

Customer Release Notes

ExtremeWireless™ Convergence Software

Software Version 10.11.01.0210

June 30, 2016

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 | 10.11.01.0210 | Minor Feature Release | June 29, 2016 |
| Previous Version | 10.01.05.0008 | Maintenance Release | June 3, 2016 |
| Previous Version | 10.01.04.0011 | Maintenance Release | April 22, 2016 |
| Previous Version | 10.01.03.0007 | Maintenance Release | March 7, 2016 |
| Previous Version | 10.01.02.0038 | Maintenance Release | February 2, 2016 |
| Previous Version | 10.01.01.0129 | Major Feature Release | December 11, 2015 |

SUPPORTED CONTROLLERS AND ACCESS POINTS

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

| Product | Image |
|--|---------------------------|
| ExtremeWireless Controller C4110 | AC-MV-10.11.01.0210-1.gxe |
| ExtremeWireless Controller C5110 | AC-MV-10.11.01.0210-1.tx |
| ExtremeWireless Controller C5210 | AC-MV-10.11.01.0210-1.rue |
| ExtremeWireless Controller C25 | AC-MV-10.11.01.0210-1.pfe |
| ExtremeWireless Controller C35 | AC-MV-10.11.01.0210-1.cwe |
| ExtremeWireless Virtual Appliance V2110 VMware | AC-MV-10.11.01.0210-1.bge |

| | |
|--|---------------------------|
| ExtremeWireless Virtual Appliance V2110 MS Hyper-V | AC-MV-10.11.01.0210-1.ize |
| Wireless AP3935i/e_FCC/ROW | AP3935-10.11.01.0210.img |
| Wireless AP3965i/e_FCC/ROW | AP3935-10.11.01.0210.img |
| Wireless AP3801i | AP3801-10.11.01.0210.img |
| Wireless AP3805 & AP3805i_FCC/ROW | AP3805-10.11.01.0210.img |
| Wireless AP3865 | AP3825-10.11.01.0210.img |
| Wireless AP3825 | AP3825-10.11.01.0210.img |
| Wireless AP3715 | AP3715-10.11.01.0210.img |
| Wireless AP3710 | AP3710-10.11.01.0210.img |
| Wireless AP3705i | AP3705-10.11.01.0210.img |
| Wireless AP3765 | W78XC-2-10.11.01.0210.img |
| Wireless AP3767 | W78XC-2-10.11.01.0210.img |

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*.

Installation Notes

- The minimum system software version is 09.21.01 to upgrade to this software version.
- 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.
- The V2110 is supported on ESXi version 5.5 and 6.0. 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.
- 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. VMware requires that the customer purchase a license to use this feature.
- 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. The V2110 is supported on ESXi version 5.5 and 6.0. 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.
- If configuring a service that will incur topology changes after user gets an IP address via DHCP, for example due to authentication state, it is recommended to use short lease times on the initial topology (un-auth topology) so that clients automatically re-negotiate a new address faster (typically at half-lease). Alternatively, it may be required to manually renew the DHCP lease from the client.
- 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.
- 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.
- 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.
- \, ', " characters are not supported in WLAN/VNS fields.
- In case of upgrade to V10.XX, if an existing VNS has WMM disabled, only legacy clients will be serviced until WMM is enabled.
- For APs with dual Ethernet ports, both interfaces need to be connected to the same subnet/VLAN for Link Aggregation.

Upgrading Virtual Appliance V2110 VMware to the Current Release

You only need to install the ".ova" file when you first install the V2110 VMware. The latest .ova file is V2110-10.01.02.0038.ova. 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 Convergence Software Maintenance Guide".

Upgrading V2110 Virtual Appliance V2110 MS Hyper-V to the Current Release

You 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 Convergence Software Maintenance Guide".

Configuring the Shared Secret for Controller Communication

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 *User Guide* (v5.1 or higher) for a description of how to configure the shared secret on a Wireless Manager.

NETWORK MANAGEMENT SOFTWARE SUPPORT

| Network Management Suite (NMS) | Version |
|---|---------------|
| ExtremeManagement™ | 6.3 or higher |
| ExtremeManagement™ Wireless Advanced Services | 4.4 |
| ExtremeControl™ | 6.3 or higher |

Note:

Configuration of the AP3935/AP3965 is not yet supported via ExtremeManagement™'s WirelessManager.

IMPORTANT: EXTREMEWIRELESS V10 LICENSING CHANGES

Consolidated the regulatory domains to FCC, ROW, Base (for no domain specified). The FCC domain is limited to the US (and US territories), Puerto Rico, and Colombia. All other countries where an AP is certified falls under the Rest-Of-World (ROW) regulatory domain including countries previously under the NAM domain (e.g. Canada). BASE only allows management of AP3935/AP3965. Customers that have a valid maintenance contract must request a V10.01 upgrade license (available through the Extranet Licensing Site) before upgrading the appliance to V10.01.

EXTREMEWIRELESS V9 TO V10 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 9 to version 10). Old activation keys will not carry over in the upgrade process, but feature licenses (incremental AP licenses, Radar, etc.) are carried over on the same controller.

After an upgrade from NAM to FCC, if the AP country is not supported, then the AP radios are disabled.

After an upgrade, a customer is given a 7-day grace period. If customer does not activate an upgraded system, then customer loses the ability to manage VNS configuration and Radar scanning. Logs are recorded every 15 minutes to remind the customer to install a valid 10.01 activation key.

To request a new V10 license key:

1. Log into your Extreme Networks Extranet account (<https://extranet.extremenetworks.com/>).
2. Select the Product Licensing link (<https://extranet.extremenetworks.com/mysupport/licensing>).
3. Select the **ExtremeWireless Upgrade Licenses** option from the list of tasks on the right-hand menu.
4. Fill in the simple form:

Upgrade Version: select V10

Contract Number: type your service contract number

MAC Address: type the dash-delimited MAC Address of your ExtremeWireless controller

5. Click **Submit**.
6. Once the form has been submitted, it will be reviewed by Order Management to confirm the contract is valid for a version 10 upgrade.
7. Upon approval, the user is notified by email and given an Entitlement ID that must be redeemed through the user's Extranet account (follow the emailed instructions).
8. Once the Entitlement is redeemed, an activation key is emailed to the user (it can be directly copied by the user).
9. Enter 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

| Enhancements in 10.11.01.0210 |
|---|
| Software |
| Enhanced customer control over network traffic operation, by providing visibility of the Top 5 application groups per SSID and per individual user on the wireless appliance dashboard and report. |
| Introducing new policy definition and enforcement to support Layer7/application rules specific to control (allow, deny, QoS, rate limiting, VLAN containment) for over 3,000 fingerprints covering 2,000+ web-based applications. |
| Improved visibility of associating devices by providing improved fingerprinting of client device's device type and operating system. Device characteristics are represented on the device's report as well as an aggregate representation of top 5 device types and OS on a per WLAN basis. |
| Improved visibility and flexibility of roles defined for Captive Portal functions, by introducing an explicit REDIRECT action. This action allows user to specifically define when HTTP/HTTPS redirection should take place within the role. |
| Enhanced Access Points (AP38XX/39XX) to directly support redirection and Firewall Friendly External Captive Portal (FFECP) for distributed topologies. |
| Added support for wireless countermeasures to the AP39XX Series platforms. |
| Added the ability to hide the SSID for a WDS mesh for increased security. |
| Streamlined the AP configuration simplifying the process of provisioning of large scale AP deployments. |
| Upgraded the operating system to a 64bit kernel for the wireless appliances. |
| Enhanced Batch Location Report (BLR) to include the option to provide snapshot of full set of statistic metrics for associated Mobile Units (Mus) |
| Increased the number of APs that can be configured as a site to 100 and 2,000 sessions. |
| Enhanced the SNMP interface to include PerProtocol statistics. |
| wns0015080 Added country support for Ecuador to the AP3965e-ROW. |
| wns0015082 Added country support for Colombia to the AP3805i-FCC. |
| wns0015077 Added country support for United Arab Emirates to the AP3965i/e-ROW. |
| wns0015087 Updated Pakistan and Mexico to the latest regulations for all tables. |
| wns0015081 Added country support for Mexico to the AP3965i/e-ROW. |
| wns0015096 Added country support for India to the AP3935i/e-ROW. |
| wns0015086 Added country support for Pakistan to the AP3805i/e and AP3825i/e. |
| wns0015093 Added country support for Mexico to the AP3935i/e-ROW. |
| wns0015079 Added country support for India to the AP3965i/e-ROW. |
| wns0015085 Added country support for Argentina to the AP3805i/e and AP3865e. |
| wns0014815 Added country support for Malaysia to the AP3935i/e and AP3965i/e-ROW. |
| wns0015078 Added country support for Hong Kong to the AP3965i/e-ROW. |

| |
|--|
| wns0015084 Added country support for Morocco to the AP3825i |
| wns0015094 Added country support for United Arab Emirates to the AP3935i/e-ROW. |
| wns0015076 Added country support for Pakistan for the AP3935i/e and AP3965i/e-ROW. |
| wns0015083 Added country support for Saudi Arabia to the AP3805i-ROW |

| Changes in 10.11.01.0210 | |
|---------------------------------|--|
| wns0014954 | AP3900 Series need to be configured as part of a Radar “In-service” scanning group in order for location information to be consistently reported. Otherwise, there could be periodic interruptions in location reporting |
| wns0013712 | Addressed possible exposure to OpenSSH keyboard-interactive authentication (CVE-2015-5600) |
| wns0014390 | Improved memory allocation management for AP3705 to better handle high utilization loads. |
| wns0014899 | Fixed timer for Inter-AP Protocol to reduce the number of multicast transmissions for Auto Channel Selection exchanges |
| wns0014333 | Addressed possible issue with radio operational mode after removal of WLAN services. When administrator adds or removes wlangs services from the radio, clients associated to other wlangs on the same radio may experience temporary service interruption. Clients on the radio are disassociated and will re-associate soon after service is restarted. |
| wns0014488 | For AP3705i, booting up is delayed until flash clean-up is finished (up to 5 minutes). Improved resilience on recovery from hard-power reset/interruption |
| wns0014431 | Fixed password generator tool for the add guest user dialog |
| 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 |
| wns0014080 | Corrected issue with handling of Multicast definitions for Access Points configured in Site Mode |
| wns0013918 | Ensure consistency of user-name reporting in radius accounting-request packets |
| wns0013916 | Addressed Acknowledgment to NAC on policy change authentication after a Captive Portal authentication |
| wns0013997, wns0014278 | Addressed Potential Vulnerability of APs to CVE-2015-4000, CVE-2015-3197, CVE-2015-0204, CVE-2016-0800 |
| wns0014009 | Improved key management protection to address possible key corruption for 802.1x authentication |
| wns0014729 | Addressed Radius client recovery after target Server IP configuration changes |
| wns0014298 | Corrected handling of deny default action on B@AP for AP39xx series devices |
| wns0014415 | Fixed channel plan pop-up when adjusting large number of APs in multi-edit |
| wns0014426 | Addressed memory management issues when configuring MU blacklists |
| wns0014565 | Addressed issue with possible corruption of Radius IP address configuration via SNMP |
| wns0014085 | Corrected IPv6 address parsing for the management interface when added via the CLI |
| wns0015240 | Adjusted validation logic for derived key maximum key length for 802.11r (Fast Transition) configuration. Misconfiguration could cause AP3800 series radio to not initialize correctly. |

| | |
|------------|--|
| wns0013505 | Fixed issue when controller didn't send Siemens-SSID RADIUS value for a fast-failover event |
| wns0014148 | Addressed Potential Vulnerability of APs to CVE-2015-7547 |
| wns0014251 | Updated AP3825i/e power settings for band 1 and 4 to comply with new FCC Part 15 UNII rule with DFS, introduced new AP-ID number (-1). This is required in order to keep shipping beyond June 2016. The new rules increased power in band 1 but reduced power in band 4. |

| Changes in 10.01.05.0008 | |
|---------------------------------|--|
| wns0013289 wns0014572 | Improved handling of broadcast packets for AP3900 series APs |
| wns0014085 | Added support of topology groups in the exception filters for internal captive portal |
| wns0014371 | Improved probe suppression logic to also block 802.11 AUTH requests |
| wns0014415 | Fixed channel plan pop-up when adjusting large number of APs in multi-edit |
| wns0014426 | Addressed memory management issues when configuring MU blacklists |
| wns0014431 | Fixed password generator tool for the add guest user dialog |
| wns0014570 | Resolved issue with APs in Guardian mode not reporting location data for 5.0 GHz radio. |
| wns0014777 | Fixed race condition when learning new addresses with ARP proxy enabled |
| wns0014633 | Enhanced Location logs to include X,Y coordinates for tracked devices |
| wns0014690 | Resolved issue with possible image upgrades failures to 10.01.04 build for AP3900 series APs |
| 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 |

| Enhancements in 10.01.05.0008 | |
|--------------------------------------|---|
| wns0013123 | Added country support for Russia to the AP3935i/e |
| wns0014654 | Added country support for Bosnia Herzegovina to AP3801i |
| wns0015077 | Added country support for Bosnia Herzegovina to AP3805i/e |
| wns0014656 | Added country support for Bosnia Herzegovina to AP3805i-ROW |
| wns0014657 | Added country support for Bosnia Herzegovina to AP3825i/e |
| wns0014658 | Added country support for Bosnia Herzegovina to AP3825i/e-1 |
| wns0014659 | Added country support for Bosnia Herzegovina to AP3865e |
| wns0014660 | Added country support for Bosnia Herzegovina to AP3935i/e |
| wns0014661 | Added country support for Bosnia Herzegovina to AP3965i/e |
| wns0014677 | Added country support for Peru to AP3965i/e |

| |
|---|
| wns0014679 Added channels 52-144 (DFS) for Colombia, Puerto Rico, and United States to AP3965i/e |
| wns0014806 Added country support for Hong Kong to the AP3805i-ROW |
| wns0014807 Added country support for Kuwait to the AP3805i-ROW |
| wns0014808 Added country support for Peru to the AP3805i-ROW |
| wns0014809 Added country support for Dominican Republic to the AP3805i-ROW |
| wns0014810 Added country support for Malaysia to the AP3805i-ROW |
| wns0014811 Added country support for Qatar to the AP3805i-ROW |
| wns0014812 Added country support for Singapore to the AP3805i-ROW |
| wns0014813 Added country support for China to the AP3805i-ROW |
| wns0014814 Added country support for Chile to the AP3935i/e and AP3965i/e |
| wns0014815 Added country support for Malaysia to the AP3935i/e and AP3965i/e |
| wns0014816 Added country support for Kuwait to the AP3965i/e |
| wns0014817 Added country support for Qatar to the AP3965i/e |
| wns0014818 Added country support for Ecuador to the AP3935i/e |
| wns0014765 Added country support for South Africa to the AP3935i/e |
| wns0014766 Added country support for South Africa to the AP3965e |
| 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 10.01.04.0011 | |
|---------------------------------|--|
| wns0013847 | Corrected logic for timer handling to address possible connectivity issues for APs operational for long-periods of time |
| wns0013916 | Addressed Acknowledgment to NAC on policy change authentication after a Captive Portal authentication |
| wns0013918 | Ensure consistency of user-name reporting in radius accounting-request packets |
| wns0014298 | Corrected handling of deny default action on B@AP for AP39xx series devices. |
| wns0014358 | Updated probe suppression algorithm to adhere to Qualcomm usage pattern, addressing possible resource exhaustion |
| wns0014371 | Improved probe suppression logic to also block 802.11 AUTH requests |
| wns0014389 | Addressed possible transmit lockup due to group rekeying operations |
| wns0014390 | Improved memory allocation management for AP3705 to better handle high utilization loads. |
| wns0014416 | Fixed channel plan pop-up when adjusting large number of APs in multi-edit |
| wns0014037 | Improved More-Data indication for Power Save mode. Improved WMM (QoS) logic to ensure that AMPDU is only enabled for clients that support the function. |
| wns0013997 | Addressed Potential Vulnerability of APs to CVE-2015-4000, CVE-2015-3197, CVE-2015-0204 |
| wns0014148 | Addressed Potential Vulnerability of APs to CVE-2015-7547 |

| Enhancements in 10.01.04.0011 | |
|---|---|
| wns0013106 | Add country support for Hong Kong to the AP3935i/e |
| wns0013124 | Add country support for Saudi Arabia to the AP3935i/e |
| wns0013126 | Add country support for Singapore to the AP3935i/e |
| wns0013129 | Add country support for Thailand to the AP3935i/e and AP3965i/e |
| wns0013542 Introduce support for AP3805 FCC & ROW models | |
| wns0013757 | Add country support for Indonesia to AP3801i, AP3805i/e and AP3825i/e |
| wns0014239 | Add country support for Peru for AP3935i and AP3935e |
| wns0014240 | Add country support for Taiwan for AP3965i and AP3965e |
| wns0014241 | Add country support for Singapore for AP3965i/e |
| wns0014242 | Add country support for Channels 116-128 on AP3935i/e in Taiwan |
| wns0014251 Add support for AP3825i-1 and AP3825e-1 models | |
| wns0014347 | Add support WS-AO-DX10055N antenna to AP3965e |
| wns0014448 | Add country support for China to AP3935i/e and AP3965i/e |
| wns0014449 | Add country support for Qatar to AP3935i/e |
| wns0014450 | Add country support for Kuwait to AP3935i/e |

| | |
|------------|---|
| wns0014451 | Add country support for Egypt to AP3935i/e and AP3965i/e |
| wns0014452 | Add country support for Jordan to AP3935i/e and AP3965i/e |
| wns0014453 | Add DFS Support (Channels 52-144) to AP3935i/e-FCC models |
| wns0014454 | Add country support for Philippines to AP3935i/e and AP3965i/e. |
| wns0014455 | Add country support for Indonesia to AP3935i/e and AP3965i/e |
| wns0014456 | Add country support for Saudi Arabia to AP3965i/e |
| wns0014457 | Add country support for Brunei to AP3805i and AP3865e. |
| wns0014458 | Add country support for Vietnam to AP3805i, AP3825i, and AP3825i-1. |
| wns0014459 | Add country support for Malaysia to AP3805i, AP3825e, AP3825e-1, and AP3865e. |
| wns0014460 | Add support for WS-AI-DX10055 antenna to AP3935e |

| Changes in 10.01.03.0007 | |
|---------------------------------|--|
| 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 |
| wns0014080 | Fixed site mode B@AP multicast filter configuration updates AP properly |
| 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 10.01.02.0038 | |
|---|--|
| Hardware | |
| Introduces support for the ExtremeWireless AP3965i/e, a fully featured outdoor 4x4:4 dual radio 802.11ac Wave 2 AP, providing up to 2.5 Gbps over-the-air performance, multi-user MIMO, built-in wired load balancing for high-density and mission critical deployments. | |
| Software | |
| Added support for wireless countermeasures to the AP39XX Series platforms. | |
| Added country support for the Philippines to the AP3825i/e under the ROW domain. | |
| Extended the AP3935/3965 functionality to support higher power request levels via LLDP. | |
| For AP3935 and AP3965, a manual overwrite configuration function through the Controller interface was provided to allow the administrator to overwrite the power mode, setting the AP explicit into full power mode (equivalent to 802.3at operation for full 4x4:4 operation). | |
| For AP3935 and AP3965, the per-radio user capacity was increased to at least 240 devices. | |

| Changes in 10.01.02.0038 | |
|---------------------------------|---|
| wns0011674 | Corrected a problem when the controller was no longer reachable via SMTPv3 if the user set a password with special characters. |
| wns0012997 | Restricted transmission of Ethernet pause frames on the AP3805i. |
| wns0012007 | Bypass filtering functions if no filter rules defined. |
| wns0013502 | Corrected Radius accounting state machine relevant start messages when the interval was set to 0. |
| wns0013505 | Corrected a problem whereby the controller didn't send Siemens-SSID RADIUS value for a fast-failover event. |
| wns0013712 | Addressed a possible exposure to the OpenSSH keyboard-interactive authentication vulnerability (CVE-2015-5600). |
| wns0013620 | Resolved iStat device not staying connected with WPA2-PSK authentication. |
| wns0013761 | Updated the AP3865e power settings to comply with the latest Industry Canada (IC) Regulations. Removed band 1 for all antennas with the exception of the WS-ANT-5DIPN; changed band 1 channels 36-48 power to meet 50mW limit and indoor Only for WS-ANT-5DIPN. |

| Enhancements in 10.01.01.0129 |
|--|
| Hardware |
| Introduces support for the ExtremeWireless AP3935i/e, a fully featured 4x4:4 dual radio 802.11ac Wave2 AP, providing up to 2.5 Gbps over-the-air performance, multi-user MIMO, built-in wired load balancing and transparent PoE failover for high-density and mission critical deployments. |
| Adds support for new quad and eight-feed MIMO antennas to optimize the RF advantages of 4x4:4 in high-density deployments. |
| Software |
| Enhanced the discovery mechanism of the management plane on the AP39XX Series enabling secure discovery over SSL of the management service through the public cloud. The on-premise discovery mechanism and secured control channel for on-premise controllers remains unchanged from previous releases. |
| Added support for Hotspot 2.0 functionality, enabling transparent mobility between cellular data networks and hotspot Wi-Fi networks. New services include support for 802.11u, enabling pre-authentication network selection. |
| Enhancements doubles the maximum user/device capacity of the C5210 wireless appliance from 8,000 to 16,000 users/devices per appliance and a total of 32,000 users in high-availability mode. |
| Increased the map size for location tracking and added enhancements to track and report location of un-associated devices. |
| Licensing modifications to support moving regulatory enforcement to the AP39xx Series APs, enabling flexibility for global deployments by eliminating controller regulatory restrictions; a single wireless appliance installation can support both FCC and ROW deployments. |
| Provide administrative control over guest password generation algorithm so as to generate simpler and more localized passwords for Guest Login. |
| Include Area/Location information elements in 802.1x requests when Area Notification for MBA enabled (wns0012660) |

| Enhancements in 10.01.01.0129 |
|--|
| Resolved limitation on V2110-Small to provide N-Packet mirroring for Application Visibility integration. N-Packet Mirroring supported on all capacity variants of V2110 (wns0012749) |
| Validated support for V2110 installations on VMWare ESXi 6.0. |
| Enhanced Batch Location reporting interface to support definition of header authentication credentials. |
| Introduced administrative method for configuring the level of security protocol used in inter-controller and controller / NetSight communications. |
| Enhanced export of AP inventory report to include the BSSID information for configured services per AP. |
| Added support to automatically bind the inter-controller communications channel to user installed (CA signed) certificate. |
| Extended information elements of Location Batch Report to include Area, AP SN and Authentication state identifiers. |
| Enforce definition of AP password on controller install through CLI and GUI install wizards. |
| Static routing entries can now refer to next hops reachable through B@AC (L3) topologies. |
| Added option to customize format of CallingStation-ID field in 802.1x requests by allowing binding to format definition of Mac-Based-Authntication (MBA) |
| Introducing the new ExtremeWireless™ branding. |

KNOWN RESTRICTIONS AND LIMITATIONS:

| Known Restriction or Limitation | I.D. |
|---|-------------------|
| <p>The following cipher-suites have been obsoleted in release 10.01 as compared with the 9.21 release:</p> <p>DES-CBC3-MD5 RC2-CBC-MD5 DES-CBC-MD5 EXP-EDH-RSA-DES-CBC-SHA EXP-EDH-DSS-DES-CBC-SHA EXP-DES-CBC-SHA EXP-RC2-CBC-MD5 EXP-RC4-MD5</p> <p>If any of the above cipher-suites was being used to configure the "message-bus-ciphers" under the CLI "secureconnection" context in a 9.21 EWC release, then after upgrading the EWC to the 10.01 release, then the "message-bus-ciphers" is automatically set to "none" which maps to the default "RC4-MD5" cipher-suite setting.</p> | wns0013172 - Info |
| <p>Rule Based Redirection (RBR) provides users better visibility and control on how and when Captive Portal redirection works. Administrators can now explicitly define where in the Role the redirection will take place. However, if opting to use this function, be aware that the rule order for the REDIRECT action is critical to the proper functionality. The REDIRECT action rules for ports 80, 8080 and 443 must be added below the rules that define allowed access to the intended External Captive Portal server and any other allowed (Walled Garden) destinations. The rule must also be positioned above the 'Deny All' Default action.</p> | wns0014608 - Info |
| <p>The Deep Packet Inspection mechanism employed for Layer 7/Application rule enforcement requires several frames of a flow in order to make a decisive fingerprint. This operation is therefore incompatible with Rule Based Redirection (RBR) [aka, REDIRECT action], as that function triggers directly off the first frame (SYN) in the flow. Therefore, Layer 7/Application rules cannot be combined in the same role with redirection operations, whether implicit redirection (traditional redirection triggered from DENY traffic) or explicit REDIRECT rule action. When defining a role to be used in support of HTTP/HTTPS redirection, the role can only contain Layer 2-4 rule sets.</p> | wns0014726 - Info |
| <p>For Policy/Roles mapped to centralized topologies, references to layer 7 application group 'Streaming' (Allow or Deny actions) cause mobile YouTube Applications to not show content. Issue not observed with YouTube access via browser. Issue is being investigated and will be addressed in a future release</p> | wns0014846 - Info |
| <p>When configured to 100% Airtime, the Flexible Client Access (FCA) [aka, Airtime Fairness] feature is limited to 50 simultaneously transmitting clients per radio on aP3900 series models.</p> | wns0015037 - Info |
| <p>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.</p> | |
| <p>For deployments with AP39xx, ARP Proxy function for Bridged@AP topologies must be disabled, otherwise it can trigger instability. Fix is under investigation.</p> | wns0014780 – Info |

| | |
|--|-------------------|
| <p>When changing SNMPv3 user credentials, or deleting a user and adding a new one with the same name and credentials, a controller reboot is required, or restart the SNMP Trap Agent process in the CLI using the “restart snmp trap agent” command.</p> <p>When switching between SNMPv3 and SNMPv1/2, a controller reboot is required, along with rediscovery of the controller on the SNMP tool.</p> | wns0013972 – Info |
| <p>When upgrading from V9.21 (or earlier) to V10.01.02, SNMP tools (such as NetSight MIB Tools) will need to rediscover the controller with an updated Engine ID (even if using the same SNMP user & credentials) as the prefix used in the Engine ID has been changed from Siemens to Extreme Networks.</p> | wns0013973 – Info |
| <p>A limitation was found for clients that will not connect in ac-strict radio mode. The list includes Nexus 9, Galaxy S4, iPad Air, Intel7260.</p> | wns0013397– Info |
| <p>Due to changes to the SNMP agent in V10.01.02, “counter64” type OIDs are no longer supported. To support this type OID, use SNMP V2c or V3.</p> | wns0013536– Info |
| <p>Some versions of Apple Mac Books might exhibit low throughput performance when Management Frame Protection (PMF) is enabled.</p> | wns0012889– Info |
| <p>In order to capture NULL and QOS_NULL packets with WireShark, do not set a Capture Filter and disable "Do not capture own RPCAP traffic" under Remote Settings. In WireShark v1.12.3, select Capture --> Option --> Double Click Interface Row --> Remote Settings.</p> | wns0012862– Info |
| <p>The Access Point Name field can be up to 23 characters and must start with alpha characters, not numeric.</p> | wns0012722 – Info |
| <p>When enabling Sites Mode, the Controller’s topology capacity is capped at 128 topologies. Currently, APs are unable to process more than 128 topologies. In site configuration, all topologies get pushed to all APs, which effectively limits the maximum per-controller topologies to 128.</p> | wns0012793 – Info |
| <p>Countermeasures for honeypot AP threat may be less effective for the iPhone (with version 8.3) client device than other device types</p> | wns0012678 – Info |
| <p>We recommend that you do not enable 802.11k along with the Quiet IE option for installations with Ascom i62 phones.</p> | wns0012567– Info |
| <p>Rogue AP Detection applies only ‘Open’ hotspots. Countermeasures can be enforced against other link-protected hotspots if designated as a threat.</p> | wns0012296– Info |
| <p>Instability issues observed on the network with Intel AC-7260 based clients. Workaround: Update the Intel AC-7260 driver and disable the Throughput Boost setting in the client driver Advanced options. This issue is not present if the client driver is running 18.20.0.9 or above.</p> | wns0011519 – Info |
| <p>AP38XX supports TKIP with the following restrictions due to new Wi-Fi Alliance certification requirements: Only available for Legacy rates; not supported with 11n nor 11ac rates 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.</p> | wns0011589 – Info |
| <p>RADIUS attribute-value pair limits the location data size to 251 characters. When the location data size is more than 251 characters, the data is sent to the RADIUS server truncated to 251 characters.</p> | wns0011467– Info |

| | |
|--|--------------------------|
| <p>The Location Batch Report file contains two timestamp attributes that are currently in local time. However, the time zone indicator is missing. These fields should be reported as UTC time with the time zone is set to 'Z'.</p> | <p>wns0011008– Info</p> |
| <p>The Chrome auto-complete function fills in fields incorrectly. Disable password saving and password field auto completion in a Chrome configuration.</p> | <p>wns0010642– Info</p> |
| <p>APs advertising the SSIDs of administratively disabled WLAN Services are not detected as internal honeypots until the WLAN Service is enabled.</p> | <p>wns0008740 – Info</p> |
| <p>For "g/n" mode operation of the AP with wireless clients based on Intel 6300N chipset with driver 15.x/14.3.x, we recommended disabling the "11g protection" setting. Set AP/Radio2/Advanced --> 11g Settings / Protection mode --> None.</p> | <p>wns0008979 - Info</p> |
| <p>When the AP is used in a WDS or Mesh service, the AP name must be under 32 characters.</p> | <p>wns0008035 - Info</p> |
| <p>On C5210, status on interface without physical transceivers plugged reported Up and Down.</p> | <p>wns0008023 - Info</p> |
| <p>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 an incorrect topology assignment. We recommend that you do not configure Topology groups if Site deployments are in use.</p> | |
| <p>Info MacBook Air running SW prior to 10.8.4 can experience random disconnections (mostly noticeable during video streaming). The issue is caused by a bug in the Apple WiFi driver, and it is corrected in SW 10.8.4.</p> | |
| <p>Info Intel AC7260 with latest drivers 18.32 or 18.33 may become un-responsive when client roams outside of Wi-Fi Coverage area. 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. Recommend customers standardize on version 18.21, which does not show the same problem. Issue is being escalated with Intel™ .</p> | |
| <p>How to use Real Capture Tool</p> <ul style="list-style-type: none"> • 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. • You have the option 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 does not report its own Beacons, Retransmission, Ack, and 11n Block Ack. If this information is needed, then perform the real capture from a close-by second AP. Change the second AP's wireless channel to match the AP that is being troubleshoot. Let the second AP broadcast an SSID to activate the radios, but do not broadcast the same SSID you are troubleshooting, so that you can prevent the clients from connecting to your second capturing AP <p>Note: For AP3935/AP3965 some frames generated by the AP's radio, such as Beacons, ACK, RTS/CTS are not captured.</p> | |

SUPPORTED WEB BROWSERS

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

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

The Wireless Clients (Captive Portal, AAA):

| Browsers | Version | OS |
|------------|--------------------------|---------------------|
| Chrome | 46.0.2490.71 dev-m | Windows server 2012 |
| Chrome | 47.0.2526.80 m | Windows 7 |
| Chrome | 38.0.2125.111m | Windows server 2012 |
| Firefox | 41.0.1 | Windows server 2012 |
| Firefox | 38.0.5 | Windows XP |
| IE 11 | 11.0.9600.18059 | Windows 7 |
| IE 9 | 9.0.8112.16421 | Windows 7 |
| IE 8 | 8.0.6001.18702 | Windows XP |
| Opera beta | 34.0.2036.24 | Windows 7 |
| Safari | preinstalled with iOS9.1 | iOS9.1 |

PORT LIST

The following list of ports may need to remain open so that the controllers/APs will function properly on a network that includes protection equipment like a firewall.

ExtremeWireless TCP/UDP Port Assignment Reference

| Comp. Source | Comp. Dest | Protocol (TCP/UDP) | Src Port | Dest Port | Service | Remark | Open Firewall Req'd |
|--|--------------|--------------------|----------|-----------|---------------|--|---------------------|
| Ports for AP/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 |

| Comp. Source | Comp. Dest | Protocol (TCP/UDP) | Src Port | Dest Port | Service | Remark | Open Firewall Req'd |
|---|---------------|--------------------|----------|------------|-----------|--|---------------------|
| 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 |
| 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 |

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.

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.

| Comp. Source | Comp. Dest | Protocol (TCP/UDP) | Src Port | Dest Port | Service | Remark | Open Firewall Req'd |
|--|------------------|--------------------|----------|-----------|---|---|---------------------|
| 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) | Stanley Healthcare/ 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 |

EXTREME NETWORKS PRIVATE ENTERPRISE MIB SUPPORT

Extreme 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.

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 |
| 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 V10.01 software release:

Windows 10

| Device | Model | Driver | Radio |
|-----------------|-----------------|---------------|------------|
| Intel | AC-7260 | 18.21.0.2 | a/b/g/n/ac |
| Microsoft Lumia | 950 xl dual sim | 10.0.10586.11 | a/b/g/n/ac |

11ac MU-MIMO

| Device | Model | Driver | 1x Support | Radio | 11ac Strict | MU-MIMO |
|----------------|--------------------------|------------|------------|------------|-------------|-------------|
| Dell Alienware | Killer Wireless Qualcomm | 12.0.0.102 | yes | a/b/g/n/ac | N/A | 2x2 Mu-MIMO |
| Acer E4 | QCA9377 Qualcomm | 12.0.0.116 | yes | a/b/g/n/ac | N/A | 2x2 Mu-MIMO |

Due to limited availability of the real clients, most of the feature testing was done with IxVeriWave tool.

| Device | Model | OS | 1x Support | Radio | 11ac Strict | MU-MIMO |
|--------------|----------|-------------|------------|------------|-------------|-------------|
| Google Nexus | Nexus 5x | Android 6.0 | yes | a/b/g/n/ac | yes | 2x2 Mu-MIMO |

The following clients passed the 11ac strict mode test.

| Client | Driver Version | Test Case | Build | Result |
|---------------------------------|--|------------------|-------|--------|
| AC 1200 D-Link | 1027.4.630.2015 | 11ac Strict mode | | Pass |
| Broadcom 802.11 ac | 6.30.223.102 | 11ac Strict mode | | Pass |
| AirPort Extreme (0x14E4, 0x117) | Broadcom BCM43xx 1.0 (6.30.223.74.22) | 11ac Strict mode | | Pass |
| Cisco AE6000 | AE6000_v5.0.7.0_Driver_Win7 | 11ac Strict mode | | Pass |
| iPhone 6 - iOS 9.1 | Modem firmware 2.23.03 | 11ac Strict mode | | Pass |
| ASUS PCE-68ac | 6.30.223.75 | 11ac Strict mode | | Pass |
| MacBook Air | Broadcom BCM43xx 1.0 (6.30.223.154.65) | 11ac Strict mode | | Pass |
| iPhone 6 - iOS 9.1 | Modem firmware 4.32.00 | 11ac Strict mode | | Pass |
| Nexus 5X | Kernel Version 3.10.73-g60cf314 | 11ac Strict mode | | Pass |

Other 11ac and 11n devices:

| Device | Model | OS | Radio |
|---------------------|-----------------------|----------------------------|--------------------------|
| Apple | A1396 | iPad OS | 11abgn |
| Apple | iPad | IOS 7.1.2 | |
| Apple | iPad (4th generation) | iOS9.1 | a/b/g/n |
| Apple | iPad 3 | iOS 8.4.1 | a/b/g/n |
| Apple | iPad Air 2 | IOS9.1 | a/b/g/n |
| Apple | iPad Mini | iOS 8.4.1 | |
| Apple | iPhone 5 | iOS 9.1 | a/b/g/n/ |
| Apple | iPhone 5 | iOS | 11abgn |
| Apple | iPhone 5 S | IOS 6.1.4 | a/b/g/n |
| Apple | iPhone 6 | iOS 9.1 | a/b/g/n/ac |
| Apple | iPhone 6 GSM | iOS8.4.1 | a/b/g/n/ac |
| Ascom | 902202 | | |
| Asus | 2 in 1 | Windows 8.1 | abgn |
| Blackberry | Bold 9000 Smartphone | Blackberry OS 4.6.0.282 | |
| Chromebook | 503C32-K01 | Chrome OS | 11abgn |
| Chromebook | Asus C200 | Chrome 46.0.2490.82 | abgn |
| Galaxy S4 | Galaxy S4 | Android | |
| Google Nexus | Nexus 5x | Android 6.0 | a/b/g/n/ac |
| Laptop PC | Intel AC-7260 | Win10 (all builds) | 11 abgnac |
| Nexus 9 | Nexus 9 | Android | a/b/g/n/ac |
| Nokia 830 | | Win8.1 | 802.11abgnac |
| Polycom Spectralink | 8440 | | |
| Samsung | Galaxy Note4 | Android v5.0.1 | a/b/g/n/ac |
| Surface 3 Pro | | Win 8.1 / Win 10 | Marvel Avastar 802.11 ac |

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 |

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 |
| Extreme | G3 | 01.00.02.0001 | For PoE |
| | G3 | 06.11.01.0040 | |
| | C20N1 | Version 12.1(19)EA1c | No PoE |
| | B3G124-48P | 06.61.03.0004 | for AP 802.1x, PoE |
| | B3 | 01.02.01.0004 | 10480068225P |
| | C5 | 06.42.06.0008 | 11511205225K |
| | B3G124-48P | 06.61.03.0004 | for AP 802.1x, POE |
| | 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 |
| | X-460-G2 | | 802.3at interoperability with AP3935 |
| 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: +1 877-801-7082 (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.
145 Rio Robles
San Jose, CA 95134

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

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries. All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners. Extreme Networks IPS includes software whose copyright is licensed from MySQL AB.

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