. This is a fully featured 2x2:2 single radio 802.11 ac/an/bgn AP with configurable single radio (2.4GHz or 5GHz), 1 GE interface, and 802.3af/PoE compliant.
Introducing support for the ExtremeWireless ™ Wireless C35 high performance midlevel wireless appliance. This wireless appliance is able to manage 125 APs in standalone mode and 250 APs in H/A mode; 2,000 Users in standalone mode and 4,000 Users in H/A mode. It features 4 x GE Data Forwarding Interfaces and 1x GE Management Interface.
Software
802.11r support in 3700/3800 Series; eliminates much of the handshaking overhead while roaming, thus reducing the handoff times between APs while providing security and QoS.
802.11k support on 3700/3800 Series; this enables the client stations to understand the radio environment in which they exist so that they have more information to make decisions about roaming and performance.
802.11w WiFi protected management frames support on 3700/3800 Series; improves security by providing data confidentiality of management frames, mechanisms that enable data integrity, data origin authenticity, and replay protection.
New intelligent RF medium control reduces the aggregate amount of probe responses transmitted by APs through inter-AP communication improving overall network performance. This is important for high density wireless deployments like stadiums, arenas, lecture halls, lobbies and large common areas.
VLAN pooling on ExtremeWireless™ wireless appliance introduces the ability to distribute wireless load across subnets via multiple selection mechanisms reducing the broadcast domain and improving performance. This new capability is useful in high density deployments and large campus deployments that are using a centralized topology.
Elastic virtual ExtremeWireless™ wireless appliance for VMware; increases the scale in terms of User/AP support on the virtual wireless appliance by adjusting the resources allocated to the virtual machine hosting the wireless appliance. Support for up to 525 APs in standalone mode and 1,050 APs in High Availability (H/A) mode. Support for up to 4096 users in standalone mode and 8192 users in H/A mode.
Native integration with Purview provides application visibility in the wireless network enabling customers to understand the user, device and application performance without the need of adding specialized equipment into the network. The ExtremeWireless™ Wireless appliance forwards Netflow records to the Purview engine for both centralized and distributed topologies.
Wireless reporting enhancements including new AP performance statistics, new RADIUS features like completion of support of RFC 4372 Chargeable User Identity (CUI) provide more visibility for troubleshooting and performance tuning
Turbo Voice for WiFi Multi-Media on AP38XX 5GHz is targeted at enterprise campus, hospital, educational campus or stadiums with a dense Wi-Fi network deployment (heavy traffic loads). Using WMM-Admission Control helps ensuring that the network can support good quality voice calls before admitting the voice call

Enhancements in 9.21.01.0179
Hardware
traffic stream, and assigns the voice call priority over other traffic such as downloads, email, and other best effort traffic.
Adds country support for Malaysia for the AP3805e under the Rest-of-World (ROW) regulatory domain.
Adds country support for Malaysia for the AP3801i under the ROW regulatory domain.
Adds country support for Kazakhstan for the AP3805i/e and AP3801i under the ROW regulatory domain.

Changes in 9.21.01.0179	
wns0011052	Corrected an issue whereby the configuration of an AP could be overwritten by the foreign controller in a high availability configuration.
wns0011536	customer requesting to know max # of ECP redirect sessions possible
wns0011624	Improved Power-Save interaction with Chromebook Devices.
wns0011698	Addressed issue with aging of ARP Proxy entries when clients roamed away without completing de-association.
wns0011755	Improved audit logging of CSR key (re)generation.
wns0011881	Improved performance of AP indexing for radius client operations.
wns0012244	Improved verification of Captive Portal Credentials to increase security against interception
wns0012432	Adjusted removal of expired Guest Portal accounts to 30 days after expiration date.

Enhancements in 9.15.07.0008
wns0010605 Introduce definable threshold below which APs will not respond to probe requests from weak clients.
wns0011569 Improved support for configuring Minimum Basic Rate for management frame for AP38xx
wns0011571 Improved identification of APs during site survey by including AP configured name in beacons.
wns0012222 Added support for Session-Timeout field in processing of Change of Authorization (CoA) requests.
wns0011411 Improved cleanup of ARP Proxy entries by inspecting DHCP Release client messages
wns0012394 Enhanced AP Logging of Radar Beam detection events
wns0011463 wns0012310 Added support for AP3805i/e and AP3865e for country Bermuda
wns0011773 Added support for AP3805i/e for country China
wns0012311 Added support for AP3805i/e for country Qatar
wns0012312 Added support for 3805i/e for country South Africa
wns0012313 Added support for AP3805i/e for country Egypt
wns0012314 Added support for AP3805i/e for country Peru
wns0012315 Added support for AP3805i/e for country Uruguay
wns0012316 Added support for AP3805i/e for country Kuwait
wns0012339 Removed configuration of channels 8-12 for Mexico, Puerto Rico and the US for AP AP3660 models using the WS-AO-2S10360 GN-HT40

Changes in 9.15.07.0008	
wns0012210	Fixed an issue with RADIUS Interim Update to contain correct AP Name during roaming event
wns0012379	Fixed an issue where AP's lost their configuration on upgrading to 9.15.06 software for Japan domain

Changes in 9.15.07.0008	
wns0011605	Fixed an issue with SNMP agent which was causing service disruption when policy was updated on wireless appliance through policy manager
wns0011919	Improved communication between wireless appliance in high availability mode for a roam event
wns0012141	Improve enforcement of authentication mode for Guest Portal
wns0012357	Improved connection rate for 802.11g only clients on 3600 series AP’s
wns0012399	Fixed an issue with Apple iOS devices not getting IP address on WEP enabled SSID

Enhancements in 9.15.06.0010
wns0012031 Adds country support for Jordan to the AP3805i/e under the ROW regulatory domain.
wns0011122 Adds country support for Trinidad and Tobago to the AP3865e under the ROW regulatory domain.
wns0011875 Adds country support for Trinidad and Tobago to the AP3805i/e under the ROW regulatory domain.
wns0011177 Adds country support for Costa Rica to the AP3865e under the NAM/FCC regulatory domain.
wns0011835 Adds country support for Curacao to the AP3825i/e under the NAM/FCC regulatory domain.
wns0011774 Adds country support for Taiwan to the AP3805i/e under the ROW regulatory domain.
wns0011836 Adds country support for Taiwan to the AP3865e under the ROW regulatory domain.
wns0011870 Adds country support for Antigua to the AP3825i/e under the ROW regulatory domain.
wns0011871 Adds country support for Antigua to the AP3805i/e under the ROW regulatory domain.
wns0011872 Adds country support for Antigua to the AP3865e under the ROW regulatory domain.
wns0011905 Adds country support for Thailand to the AP3805i/e under the ROW regulatory domain.
wns0011906 Adds country support for Argentina to the AP3825i/e under the ROW regulatory domain.
wns0011954 Adds country support for Saudi Arabia to the AP3805i/e under the ROW regulatory domain.
wns0011955 Adds country support for Korea ROC to the AP3825e under the ROW regulatory domain.
wns0011956 Adds country support for Peru to the AP3865e under the ROW regulatory domain.
wns0011958 Adds country support for South Africa to the AP3865e under the ROW regulatory domain.
wns0011959 Adds country support for Japan to the AP3825i/e under the Japan (JP) regulatory domain.
wns0011960 Adds DFS support for FCC UNII bands 2 and 3 to the AP3865e under the NAM/FCC regulatory domain.
wns0011961 Adds DFS support for FCC UNII bands 2 and 3 to the AP3805i/e under the NAM/FCC regulatory domain.
wns0012032 Adds country support for UAE to the AP3805i/e under the ROW regulatory domain.
wns0012033 Adds country support for Hong Kong to the AP3805i/e under the ROW regulatory domain.
wns0012034 Corrected an issue for 3765i when radio is set to AN 20MHz and some channels are unavailable
wns0012038 Adds country support for the Dominican Republic to the AP3805i/e under the ROW regulatory domain.
wns0012039 Adds country support for Jordan to the AP3805i/e under the ROW regulatory domain.
wns0012080 Corrected an issue whereby 802.11a UNII Band 2 channels where not available for the AP3765i in Mexico.
wns0012002 Corrected Mexico channel plan to include channels 36-48 (5.0 GHz Band 1) for AP3865e combination with WS-AO-5D23009N antenna.

Changes in 9.15.06.0010	
wns0011410	Corrected possible stability issue with SMMP agent when managed through Netsight

Changes in 9.15.06.0010	
wns0011738	Corrected an issue that could prevent an MU from getting an IP address in centralized deployment (Bridge@controller) after upgrading to V9.15.03.
wns0011805	Corrected issue with forwarding of Ekahau Tag/Location Based Services (LBS) messages though the controller
wns0011895	Corrected an issue that could result in sporadic connectivity issues with meshed APs on V9.15.04.
wns0011946	Corrects an intermittent issue when Radar and Sites mode is enabled on an AP that could cause connectivity issues.
wns0011993	Corrects reported connectivity issues with Cisco Phones 7921/7925 and AP3610 after upgrading to V9.15.04.
wns0011974	Corrected reported connectivity issues with Ascom / WL3 phones after upgrading to V9.15.05.
wns0011561	Corrected performance issues with Samsung Chromebooks xe303-c12 and AP3610.
wns0011994	Corrected intermittent client connectivity issues with AP36XX on V9.15.04.
wns0011899	Corrected an issue that could result in high latency with AP36xx on V9.15.04.
wns0012018 wns0012019	Improved protection for processing of received malformed probes.
wns0012096	Corrected an issue whereby the next hop gateway MAC information was leaked to the client causing connectivity issues.
wns0012153	Corrected an issue that resulted in getting responses of “Critical Radius Accounting No Response” from the Radius accounting server.
wns0011790	Backup transfers using SolarWinds SCP is not supported. User is informed that Backup will fail.

Changes in 9.15.05.0007	
wns0009964	Added a feature so that the AP37xx and AP38xx will fragment and forward packets regardless of whether or not the doNotFragment bit is set by the end device. This feature ensures interoperability with Draeger Infinity M300s.
wns0011742	Corrected an issue causing the controller web server to failed after change in admin port IP address
wns0011829	Updated allowed character set in SNMP password string to include all but ‘;’ and ‘=’ characters.
wns0011845 wns0011846 wns0011869 wns0011856	Modified upgrade process whereby minor errors are logged and the process is allowed to complete instead of terminating process prematurely.
wns0011852	Corrected an issue causing the controller GUI process to terminate due to insufficient memory.
wns0011867	Corrected an issue in external captive portal interface which caused the role name decoded incorrectly
wns0011878	Corrected mobility group tunnel stability issue caused by incorrectly formatted message.
wns0011911	Reverted minor optimization that was causing intermittent instability on the AP3715

Enhancements in 9.15.04.0011	
wns0010732	Added country support for Philippine for AP3705i, AP3715i/e and AP3825i/e
wns0011161	Add support for FCC UNII bands 1 & 4 to AP3865e model
wns0011762	Added country support for Chile for AP3825i and AP3825e
wns0011763	Added country support for Singapore for AP3805i/e
wns0011771	Added country support for Philippines for AP3805i

Enhancements in 9.15.04.0011
wns0011772 Added country support for Philippines for AP3865e
wns0011776 Added country support for India for AP3805i/e

Changes in 9.15.04.0011	
wns0011227	Improved the resiliency of AP3xxx series APs for high-density environment
wns0011468	Corrected an issue with the 3800 Series that could cause sporadic connectivity issues in high-density environments
wns0011604 wns0011706	Corrected an issue which intermittently prevented some clients to receive IP address
wns0011614	Corrected LLDP messages to include all attributes on periodic announcements
wns0011683	Corrected issue with configuration of Load balancing groups for High Availability pairs
wns0011700	Corrected and issue with policy name length
wns0011705	Corrected an issue which was preventing reading SNMP table after upgrades on C5110
wns0011710	Corrected an issue that was causing Ekahau MAC address to be saved incorrectly for location services.
wns0011759	Corrected button rendering for Guest Portal configuration screens
wns0011779 wns0011785	Improved radio stability and addressed connectivity issues when Dynamic Channel Selection(DCS) is active / monitor.

Enhancements in 9.15.03.0005
wns0011124 Adds country support for Kuwait under the ROW regulatory domain for the AP3865e.
wns0011503 Adds country support for Saudi Arabia under the ROW regulatory domain for the AP3865e.
wns0011544 Adds additional statistic for traffic transfer between the controller and its wired interface.
wns0011632 Adds country support for Jordan under the ROW regulatory domain for the AP3865e.
wns0011633 Adds country support for Peru under the ROW regulatory domain for the AP3825i and AP3825e.
wns0011634 Adds country support for Thailand under the ROW regulatory domain for the AP3825i and AP3865e.
wns0011635 Added capability to turn off interim Radius accounting update messages.
wns0011636 Adds country support for the Philippines under the ROW regulatory domain for the AP3715i and AP3715e.
wns0011637 Adds country support for Malaysia under the ROW regulatory domain for the AP3715i.

Changes in 9.15.03.0005	
wns0011239	Corrected an issue with the Radius accounting process which causes excessive logs for clients with multiple sessions.
wns0011455	Improved editing of the guest user UI page by creating a drop down menu for year selection.
wns0011517	Corrected an issue with the Guest splash page to prevent users from entering any embedded code in the username field.
wns0011626 wns0011523	Corrected a memory management issue in certain high-density deployments with the AP37xx or AP36xx
wns0011543	Corrected an issue that caused under reporting of topology data traffic volume.
wns0011574	Corrected an issue causing a stale NAS-IP address field to be used in Radius authentication messages after a change in the controller IP address.
wns0011595	Corrected an issue that allowed policy incapable AP26xx to pass all traffic in a policy enabled environment

Changes in 9.15.03.0005	
wns0011612	Corrected an issue that was causing the Ekahau server IP address to display incorrectly for location services.
wns0011620	Improved the handling of https redirection for authentication by auto updating required policy parameters.
wns0011642	Improved handling of Unicode characters in the username field
wns0011647	Corrected an instability issue in 9.15.02.0009 with AP36xx caused when a corrupted frame is received.

Enhancements in 9.15.02.0009
wns0011117 Adds country for the AP3825e for Costa Rica under the NAM (FCC) regulatory domain.
wns0011163 Adds country support for Mexico to the 3825i/e and 3865e under the NAM (FCC) regulatory domain.
wns0011303 Provide admin control over max power for ACS.
wns0011429 Update power tables for AP37xx and AP38xx per new limits and enable 5GHz for Macau
wns0011462 Add support for Bermuda in NAM regulatory domain for the AP3825i/e
wns0011491 Add support for the AP3805e model. **For AP3805e to work properly, the firmware revision must be 9.15.02.0009 or higher**
wns0011499 Add support for Malaysia in ROW regulatory domain for the AP3705i
wns0011500 Add support for Hong Kong in ROW regulatory domain for the AP3825i/e
wns0011501 Add support for Hong Kong in ROW regulatory domain for the AP3865e
wns0011502 Add support for UAE in ROW regulatory domain for the AP3865e
wns0011527 Add Support for Barbados in NAM regulatory domain for the AP3825i/e and the AP3865e
wns0011528 Add support for Jordan in ROW regulatory domain for the AP3825i
wns0011529 Update channels and power settings for AP3765 and AP3767 models for Macau

Changes in 9.15.02.0009	
wns0011252	Corrected a memory management issue that prevented an AP from authenticating correctly via 802.1x to a switch.
wns0011363	Corrected a memory management issue that could prevent users from authenticating to the wireless network.
wns0011468	Corrected an issue with the 38XX Series that could cause sporadic connectivity issues in high-density environments.
wns0011508	Corrected an issue that prevented APs from sending their hostname in a DHCP request.
wns0011520	Corrected an issue that prevented clients for obtaining a new session when inter-WLAN roaming is disabled in fast failover mode.
wns0011552	Corrected an issue with certificate passwords containing “#”.
wns0011562	Corrected a memory management issue caused by creating and deleting a large number of policies.
wns0011581	Corrected a memory management issue that could affect 802.11ac client connections.

Enhancements in 9.15.01.0121
Introducing support for the ExtremeWireless AP3805i, 2x2:2, dual-radio 802.11ac + abgn, indoor access point. This entry-level 802.11ac access point extends all the performance benefits of the new 802.11ac without the premium price.

Enhancements in 9.15.01.0121
Introducing support for the V2110 Virtual Appliance running on Microsoft Hyper-V platform; reduces the deployment costs of an enterprise-grade wireless network for customers that already have an investment in Microsoft Hyper-V data centers.
High-availability for location services ensures that devices, users, and threats are always visible in the network to ensure maximum up-time and performance.
High-Availability for IdentiFi Radar ensures continuous protection on the wireless networks, even in the event of WAN or hardware failures.
New enhancements for primary / backup Radius deployments allow the administrator to configure Radius authenticaton so that after a primary server failure and request are forward to the backup server, new authentication requests will revert back to the primary Radius sever after the primary server is back online.
A new area notification feature is designed to track client locations within pre-defined areas using either the Location Engine or the AP Location field. When the clients change areas, a notification is sent; this feature is useful to apply policies to clients based on their physical area.
New features for Radar including: 1. Passive monitoring of DFS channels 2. Passive monitoring of regulatory prohibited channels 3. Scanning 80MHz wide channels on the 38xx series
Periodic push of location data over the web for Third Party Location Services and Analytics solution (e.g. Purple WiFi).
Adds a new feature to improve the deployment flexibility of an External Captive Portal (ECP) securely across firewall boundaries. The new feature implements a comparable level of control and trust via the use of HTTP redirections between the ECP and EWC that can be 'proxied' by the user's browser. These messages do not require additional ports be open on the firewall.
Increases Location Engine Limits to match the maximum clients limit of the wireless appliance.
Guest Portal redirection has been enhanced to redirect HTTPS requests to the Guest Portal page. The redirection will result in a security warning from most modern browsers because the original HTTPS request has been redirected to either an insecure open portal or to an HTTPS portal that is using a different SSL cert than the original request. If the user selects continue after the warning, the Guest Portal will come up so that they can sign into the network.
Adds country support for Iraq to the WS-AP3705 under ROW regulatory domain.
Adds country support for Taiwan to the WS-AP3825i/e under the ROW regulatory domain.
Adds country support for Zambia to the WS-AP3715i only under the ROW regulatory domain.
Adds country support for Singapore to the WS-AP3825i/e and WS-AP3865e under the ROW regulatory domain.
Adds country support for Angola to the WS-AP3765i under the ROW regulatory domain.
Adds support for the WS-AO-DX07025N & WS-AO-5D23009N for ETSI to the AP3865e.
Adds country support for all the 3700 and 3800 Series access points for Georgia under the ROW regulatory domain.
Adds country support for Armenia to WS-AP3705i, WS-AP3715i, WS-AP3825i, WS-AP3865e under the ROW regulatory domain.
Adds country support for Trinidad and Tobago for the AP3825i/e under the ROW regulatory domain.
Adds country support for Kuwait to the AP3825i/e under the ROW regulatory domain.
Adds country support for Angola to WS-AP3705i, WS-AP3715i/e, WS-AP3765i/e, WS-AP3767e, WS-AP3825i/e and WS-AP3865e under the ROW regulatory domain.
Adds country support for India to the WS-AP3865e under the ROW regulatory domain.
Adds country support for Qatar to the WS-AP3825i/e under the ROW regulatory domain.
Adds country support for Saudi Arabia to the WS-AP3825i/e under the ROW regulatory domain.
Adds country support for Mexico under the ROW and NAM regulatory domains.

Enhancements in 9.15.01.0121
Support for HTTPS Traffic redirect to the Captive Portal.
Support for using Individually assigned MAC Address per Ethernet Port.
Extend auto-login captive portal detection to Android, Windows and Blackberry.
Remove need for administrator to approve certificates for maintenance releases.
Update NAC VNS Wizard to include Default VSAs.

Changes in 9.15.01.0121	
wns0011052	Corrected an issue whereby the configuration of an AP could be overwritten by the foreign controller.

Enhancements in 9.12.04.0003
wns0008230 Adds country support for Iraq to the WS-AP3705i under the ROW regulatory domain.
wns0010628 Adds country support for Taiwan to the WS-AP3825i under the ROW regulatory domain.
wns0011066 Adds country support for Armenia to WS-AP3705i, WS-AP3715i, WS-AP3825i, WS-AP3865e under the ROW regulatory domain.
wns0011212 Adds country support for India to the WS-AP3865e under the ROW regulatory domain.
wns0011214 Adds country support for Qatar to the WS-AP3825i/e under the ROW regulatory domain.
wns0011215 Adds country support for Saudi Arabia to the WS-AP3825i/e under the ROW regulatory domain.
wns0011141 Adds country support for Angola to WS-AP3705i, WS-AP3715i/e, WS-AP3765i/e, WS-AP3767e, WS-AP3825i/e and WS-AP3865e under the ROW regulatory domain.

Changes in 9.12.04.0003	
wns0010987	Corrected a VLAN tagging issue on WS-AP3705i port, when using Bridge @ Controller mode
wns0011118	Added support to use colon “:” in a policy name
wns0011119	Corrected a memory management issue that could cause an WS-AP3610 to reset
wns0011138	Corrected platform validation issue that affected firmware upgrade of WS-AP2600 from CLI
wns0011166	Corrected a memory management issue that affecting location capabilities under high load
wns0011233	Corrected a synchronization issue that prevents saving of Virtual Network Services settings

Enhancements in 9.12.03.0009
wns0010723 Adds country support for AP3715i for Zambia under the Rest-Of-World regulatory domain.
wns0010724 Adds support for the AP3825i/e and the AP3865e for Singapore to the Rest-Of-World regulatory domain.
wns0010889 Adds country support for the AP3765i for Angola under the Rest-Of-World regulatory domain.
wns0011054 Adds support for the WS-AO-DX07025N & WS-AO-5D23009N for ETSI to the AP3865e.
wns0011064 Adds country support for all the 3700 and 3800 Series access points for Georgia under the Rest-Of-World regulatory domain.
wns0011121 Adds country support for Trinidad and Tobago for the AP3825i/e under the ROW regulatory domain.
wns0011123 Adds country support for Kuwait to the AP3825i/e under the ROW regulatory domain.

Changes in 9.12.03.0009	
wns0010604 wns0010923	Corrected an issue that could cause new or re-authenticated client sessions to not connect due to a synch issue between local and foreign controllers in a mobility domain.

Changes in 9.12.03.0009	
wns0010916	Corrected an issue that would cause the channel setting to be changed from custom to auto when upgrading from V9.01.03 to V9.12.01.
wns0010964	Corrects an issue that could cause legacy 3600 Series to reboot.
wns0010969	Improved the cleanup algorithms to recover resources from disassociated client sessions faster increasing resiliency of the APs in high-density deployments.
wns0010994	Added an enhancement to allow Guest Portal Admin to search for user accounts by both user name and user ID.
wns0011010	Added an enhancement to preserve the previously configured default gateway if the change to an IP address on the controller is still in the same subnet as the default gateway.
wns0011014	Corrected an issue that prevented V9 policies configured on the controller from being imported into Policy Manager.
wns0011026	Corrected an issue that could cause APs to reboot when there is a large deployment of APs (500+) on the same multicast domain.
wns0011027	Addressed a corner-case race condition whereby a captive portal user could get a "refresh" browser message before the system had changed their topology from an unauthenticated to an authenticated state.
wns0011038	Improved the resiliency of the AP in very high-density user environments that results in heavy log event generation.
wns0011041	Corrected a corner condition whereby the last fragment of a certificate chain was incorrectly fragmented by the AP to the controller if the certificate size caused the frame size to exceed the MTU size.
wns0011093	Corrected an issue that would prevent jumbo frames from working correctly when configured in conjunction with link aggregation on the controller.

Enhancements in 9.12.02.0006
wns0009964 Added a feature to ensures interoperability with Draeger Infinity M300s.
wns0009320 Adds country support for Oman to the AP3765e under the ROW regulatory domain.
wns0009556 Adds country support for Ecuador to the AP3705i & AP3715i/e under the ROW regulatory domain.
wns0010845 Adds support for the following new TLVs for MAC-based, 802.1x, and captive portal authentication: for all RADIUS accounting messages (Event Timestamp, Operator Name), and for interim and accounting stop messages (Acct-Input-Gigawords, Acct-Output-Gigawords).
wns0010906 Adds country support for South Africa to the AP3825e under the ROW regulatory domain.
wns0010960 Adds support for DFS channels 52 – 64 and 100 – 140 for the AP3825i/e under the NAM (FCC) regulatory domain.

Changes in 9.12.02.0006	
wns0010710	Corrected a memory management issue that could cause an AP3705i to reset.
wns0010843	Corrected a memory management issue affecting 3800 Series access points.
wns0010983	Corrected the power output for AN-HT40 rates for the 376X Series APs for Argentina.
wns0010879	Corrected the power settings for New Zealand for the AP3865e when using the WS-DS02360N antenna.

Enhancements in 9.12.01.0067
Introducing support for the ExtremeWireless AP3865e, a high-performance, high-availability IEEE802.11ac 3x3:3 MIMO outdoor access point for high-density deployments in extreme weather conditions.

Enhancements in 9.12.01.0067
Adds support for “application” policy rules enabling granular control of Bonjour/LLMNR service requests and service advertisements.
Adds support for Guardian mode to the AP376X and AP3865 as well as in-service mode for the AP3865e.
Adds support for Rogue AP detection in Guardian mode to the 3800 Series.
Adds support for scheduled AP Log Collection for the 3000 Series. The AP log collection feature does not work if the APs are deployed on the secure side of a firewall and the controller is deployed on the unsecure side.
Increases the number of MUs tracked by the location services engine to 2,500 for the C5110, C4110, and V2110 and to up to 1,024 MUs for the C25.
The AP3825 and AP3865 became WiFi Alliance compliant and received the “WiFi certified” status from TUV.

Changes in 9.12.01.0067	
wns0010129	Corrected a memory management issue on 11n APs that could cause the AP to reboot.
wns0010481	Corrected an issue whereby a transient RF event could result on a false positive and subsequent AP reset on the 3710s.
wns0010826	Corrected an issue that could generate an intermittent debug message if the GUI application could not collect the necessary data to render a configuration screen.
wns0010034	Corrected a memory management issue that could cause the AP36XX Series APs to reboot.
wns0010174	Corrected a memory management issue with the LLDP service on the APs that could cause the AP to reboot.
wns0010056	Corrected an issue that prevented some Apple devices from connecting to a hidden SSID.
wns0010645	Corrected an issue with broadcast/multicast filtering that could result in DHCP packets being dropped intermittently when using DHCP relay and routed topologies.
wns0010581	Corrected the DFS algorithm used for the AP3710i/e for Mexico in the regulatory tables.
wns0010575	Corrected regulatory tables for channels 149-165 for Korea.
wns0010553	Added a GUI enhancement to prevent an administrator from entering a bad ICP non-auth configuration.

Enhancements in 9.01.03.0008
Adds support for Taiwan to the AP3715i/e under the ROW regulatory domain.
Improved the default security stance of SSHd by disabling 96-byte MD5 and SHA1 key sizes.
Adds support for Turkmenistan to the AP3700 Series and AP3825i/e under the ROW regulatory domain.
Adds support for India to the AP3825i/e under the ROW regulatory domain.
Adds support for Band 4 of the 5G spectrum for Macau to the AP3715i/e.
Adds support for Band 4 of the 5G spectrum for Macau to the AP3825i/e.
Adds support for the 2.4G spectrum for Macau to the AP376X Series.
Adds support for Turkmenistan to the AP376X Series under the ROW regulatory domain.
Added support for DFS channels 52-64 and 100-140 for all AP376X models under the NAM (FCC) regulatory domain.

Changes in 9.01.03.0008	
wns0008388	Improved the resiliency of the AP3600 Series when a malformed E/N packet is received on the wired port.

Changes in 9.01.03.0008	
wns0010034	Corrected a memory management issue that could cause the AP36XX Series APs to reboot.
wns0010473	Corrected a memory management issue that could cause a controller to reset
wns0010551	Corrected an issue with the ECP interface whereby the controller was not returning the correct topology name for an MU associated to an unauth policy.
wns0010585	Corrected an issue whereby the AP would continue to send packets to a mobile device that was in sleep mode causing the loss of data packets.
wns0010638	Increased the length of the SNMP password parameter to account for protecting the password via encryption in the configuration file.
wns0010645	Corrected an issue with broadcast/multicast filtering that could result in DHCP packets being dropped intermittently when using DHCP relay and routed topologies.
wns0010763	Corrected the power settings for Kuwait for the AP376X Series; removes channels 36-64 for outdoors.
wns0010756	Corrected the power settings for Taiwan for the AP3705i.

Enhancements in 9.01.02.0017
Adds country support for India to the WS-AP3710i/e under the ROW regulatory domain.
Adds country support for Russia to the WS-AP3715i/e under the ROW regulatory domain.
Adds country support for Russia to the WS-AP3710i/e under the ROW regulatory domain.
Adds country support for Russia to the WS-AP3825i/e under the ROW regulatory domain.
Adds country support for Korea to the WS-AP3715e under the ROW regulatory domain.
Adds country support for Korea to the WS-AP3825i under the ROW regulatory domain.

Changes in 9.01.02.0017	
wns0009570	Corrected a memory management issue that could cause legacy 2610/20 to reboot.
wns0010593	Corrected an issue that would cause AP3715 unstable when Load balance feature is enabled.
wns0010509	W788-2RR access points are not supported in release 9.0 and higher

Enhancements in 9.01.01.0228
Introducing support for the ExtremeWireless AP3825i and AP3825e, two new high-performance, high-availability IEEE802.11ac 3x3:3 MIMO indoor access points for mission critical deployments.
Enhanced IdentiFi Guardian to detect the presence of Rogue APs via a closed-loop wired/wireless mechanism thereby reducing false positives (unauthorized APs attached to an authorized network).
Adds support for automatically provisioning the power settings for professionally installed external antennas based on installer configurable attenuation levels.
The internal Captive Portal can now be configured to use either http or https.
Adds the ability to encapsulate mini-Jumbo frames for tunneled data traffic from the AP to the controller without the need to fragment and reassemble larger packets. Supported on the C5210, C5110, C4110, AP3710, AP3715 and AP3825
Adds support for the ETS Resource Utilization MIB enabling SNMP management systems to query the CPU/memory utilization of a controller.
Adds support for backing up a controller configuration to a USB key.
Adds support for dynamic LAG via LACP enabling active/active dual-Ethernet data paths to the AP3825.
Adds support for ESXi Application Monitoring to the V2110.
Increased the AP capacity of the V2110 by two APs to 250 APs in normal mode and 500 APs in failover mode, matching the C4110 for HA deployments.

Enhancements in 9.01.01.0228
Adds support for license pooling of AP and Radar capacity licenses within an HA pair and simplifies the load-balancing of APs between controllers in the HA pair.
Adds country support for Singapore to the WS-AP3710i/e under the ROW regulatory domain.
Adds country support for Aruba to the WS-AP3705i and WS-AP3715i/e under the NAM/FCC regulatory domain.
Adds country support for Curacao to the WS-AP3705 and WS-AP3715 under the NAM/FCC regulatory domain.
Adds country support for Barbados to the WS-AP3705i, WS-AP3715i/e under the NAM/FCC regulatory domain.
Adds country support for Kuwait to the WS-AP3715i under the ROW regulatory domain.
Adds country support for Egypt to the WS-AP3715i under the ROW regulatory domain.
Adds country support for Saudi Arabia to the WS-AP3715i/e under the ROW regulatory domain.
Adds country support for Angola to the WS-AP3715i under the ROW regulatory domain.
Adds country support for South Africa to WS-AP3715i/e under the ROW regulatory domain.
Adds country support for Jamaica to the WS-AP3705, WS-AP3715 under the NAM/FCC regulatory domain.
Adds country support for Trinidad and Tobago to the WS-AP3705i, WS-AP3715i/e under the ROW regulatory domain.
Adds country support for South Africa to the WS-AP3710e under the ROW regulatory domain.
Adds country support for Colombia to the WS-AP3715e under the NAM/FCC regulatory domain.
Adds country support for China to the WS-AP3715i under the ROW regulatory domain.
Adds country support for Mexico to the WS-AP3715i/e under the NAM/FCC regulatory domain.
Adds country support for Singapore to the WS-AP3715i/e under the ROW regulatory domain.
Adds support for the 2.4GHz spectrum for Macau to the WS-AP3705i, WS-AP3715i and WS-AP3715e under the ROW regulatory domain.
Adds support for the WS-AO-DX10055, a new outdoor service antenna, to the WS-AP376Xe.
Adds country support for Egypt to the WS-AP3715e under the ROW regulatory domain.
Corrects the regulatory compliance table for Taiwan for on the WS-AP3705i to allow channels 149-165.
Adds support for Macau to the WS-AP3610, WS-AP3710i/e and WS-AP376X under the ROW regulatory domain.
Adds support for Hong Kong to the WS-AP3710i/e under the ROW regulatory domain.
Adds support for DFS channels to the WS-AP3710e under the NAM/FCC regulatory domain.
Adds support for DFS channels to the WS-AP3715i/e under the NAM/FCC regulatory domain.

Changes in 9.01.01.0228 (ported from 8.32.05.0007)	
wns0010126	Corrected an issue that would cause a device to see their own MAC address when querying for duplicate addresses due to a malformed gratuitous ARP request from the originating client.
wns0010104	Corrected an issue that would cause a “no change” topology to be added to the “Active Clients by VNS” report.
wns0009915	Corrected an issue that prevented a certificate from being loaded if the certificate file matched the CSR file name of the controller.
wns0009903	Corrected an issue that was causing roaming instability with Motorola HDT scanners due to a 0 length EAP packet.
wns0009866	Corrected an issue that could result in the configuration file being corrupted during an upgrade of a V2110 in the presence of a large CDR database.
wns0009850	Corrected an issue that prevented the Traffic Summary to be reported accurately in the Active Clients By VNS report.

Changes in 9.01.01.0228 (ported from 8.32.05.0007)	
wns0009837	Corrected an issue that prevented Guest user accounts from being synchronized in a high-availability pair.
wns0009836	SNMP queries to ifOperStatus, ifAdminStatus, and IfDescr tables are now working correctly.
wns0009815	Corrected an issue that was preventing SNMP queries to the ipNetToMediaPhysAddress from working.
wns0009811	Corrected an issue that could result in a mis-configuration when changing the configuration of an AP from a 20MHz channel to Auto.
wns0009806	Corrected regulatory settings for China on the 3610s for the 5.7-5.8 band.
wns0009803	Corrected an issue with the export of “All Clients” report which prevented XML parsers from reading the report.
wns0009761	Corrects an instability issue that could cause an intermittent reset on certain APs.
wns0009743	Correctly disables channels 120, 124, and 128 for AN-HT20 for the AP3620 with the WS-ANT02 due to regulatory requirements. Unlike the AP3610, the AP3620 can be deployed outdoors and thus it is not able to operate within the DFS/weather channels.
wns0009731	Corrected an issue that resulted in traffic being blocked when a rule matched on QoS settings.
wns0009728	Corrected an issue that could result in instability when trying to apply advanced filter rules in V8.31 to legacy APs.
wns0009723	Corrected an issue that resulted in the controllers reporting an inaccurate user count.
wns0009708	Added a new configuration option via the CLI to overwrite the default timing for key exchange retries. The default retry setting of 100ms may be too aggressive for some legacy clients to respond in time.
wns0009707	Corrected an issue that could cause instability issues with legacy 26XX Series APs when applying configuration changes.
wns0009706	Increased the timeout timer for EAP re-transmissions to minimize connectivity issues with slower clients.
wns0009704	Corrected an issue that prevented a Guardian sensor from accepting a deny list configuration update after detecting a threat.
wns0009698	Corrected a timing issue between the AP and the controller with Guest Portal redirection that could cause the end-user to have to press the submit button twice to continue to their intended page.
wns0009689	Corrected a memory management issue that could result in stability problems when saving configuration changes.
wns0009632	Corrected a statistics counter which was incorrectly reporting an excessive amount of duplicate frames after a radio reset on the 3700 Series.
wns0009610	Corrected the amount of the memory allocated for internal structures to ensure there are enough resources available on the controller for high-density deployments.
wns0009520	Updated the SSH service on the APs to the latest version.
wns0009489	Corrected an issue that prevented Guest users from seeing custom Guest Portal images after an upgrade.
wns0009481	Corrected an issue with the registration service that prevented Scalance W788-2RR from connecting to a controller running V8.21 or higher.
wns0009480	Corrected an issue that caused persistent mode feature to not work.
wns0009476	Corrected an issue that caused foreign controller in the mobility zone to reboot when configuration for active client session is changed on the home controller.
wns0009466	Fixed memory leak when operating as WDS parent with no client WLAN service on AP3660
wns0009465	Corrected an interface synchronization issue after an upgrade that prevented the NTP service from synchronizing the time on the controller.

Changes in 9.01.01.0228 (ported from 8.32.05.0007)	
wns0009459	Corrected an issue that causes instability on the controller under certain scenarios where a user roams from one VNS to another.
wns0009435	Fixed corner case instability caused by synchronization issues on 3710 AP.
wns0009417	The system now rejects administrative RADIUS login passwords and login attempts using Unicode characters.
wns0009342	Fix the instability caused by unused Ethernet interface timer on AP3715
wns0009312	Corrected an issue that allowed station to roam without performing MAC authentication after initial authentication.
wns0009306	Corrected a connectivity issue between the SEN WL2 and 3600 Series introduced in 8.31.01.
wns0009262	Improved interoperability with legacy wireless devices that exclusively use old power save method
wns0009252	Removed channel 120, 124, 128 from AP default settings.
wns0009107	Corrected an issue whereby clients using bridge at controller topology stayed connected when link-persistence was enabled even though the AP-controller link was down due to a physical link layer problem with the cable.
wns0008894	Corrected an issue that causes instability when frame aggregate deletion is requested by wireless client.

KNOWN RESTRICTIONS AND LIMITATIONS:

User Guide errata:
Column K in the .csv guest file indicates the total session used time, measured in **seconds**.

Info
The client of the Intel AC7260 wireless chipset with the drivers 18.32.x or 18.33.x may become un-responsive when client roams outside of Wi-Fi Coverage area and comes back. The Symptom is a Yellow Exclamation mark within the Wi-Fi icon in the task bar. The current work around is to manually refresh the Wi-Fi connection or troubleshoot the Wi-Fi connection.
This issue is fixed in Intel drivers 18.33.3.1 or 18.33.3.2 and above.

wns0015221 – Info
Due to changes in manufacturing procedures, new AP3801i (Rev 5F) and AP3805i/e (Rev 5K) are not compatible with previous 9.21.x firmware. **The release 9.21.10.0005 is the Minimum Firmware version for AP3801i (Rev 5F) and AP3805i/e (Rev 5K) manufactured after April 2016.**

ExtremeWireless Virtual Appliance V2110 MS Hyper-V – Info
It was noticed that Hyper-V controllers with ports mapped to virtual ports of their server do not have the best performance, hence it is recommended to map controller's ports to physical ports.
Clustering Hyper-V is not supported and should not be configured.

wns0014333 – Info
For AP38xx/AP39xx, Adding or removing WLAN services from a radio may result in a temporary service interruption for all services on the radio. Clients on the radio are disassociated and will re-associate soon after service is restarted.

wns0014077 – Info
XBOX 360 client device not connecting with LDPC enabled, workaround is to disable LDPC.

wns0012730– Info
802.11v is not supported in 9.21.xx

wns0012889– Info
Some versions of Apple Mac Books might exhibit low throughput performance when Management Frame Protection (PMF) is enabled.

wns0012862– Info
In order to capture NULL and QOS_NULL packets with WireShark, do not set any Capture Filter and also disable "Do not capture own RPCAP traffic" in Remote Settings. In v1.12.3, this option is found by going to Capture --> Option --> Double Click Interface Row --> Remote Settings.

wns0012749 – Info
Purview integration for V2110 (V9.21) requires at least 3 CPU cores allocated to the VM. By default, the V2110-Small OVA creates a VM with only 2 cores. To enable Purview integration the V2110 must be reconfigured with at least one additional core (3 VCPU).

wns0012722 – Info
The Access Point Name field can be up to 23 characters and must start with alpha characters, not numeric.

wns0012793 – Info
When enabling Sites Mode (V9.21), the Controller’s topology capacity is capped at 128 topologies. Currently APs are unable to process more than 128 topologies, and in site configuration all topologies get pushed to all APs, which effectively limits the maximum per-controller topologies to 128

wns0012678 – Info
Counter measures for honeypot AP threat may be less effective for iPhone (with version 8.3) client device than other device types.

About converting AP3630/AP3640

Only controllers running 8.32 code support converting a 3630/40 back to standalone mode

How to use Real capture tool

- Click Start to start real capture server on the AP. This feature can be enabled for each AP individually. Default capture server timeout is set to 300 seconds and the maximum configurable timeout is 1 hour. While the capture session is active the AP interface operates in promiscuous mode.
- From Wireshark GUI set the capture interface to the selected AP's IP address and select null authentication. Once Wireshark connects to the AP, the AP's interfaces will be listed as available to capture traffic. eth0 is the wired interface, wlan0 is the 5Ghz interface and wlan1 is the 2.4Ghz interface.
- The user can selected to capture bidirectional traffic on eth0, wifi0 and wifi1. The capture on wifi0 and wifi1 will not include internally generated hardware packets by the capturing AP. The capturing AP will not report its own Beacons, Retransmission, Ack and 11n Block Ack. If this information is needed, then the real capture should be done from a close-by second AP. Change that second AP's wireless channel to match the AP that is being troubleshot. Let it broadcast a SSID so the radios switch on, but do not broadcast the same SSID you are troubleshooting, so that the clients do not connect to your second capturing AP.

wns0012709 – Fixed in 9.21.04.0007

Some versions of Apple IOS on iPhone or iPad might exhibit roaming instability while connected to WLAN Service with "Management Frame Protection" is set to Enabled/Required and "Fast Transition" is set to enabled.
Workaround: Disable either "Management Frame Protection" or "Fast Transition"

wns0012567– Info

We recommend not to enable 802.11k along with Quiet IE option for installations with Ascom i62 phones.

Topology groups – Info

Topology groups are not supported for Site deployments. Configuration of Services referencing Topology Groups should result in a “incompatible’ policy resolution at the site, but this may not always be the case, and could result in incorrect topology assignment. We recommend to not configure Topology groups if Site deployments are in use.

wns0012296– Info

Enforcement of Rogue AP countermeasures requires AP in Guardian mode.

wns0011596 – Info

Legacy APs have varied Policy Enforcement Capability. AP2605 does not support policy enforcement.

wns0011707 – Info

AP26xx family does not support advanced policy features such as CP redirection at the AP – contact GTAC for the full KB article.

wns0011519 – Info

Instability observed on the network with Intel AC-7260 based clients.
Workaround: Update the Intel AC-7260 driver and disable Throughput Boost setting in client driver Advanced option.
This issue is not present if the client driver is on 18.20.0.9 or above.

Wns0011589 – Info

AP38XX supports TKIP but with the following restrictions due to new Wi-Fi Alliance certification requirements:

1. Only available for Legacy rates; not supported with 11n nor 11ac rates
2. Mix configuration of AES and TKIP on one radio is not supported; for example, configuring multiple VNS with mixed types of TKIP and AES on one AP radio is not allowed.

wns0011467– Info

RADIUS attribute-value pair limits the location data size to 251 characters. In the case that the location data size is more than 251 characters then this data will be sent to the RADIUS server truncated to 251 characters.

wns0011008– Info

The Location Batch Report file contains two timestamp attributes. Both of them are currently in local time, but the time zone indicator is missing. These fields should be reported as UTC time with the time zone set to 'Z'

wns0010642– Info

Chrome autocomplete function fills in fields incorrectly. Users should disable password saving and password field auto completion in their Chrome configuration.

wns0010265 – Info

In V9.21 the conversion from AP3630/40 “thin” mode to standalone mode is not supported. To convert an AP3630/40 from standalone mode to thin mode, first use V8.32 for the conversion. Once converted to V8.32 the AP becomes a 3610/20 and can then connect to a V9.21 controller.

wns0010168 – Info

"ac-strict" radio mode may not operate correctly with all clients. At release date (June 26, 2015) the Intel AC 7260 client does not operate if ac-strict is set.

wns0008740 – Info

APs advertising the SSIDs of administratively disabled WLAN Services will not be detected as internal honeypots until the WLAN Service is enabled.

Info

MacBook Air running SW prior to 10.8.4 can experience random disconnections (mostly noticeable during video streaming). The issue was a bug in the Apple WiFi driver and it is corrected in SW 10.8.4.

wns0008979 - Info

For "g/n" mode operation of the AP with wireless clients based on Intel 6300N chipset with driver 15.x/14.3.x recommended setting is to disable "11g protection".
Set AP/Radio2/Advanced --> 11g Settings / Protection mode --> None.

wns0008035 - Info

WDS doesn't work when the AP name is over 32 characters. Please limit the AP name under 32 characters when the AP is used in WDS or Mesh service.

wns0008023 - Info

On C5210, status on interface without physical transceivers plugged reported Up and Down.

wns0006968 - Info

The SNMP agent generates traps to notify the administrator of configuration changes, component failures, disconnection of Access Points or any other events that may need the administrator’s attention. Administrators can configure the Agent and the Controller as to what level of trap they wish to receive. The traps type that are supported by the ExtremeWireless Controllers are:

1. Interfaces MIB (IF-MIB) linkDown (.1.3.6.1.6.3.1.1.5.3)
2. Interfaces MIB (IF-MIB) linkUp (.1.3.6.1.6.3.1.1.5.4)
3. HIPATH-WIRELESS-HWC-MIB apTunnelAlarm (.1.3.6.1.4.1.4329.15.3.19.4)
   - Sent by the controller when it detects that it has lost the connection to an AP. The trap identifies the AP that the controller can no longer contact
4. HIPATH-WIRELESS-HWC-MIB hiPathWirelessLogAlarm (.1.3.6.1.4.1.4329.15.3.9.6)
   - A trap containing one event that also is displayed in the controller’s Event / Log report page. The trap is sent when the event is raised and recorded on the controller.
   - This trap accounts for the vast majority of traps messages sent by the controller at most sites.
   - The trap contains the trap severity, the component on the controller that raised the event and the text string associated with the event, just as it would appear in the controller GUI.

The item listed under #4 is a generic trap that contains specific information relevant to the event. The information varies from event to event and are all carried in the trap.

wns0007074 - Info

A partially specified policy is one that has “No change” selected for filters, default topology or default qos. When a partially specified policy is assigned to a station the “no change” settings are replaced by the elements from another policy applied to the station. When a station successfully authenticates and is assigned a partially specified policy, the “No change” elements of the policy are replaced with the corresponding elements of the WLAN Service’s default authenticated policy.

Consider the following example. Suppose a VNS is defined that uses policy P1 for its default non-authenticated policy and policy P2 for its default authenticated policy. Policy P1 assigns the station to topology T1 and policy P2 assigns the station to topology T2. Suppose there is a policy P3, that has "no change" set for its topology.

A client on the VNS will be assigned to P1 with topology T1 when he first associates to the VNS. Now suppose the station is assigned P3 by the RADIUS server when the station authenticates. Even though the station is on T1 and P3 has no change set for the topology, the station will be assigned to T2. When the client is authenticated, internally on the controller, the client is first assigned to P2 then P3 is applied.

A similar scenario exists when the hybrid mode policy feature is set to use tunnel-private-group-id to assign both policy and topology but for some reason the VLAN-id-to-Policy mapping table does not contain a mapping for the returned tunnel private group id. In this case a station that successfully authenticates would be assigned the filters and default QoS of the WLAN Service's default authenticated policy and the topology with the VLANID contained in the Tunnel-Private-Group-ID of the ACCESS-ACCEPT response.

If this is not the desired behavior, then:
1. Avoid using partially specified policies.
2. When the controller is configured to map the VLAN ID in the Tunnel-Private-Group-ID response to a policy using the mapping table, ensure that there is a policy mapping for each VLAN ID that can be returned to the controller by the RADIUS server.

SUPPORTED WEB BROWSERS

For EWC management GUI, the following Web browsers were tested for interoperability:

- MS IE 8.0, IE9, IE10, IE11
- FireFox 38.0
- Google Chrome 43.0

Wireless Clients (Captive Portal, AAA):

Browsers	Version	OS
Chrome	38.0.2125.111 m	Windowx XP
Firefox	33.1	Windows XP
IE 11	11.0.9600.17420	Windows XP
IE 11	11.0.9600	Windows server 2012
Chrome 35	35.0.1916.153 dev-m	Windows server 2012
FireFox 33	33.0.2	Windows server 2012
IE 8	8.0.7601	Windows 7
Chrome	38.0.2125	Windows 7
Opera beta	26.0.1656.17	Windows 7
Chrome	38.0.2125.111 m	Windows 7
Firefox	33.0.2	Windows 7
IE	11.0.9600.17420	Windows 7
IE	8.0.6001.18702	Windows XP
Firefox 31	31.0	Windows 7
IE10	10.0.9200.17116	Windows 7
Chrome	38.0.2125.111 m	Windows 7
IE10	10.0.9200.16688	Windows server 2012
Chrome	38.0.2125.111 m	Windows 7
Chrome	38.0.2125.111 m	Windowx XP
Firefox	33.1	Windows XP
IE 11	11.0.9600.17420	Windows 8.1
IE 11	11.0.9600	Windows server 2012
Chrome 35	35.0.1916.153 dev-m	Windows server 2012
FireFox 33	33.0.2	Windows server 2012
IE 11	11.0.9600	Windows 7
IE 8	8.0.7601	Windows 7
Chrome	38.0.2125	Windows 7
Opera beta	26.0.1656.17	Windows 7
Chrome	38.0.2125.111 m	Windows 7
Microsoft Edge	20.10240	Windows 10
IE 11	11.0.10240	Windows 10

PORT LIST

The following is a list of ports that may be required to be open, in order that the controllers/APs will work properly on a network, which includes protection via equipment like a firewall.

ExtremeWireless TCP/UDP Port Assignment Reference

Component		**Protocol (TCP/UDP)**	**Src Port**	**Dest Port**	**Service**	**Remark**	**Require Firewall to open**
Source	Destination						
Ports for AP/Controller Communication							
Controller	Access Point	UDP	Any	13910	WASSP	Management and Data Tunnel between AP and Controller	Yes
Access Point	Controller	UDP	Any	13910	WASSP	Management and Data Tunnel between AP and Controller	Yes
Controller	Access Point	UDP	4500	Any	Secured WASSP	Management Tunnel between AP and Controller	Optional
Access Point	Controller	UDP	Any	4500	Secured WASSP	Management Tunnel between AP and Controller	Optional
Access Point	Controller	UDP	Any	13907	WASSP	AP Registration to Controller	Yes
Access Point	Controller	UDP	Any	67	DHCP Server	If Controller is DHCP Server for AP	Optional
Access Point	Controller	UDP	Any	427	SLP	AP Registration to Controller	Optional
Controller	Access Point	TCP/UDP	Any	69	TFTP	AP image transfer	Yes[1]

[1] TFTP uses port 69 only when the secure control tunnel is NOT enabled between the AP and controller. If the secure control tunnel is enabled TFTP exchanges take place within the secure tunnel and port 69 is not used.

Access Point	Controller	TCP/UDP	Any	69	TFTP	AP image transfer	Yes[2]
Controller	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
Ports for Controller Management							
Any	Controller	TCP/UDP	Any	22	SSH	Controller CLI access	Yes
Any	Controller	TCP/UDP	Any	5825	HTTPS	Controller GUI access	Yes
Any	Controller	TCP/UDP	Any	161	SNMP	Controller SNMP access	Yes
Any	Controller	TCP/UDP	Any	162	SNMP Trap	Controller SNMP access	Yes
Ports for Inter Controller Mobility and Availability							
Controller	Controller	UDP	Any	13911	WASSP	Mobility and Availability Tunnel	Yes
Controller	Controller	TCP	Any	427	SLP	SLP Directory	Yes
Controller	Controller	TCP	Any	20506	Langley	Remote Langley Secure	Yes
Controller	Controller	TCP	Any	60606	Mobility	VN MGR	Yes
Controller	Controller	TCP	Any	123	NTP	Availability time sync	Yes
Controller	DHCP Server	UDP	Any	67	SLP	Asking DHCP Server for SLP DA	Yes
DHCP Server	Controller	UDP	Any	68	SLP	Response from DHCP Server for SLP DA request	Yes
Core Back-End Communication							
Controller	DNS Server	UDP	Any	53	DNS	If using DNS	Optional
Controller	Syslog Server	UDP	Any	514	Syslog	If Controller logs to external syslog server	Optional

[2] TFTP uses port 69 only when the secure control tunnel is NOT enabled between the AP and controller. If the secure control tunnel is enabled TFTP exchanges take place within the secure tunnel and port 69 is not used.

Controller	RADIUS Server	UDP	Any	1812	RADIUS Authentication and Authorization	If using RADIUS AAA	Optional
Controller	RADIUS Server	UDP	Any	1813	RADIUS Accounting	If enabled RADIUS accounting	Optional
Dynamic Authorization Client (typically NAC)	Controller	UDP	Any	3799	Dynamic Authorization Server (DAS)	Request from Dynamic Authorization Client to disconnect a specific client	Optional
Controller	AeroScout Server	UDP	1144	12092	Location-Based Service Proxy (lbs)	AeroScout Location-Based Service	Optional
AeroScout Server	Controller	UDP	12092	1144	Location-Based Service Proxy (lbs)	AeroScout Location-Based Service	Optional
Controller	Check Point	UDP	Any	18187	Checkpoint	Logging to Check Point Server	Optional

IETF STANDARDS MIB SUPPORT:

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

ENTERASYS NETWORKS PRIVATE ENTERPRISE MIB SUPPORT

Enterasys Networks Private Enterprise MIBs are available in ASN.1 format from the Extreme Networks website at: http://www.extremenetworks.com/support/policies/mibs/. Indexed MIB documentation is also available.

Enterasys Proprietary MIBs

Title	Description
enterasys-configuration-management-mib.txt	Used to perform configuration backup and restore
ENTERASYS-CLASS-OF-SERVICE-MIB	Used for configuration/monitoring CoS and rate control

Title	Description
ENTERASYS-POLICY-PROFILE-MIB	Used for configuration/monitoring policy and rules assignments
ENTERASYS-RADIUS-AUTH-CLIENT-MIB	Used for configuration of RADIUS Authentication servers
ENTERASYS-RADIUS-ACCT-CLIENT-EXT-MIB	Used for configuration of RADIUS Accounting servers
ENTERASYS-IEEE8023-LAG-MIB-EXT-MIB	Used for configuration/monitoring LAG port

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
IEEE8023-LAG-MIB	LAG configuration information. Set is permitted for LAG L2 port configuration only.

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

The following 802.11ac and 80211n clients are known to work with 9.21 software release:

Device	OS	Brand	Model
Notebook	Windows XP	Cisco	WUSB600N
Notebook	Windows XP	Netgear	WN511T
USB	Window 8	ASUS	AC1200
Onboard	Windows 7	Intel	Wireless WiFi Link 4965AGN
PCMCIA	Windows XP	Broadcom	Rangemax Next WN511B
USB	Windows 8	Dell	Wireless 1901
Onboard	Windows 8	Intel	Centrino Ultimate-N 6300 AGN
Onboard	Windows 7	Intel	Centrino Ultimate-N 6300 AGN
Notebook	Windows 7	Intel	AC 7260
Notebook	Windows 8.1 Windows 10	Intel	AC-7260
USB	Windows 7	Asustek	USB N66
Notebook	Windows 8	Asus	USB-AC56
USB	Window 7		Cisco AE6000
Surface 3 Pro	Windows 8.1	Marvell	
MacBook Air	OS X 10.9.5	Apple	AirPort Extreme
iPad	iOS	Apple	iPad
iPad	iOS	Apple	iPad Air
iPad	iOS	Apple	iPad Mini
iPad	iOS	Apple	iPad 2
iPad	iOS	Apple	iPad 3
iPhone	iOS	Apple	iPhone 5
iPhone	iOS	Apple	iPhone 6
iTouch	iOS	Apple	iTouch
MacBook	iOS	Apple	MacBook Pro
Nexus	Android	HTC	Nexus 9
Nexus	Android	LG	Nexus 4
Galaxy	Android	Samsung	Galaxy 4
Galaxy	Android	Samsung	Galaxy 3
Galaxy	Android	Samsung	Galaxy S 500
PCI-e	Windows 7	Asus	PCE-AC802.11ac
Nokia Lumia 830	Windows 8.1	Microsoft	Lumia 830

RADIUS SERVERS AND SUPPLICANTS

RADIUS Servers used during testing

Vendor	Model OS	Version
FreeRADIUS45	1.1.6	FreeRADIUS
FreeRADIUS21 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
FreeRADIUS45	1.1.6	FreeRADIUS

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 Enterasys	G3	01.00.02.0001	For PoE
	G3	06.11.01.0040	
	C20N1	Version 12.1(19)EA1c	No PoE

Vendor	Model OS	Version	Tested with
	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
	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	Linux	0.9.8e

RADIUS ATTRIBUTES SUPPORT

RADIUS Authentication and Authorization Attributes

Attribute	RFC Source
Called-Station-Id	RFC 2865, RFC 3580
Calling-Station-Id	RFC 2865, RFC 3580
Class	RFC 2865
EAP-Message	RFC 3579

Event-Timestamp	RFC 2869
Filter-Id	RFC 2865, RFC 3580
Framed-IPv6-Pool	RFC 3162
Framed-MTU	RFC 2865, RFC 3580
Framed-Pool	RFC 2869
Idle-Timeout	RFC 2865, RFC 3580
Message-Authenticator	RFC 3579
NAS-Identifier	RFC 2865, RFC 3580
NAS-IP-Address	RFC 2865, RFC 3580
NAS-IPv6-Address	RFC 3162
NAS-Port	RFC 2865, RFC 3580
NAS-Port-Id	RFC 2865, RFC 3580
NAS-Port-Type	RFC 2865, RFC 3580
Password-Retry	RFC 2869
Service-Type	RFC 2865, RFC 3580
Session-Timeout	RFC 2865
State	RFC 2865
Termination-Action	RFC 2865, RFC 3580
Tunnel Attributes	RFC 2867, RFC 2868, RFC 3580
User-Name	RFC 2865, RFC 3580
Vendor-Specific	RFC 2865

RADIUS Accounting Attributes

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

GLOBAL SUPPORT:

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

For the toll-free support number in your country:
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 95119
California USA

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