

Customer Release Notes

ExtremeWireless™ Convergence Software

Software Version 10.51.11.0002

February 21, 2020

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:
<https://extremeportal.force.com/>**

FIRMWARE SPECIFICATION:

| Status | Version No. | Type | Release Date |
|------------------|---------------|-----------------------|--------------------|
| Current Version | 10.51.11.0002 | Maintenance Release | February 21, 2020 |
| Previous Version | 10.51.10.0006 | Maintenance Release | December 6, 2019 |
| Previous Version | 10.51.09.0008 | Maintenance Release | October 25, 2019 |
| Previous Version | 10.51.08.0004 | Maintenance Release | September 20, 2019 |
| Previous Version | 10.51.07.0006 | Maintenance Release | August 19, 2019 |
| Previous Version | 10.51.06.0003 | Maintenance Release | July 19, 2019 |
| Previous Version | 10.51.05.0005 | Maintenance Release | June 14, 2019 |
| Previous Version | 10.51.04.0009 | Maintenance Release | May 23, 2019 |
| Previous Version | 10.51.03.0002 | Maintenance Release | April 24, 2019 |
| Previous Version | 10.51.02.0006 | Maintenance Release | April 17, 2019 |
| Do not use | 10.51.01.0100 | Patch Release | March 20, 2019 |
| Do not use | 10.51.01.0097 | Minor Feature Release | March 1, 2019 |
| Previous Version | 10.41.13.0008 | Maintenance Release | January 25, 2019 |
| Previous Version | 10.41.12.0006 | Maintenance Release | December 6, 2018 |
| Previous Version | 10.41.11.0009 | Maintenance Release | November 9, 2018 |

| Status | Version No. | Type | Release Date |
|------------------|---------------|-----------------------|--------------------|
| Previous Version | 10.41.10.0014 | Maintenance Release | September 13, 2018 |
| Previous Version | 10.41.09.0008 | Maintenance Release | August 2, 2018 |
| Previous Version | 10.41.08.0012 | Maintenance Release | June 22, 2018 |
| Previous Version | 10.41.07.0014 | Maintenance Release | May 11, 2018 |
| Previous Version | 10.41.06.0013 | Maintenance Release | April 9, 2018 |
| Previous Version | 10.41.05.0010 | Maintenance Release | March 9, 2018 |
| Previous Version | 10.41.04.0002 | Maintenance Release | February 13, 2018 |
| Previous Version | 10.41.03.0012 | Maintenance Release | February 2, 2018 |
| Previous Version | 10.41.02.0014 | Maintenance Release | November 24, 2017 |
| Previous Version | 10.41.01.0082 | Patch release | November 3, 2017 |
| Previous Version | 10.41.01.0080 | Minor Feature Release | September 29, 2017 |
| Previous Version | 10.31.06.0007 | Maintenance Release | October 5, 2017 |
| Previous Version | 10.31.05.0003 | Maintenance Release | August 18, 2017 |
| Previous Version | 10.31.04.0009 | Maintenance Release | July 21, 2017 |
| Previous Version | 10.31.03.0012 | Maintenance Release | June 9, 2017 |
| Previous Version | 10.31.02.0007 | Maintenance Release | May 5, 2017 |
| Previous Version | 10.31.01.0048 | Minor Feature Release | March 29, 2017 |
| Previous Version | 10.21.03.0010 | Maintenance Release | March 6, 2017 |
| Previous Version | 10.21.02.0017 | Maintenance Release | January 27, 2017 |
| Previous Version | 10.21.01.0065 | Minor Feature Release | December 7, 2016 |
| Previous Version | 10.11.05.0005 | Maintenance Release | December 2, 2016 |
| Previous Version | 10.11.04.0008 | Maintenance Release | October 28, 2016 |
| Previous Version | 10.11.03.0004 | Maintenance Release | September 19, 2016 |
| Previous Version | 10.11.02.0032 | Maintenance Release | August 15, 2016 |
| Previous 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 |

| Status | Version No. | Type | Release Date |
|------------------|---------------|-----------------------|-------------------|
| 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 C5215 | AV-MV-10.51.11.0002.ice | |
| ExtremeWireless Controller C5210 | AV-MV-10.51.11.0002.rue | |
| ExtremeWireless Controller C35 | AV-MV-10.51.11.0002.cwe | |
| ExtremeWireless Virtual Appliance V2110 VMware | AV-MV-10.51.11.0002.bge | |
| ExtremeWireless Virtual Appliance V2110 MS Hyper-V | AV-MV-10.51.11.0002.ize | |
| Wireless AP3917i-FCC Wireless AP3917i-ROW Wireless AP3917e-FCC Wireless AP3917e-ROW Wireless AP3917k-FCC Wireless AP3917k-ROW | AP391x-10.51.11.0002.img | |
| Wireless AP3916ic-FCC Wireless AP3916ic-ROW | | |
| Wireless AP3915i-FCC Wireless AP3915i-ROW Wireless AP3915e-FCC Wireless AP3915e-ROW | | |
| Wireless AP3912i-FCC Wireless AP3912i-ROW | | |
| AP3916-camera | | AP3916IC-V1-0-14-1.dlf |
| Wireless AP3935i-FCC Wireless AP3935e-FCC Wireless AP3935i-ROW Wireless AP3935e-ROW | AP3935-10.51.11.0002 .img | |
| Wireless AP3965i-FCC Wireless AP3965e-FCC Wireless AP3965i-ROW Wireless AP3965e-ROW | | |
| Wireless AP3801i | | AP3801-10.51.11.0002 .img |

| | |
|--|----------------------------|
| Wireless AP3805i Wireless AP3805e Wireless AP3805i-FCC Wireless AP3805i-ROW | AP3805-10.51.11.0002 .img |
| Wireless AP3825i Wireless AP3825e | AP3825-10.51.11.0002 .img |
| Wireless AP3865e | |
| End of SW Support since Dec 31, 2018 | |
| Wireless AP3705i | AP3705-10.41.12.0006 .img |
| Wireless AP3710i Wireless AP3710e | AP3710-10.41.12.0006 .img |
| Wireless AP3715i Wireless AP3715e | AP3715-10.41.12.0006 .img |
| Wireless AP3765i Wireless AP3765e | W78XC-2-10.41.12.0006 .img |
| Wireless AP3767e | |
| Scalance W788C | |
| Scalance W786C | |

INSTALLATION INFORMATION

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

Installation Notes

- The minimum system software version is 09.21.18 to upgrade to this software version.
- After upgrading to V10.51.01 or V10.41.02 from a release earlier than V10.11.02, users with IPv4 networks will see the following changes to their IPv4/IPv6 traffic:
 - a) Users with Bridged at AP deployment: Before upgrade, Bridged at AP allowed all unicast IPv6 and multicast IPv6 traffic on the network (unless the user had an explicit rule to stop the unicast IPv6). After upgrading to V10.51.01 or V10.41.01/10.41.02, ALL unicast IPv6 traffic will continue to be allowed, but multicast IPV6 traffic will be denied – Except multicast IPv6 Router Solicitation (RS), Neighbor Solicitation (NS), and Neighbor Advertisement (NA) will be allowed.
 If the user wants to have the identical behavior as pre-V10.41.01, i.e. allow multicast IPV6 traffic, the user can add a multicast IPv6 “allow all” rule to the multicast rules.
 - b) Users with Bridged at Controller deployment: Before upgrade, Bridged at Controller denied all IPv6 traffic (unicast and multicast). After upgrading to V10.51.01 or V10.41.01/10.41.02, ALL IPv6 unicast traffic and multicast RS/NS/NA traffic will be allowed. All other multicast traffic will be denied.

If the user wants to have almost identical behavior as pre-V10.41.01, the user can add a unicast IPv6 “deny all” rule. There is no mechanism/rule to stop multicast RS/NS/NA traffic.

- 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 this case, the "Multicast to Unicast Delivery" option should be disabled.
- The V2110 is supported on ESXi version 5.5, 6.0, 6.5, and 6.7. 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 Added 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, 6.0 and 6.5. 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.
- If configuring a service that will incur topology changes after the 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.
- 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. To allow specific multicast, broadcast, and subnet broadcast traffic with the deny-all catch-all filter rule for global default policy, explicitly add specific multicast, broadcast and subnet broadcast rules one by one to allow that traffic.
- \, ', " characters are not supported in WLAN/VNS fields.
- When upgrading 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.
- **Note: End of Software Support**



- AP3710, AP3765, AP3767 reached End of SW Support on July 31, 2018 (under both 9.21 and 10.xx)
- AP3705 and AP 3715 reached End of SW Support on Dec 31, 2018 (under both 9.21 and 10.xx)
- C25, C4110-1, C4110-2, C5110-1, and C5110-2 reached on Dec 31, 2018 (under both 9.21 and 10.xx). No features or bug fixes (controller related) will be considered.

- **Note: End of Software Support**

Since the End of SW support dates have passed for AP37xx in December 2018, there will be no further features or bug fixes for the AP37xx platform. However, the AP37xx will continue to register to the V10.41 Controller. As a result, the following will be the last supported images for AP37xx:

- AP3705-10.41.12.0006.img
- AP3710-10.41.12.0006.img
- AP3715-10.41.12.0006.img
- W78XC-2-10.41.12.0006.img

Again, these AP37xx will be accepted on discovery (controller in 10.51.01 or 10.41.xx) and will work as is. No features or bug fixes will be considered.



Upgrading Virtual Appliance V2110 VMware to the Current Release

It is MANDATORY that before upgrading to v10.11.xx, 10.21.xx, 10.31.xx, 10.41.01 and 10.51.01 the “SCSI controller” setting for the VMware virtual controller (V2110) is set to “Paravirtual”

You only need to install the “.ova” file when you first install the V2110 VMware. The latest .ova file is V2110-10.41.02.0014.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 Maintenance Guide”.

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

For any v10.xx - V2110 deployments on Hyper-V with Intel/AMD CPUs, the CPUs must support the SSSE3 instruction set. Failure to meet this requirement will result in the V2110 not fully booting up and operate correctly.

You need to install the “.zip” file when you first install the V2110 Hyper-V. The latest .zip file is V2110_Hyper-V_Edition-10.41.02.0014.zip. All subsequent upgrades can be performed using the standard controller upgrade procedure to apply a “.ize” file to the V2110 Hyper-V.

V10.41.01 has been validated with Microsoft Hyper-V Server 2012 R2 and Microsoft Hyper-V Server 2016 Standard editions.

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 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 the data required for high availability between controllers. 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 an 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. Enter 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 on the devices at each end of the connection, ensuring that the two controllers, or controller and NetSight Wireless Manager, are able to communicate. Without the same shared secret on each end of the connection, features like availability will fail.

Note that changes to secure connection share secret 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™ | 8.1 or higher |
| ExtremeManagement™ Wireless Advanced Services | 4.4 |
| ExtremeControl™ | 8.1 or higher |

Note:

Configuration of the AP3935/AP3965/AP3912/ AP3915/AP3916/AP3917 is not yet supported via ExtremeManagement™ WirelessManager.

IMPORTANT: EXTREMEWIRELESS V10 LICENSING CHANGES

Consolidated the regulatory domains to FCC, ROW, EGY (Egypt), and Base (for no domain specified). The FCC domain is limited to the US (and US territories), Puerto Rico, and Colombia. All other countries, except Egypt, 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 models such as the AP3805_FCC/ROW and the AP39xx models that enforce regulatory requirements at the AP (independent of controller regulatory domain). For installation in Egypt the EGY activation key must be used. When activated EGY key will not allow management of APs for any other country.

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 V10 activation key.

To request a new V10 license key:

1. Log into your Extreme Networks Extranet account (<https://extremeportal.force.com/>).
2. Select the Product Licensing link (<https://extremeportal.force.com/ExtrLicenseLanding>).
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.

BEFORE USING THE FABRIC ATTACH FEATURE

V10.41.01.0080 (or above) is the minimum required firmware revision for Fabric Attach functionality. Out-of-Factory new APs will likely run older revisions that are not FA capable. (Except for the AP3915 family and the AP3917 family):

- For automatic provisioning of new equipment, the admin VLAN on the switch port should be set to untagged. The admin VLAN must provide (switch or routed) support for controller discoverability and connection. Controller may then upgrade the AP to the latest release.
- If the admin VLAN on the switch is tagged, then the new AP must first be pre-staged to force an upgrade to a compatible firmware release.

For AP3915 (hardware revisions before 'AB' for AP3915i and 'AC' for AP3915e), when deploying into an ERSxxx based Fabric Attach deployment, the new AP must first be pre-staged with a switch port that has Fabric to allow it to be upgraded to V10.41.01 GA (Build 80) or later.

After upgrade to a release of at least 10.41.01 GA (Build 80) the AP will then be able to fully participate in Fabric Attach function.

Note: The Fabric Attach Feature is only supported on AP3900 series APs (AP3912 / AP3915 / AP3916 / AP3917 / AP3935 / AP3965).

Note: The manufacturing revision of an access point is reflected in the last 2 digits of the "Shipping" ID printed in the unit's gift-box label.

Disable the Fabric Attach functionality in Extreme ERS switches if Fabric is not actually provisioned.

- Extreme ERS family switches ship from the factory with Fabric Attach enabled. Even if the switch is not actually provisioned into an Extreme Fabric Connect, it will advertise the availability of Fabric Attached to connecting devices.



- One of the elements of the advertisement is the attribute of Management VLAN (VLAN ID 1 by default). That announcement however is processed by ExtremeWireless™ APs and will cause the AP to configure itself to use that VLAN ID for its management function. That VLAN ID (1) is typically not the actual VLAN the AP should be using to access its management network and the corresponding managing controller. Therefore, it will lead to the AP losing network connectivity.
- Workaround:
 1. If you have an ERS series switch that is not actually deployed into a Fabric Attach network, disable the switch's FA function.
 - Syntax: *no fa port-enable <port #s>*
 2. Recover the AP by resetting to the factory default. (Typically push and hold the reset pin.) Refer to the corresponding AP model's Installation guide for details on the reset procedure.
 - The AP will recover by using the default untagged access or a more specific VLAN, if provisioned by the ExtremeWireless™ appliance.

NEW FEATURES, SOFTWARE CHANGES, AND ENHANCEMENTS

This Maintenance release includes all previous 10.51.xx.xxxx features and changes



| Changes in 10.51.11.0002 | |
|--------------------------|--|
| wns0022883 | Improved session management in high capacity environments. |
| wns0022890 | Improved handling of data frames when Secure Tunnel for Control is configured. |

| Enhancements in 10.51.11.0002 | |
|-------------------------------|--|
| wns0022839 | Added country support of AP3915i-ROW for Brunei. |

| Changes in 10.51.10.0006 | |
|--------------------------|--|
| wns0022140 | Handled race condition where RADIUS CoA-Request would not get acknowledged by the Controller while a client was roaming to a new AP. |
| wns0022571 | For APs that support RADAR WIPS, we added a new device ID for the AP that is associating as a client. It now displays as EXTR-RADAR-MU under All Client Reports. |
| wns0022835 | Improved AP Load Group->Client Balancing algorithm for AP39xx. |
| wns0022857 | Resolved compatibility issue that was found in the Python dependency on the Controller, which could cause instability. |
| wns0022860 | Improved AP logic to revert to the original DFS channel after reboot. |

| Enhancements in 10.51.10.0006 | |
|--------------------------------------|---|
| wns0022870 | Improved resiliency for AP39xx in environments with high noise floors. |
| wns0022789 | Enhanced AP Name in Beacon setting by including the AP Name in Vendor-Specific IE for Probe Responses, de-coupled the setting from LED Mode, and added the ability to configure AP Name in a Beacon per WLAN Service. |

| Changes in 10.51.09.0008 | |
|---------------------------------|--|
| wns0021351 | Added support for EAP Identity fields starting with 0x00 and Identity is over the maximum RADIUS username limit of 253 bytes |
| wns0022066 | Improved controller stability for Guest Splash in an availability pair by properly cleaning up client session tokens |
| wns0022559 | Improved stats accuracy for RADIUS Accounting packets in those instances where clients would disconnect/reconnect |
| wns0022838 | Enhanced channel recovery time after a DFS event on AP3825 with ATPC enabled |
| wns0022846 | Resolved IP address gateway conflict with AP's using subnet 1.1.0.0/16 and Controller also using 1.1.1.1 for FFECF |
| wns0022842 | Improved compatibility between Vocera badges and AP when FT is enabled |

| Enhancements in 10.51.09.0008 | |
|--------------------------------------|---|
| wns0022786 | Added Chinese Character Support for SSIDs |
| wns0022822 | Added V2110 (VMware) Jumbo Frame Support |
| wns0021062 | Changed default value for RADAR -> "Remove network access from violating clients (WIPS)" from 900s to 30s |

| Changes in 10.51.08.0004 | |
|---------------------------------|--|
| wns0022528 | Addressed TCP vulnerability CVE-2019-11477 for C35, C5210, C5215, V2110 and V2110H |

| Enhancements in 10.51.08.0004 | |
|--------------------------------------|---|
| wns0022788 | Modified factory default settings for AMSDUs, TxBF, PMF and 802.11e |

| Changes in 10.51.07.0006 | |
|---------------------------------|---|
| wns0020720 | Improved AP handling for clients with hostnames greater than 31 characters. |
| wns0020760 | Addressed handling of commas in Guest User description field where exporting the file and importing it back would generate an error. |
| wns0021161 | Addressed DNS not properly caching hostnames for FQDN related input fields after Controller upgrade. |
| wns0021916 | Improved MU inter-controller roaming between APs configured with an encrypted SSID whereby clients (WL3) were slow or unable to associate to a previously authenticated AP. |
| wns0022066 | Improved robustness of any WLAN Service using Authentication when # of simultaneous authenticating clients exceeds 4096. |
| wns0022508 | Improved handling of single quote(s) in SSID name when any action related to shutting down Radio/WLAN Service; such as channel-scan or In-Service auto channel-scan. |
| wns0022542 | Corrected issue with exporting of strings with special character 'Ö'. Character would be missing after upgrade. Corrected for upgrades from 10.51.07 onwards. |
| wns0022650 | Enhanced accuracy of RSSI readings sent from AP to ExtremeLocation server. |
| wns0022659 | Included "Radio Mode" in Active AP report when exporting to XML. |
| wns0022709 | Corrected issue with lack of exporting a Max Session Lifetime of zero (0 - forever) for Guest portal users, which results in the setting resetting to 30 minutes. From this build forward export/import and upgrade will work correctly. For upgrades from previous releases, please reset the value after the upgrade completes. |

| Changes in 10.51.06.0003 | |
|---------------------------------|---|
| wns0021532 | Improved U-APSD support with VoWLAN phones to properly manage Tx queues on AP38xx platform. |
| wns0022104 | Improved EAP-TLS re-authentication handling for AP38xx and AP39xx authenticating against wired switch-port. |
| wns0022527 | Addressed TCP vulnerability CVE-2019-11477 for AP38xx and AP39xx. |

| Enhancements in 10.51.05.0005 | |
|--------------------------------------|---|
| wns0022412 | Per Egypt Regulatory, removed 5GHz Band 4 channel support (channels 149, 153, 157, 161, 165) for AP3965i/e-ROW deployed outdoors. |

| Changes in 10.51.05.0005 | |
|---------------------------------|---|
| wns0022313 | Improved stability with 802.11h enabled and DFS events to properly scan for new channel after a radar event has occurred. |
| wns0022415 | Addressed WLANs (having special character "@" in the name) being removed from Sites Configuration during upgrade |

| Enhancements in 10.51.04.0009 | |
|--------------------------------------|---|
| wns0022323 | Support override of Called Station ID to MAC:SSID for RADIUS accounting, in compliance with RFC3580 |

| Changes in 10.51.04.0009 | |
|---------------------------------|--|
| wns0021459 | Addressed issue with management of ACL rules which could cause AP instability. |
| wns0021760 | Adjusted logic for managing nameservers (DNS) to better rely on DHCP information versus persisted settings. |
| wns0022036 | Improved filtering logic for wireless packet capture to focus on end-system traffic, removing internal state frames. |
| wns0022254 | Improved escaping of special characters in user-provided descriptive configuration fields, for configuration backups that could otherwise cause import and upgrade issues. |
| wns0022319 | Improved bounds checking protection for large hostnames in client statistics reporting. Maximum 32 character enforced. |
| wns0021218 | Enforced that AP391x generate IGMP JOIN when configured for SIAPP (Multicast) dependent functions such as Site and Load balancing |

| Changes in 10.51.03.0002 | |
|---------------------------------|--|
| wns0021949 | Corrected classification and parsing of IPv6 malformed packets (on the ethernet driver level) which could cause AP3915 to lock-up. |
| wns0022015 | Improved inter-communication between Controller appliances with Mobility enabled. |
| wns0022016 | Improved compatibility for FabricAttach between AP39xx and EXOS 30.2 for Element Types '4' and '5'. |

| Changes in 10.51.02.0006 (includes all 10.51.01.xxxx features and changes) | |
|---|--|
| wns0021243 | Improved co-existence for 2.4GHz radio between client connectivity with interference scans for both in-service and Guardian modes on AP38xx and AP39xx. |
| wns0021803 | Addressed activation date for user accounts in captive portal field behaving incorrectly when inputting minutes between 0-9. |
| wns0021882 | Corrected behavior when changing EWC data port configuration between tagged <-> untagged could result in packets being dropped. |
| wns0022038 | Addressed Potential Vulnerability of Controller in CVE-2018-15473. |
| wns0022136 | Updated Client Reports for 11ac clients which could appear incorrectly as 11n capable only. |
| wns0022144 | After a Controller firmware upgrade from 10.41.xx to 10.51.01, it was discovered upon AP39xx initial re-registration to the Controller there was potential of AP39xx configuration being reset (factory defaulted) which would cause loss of service requiring admin to reconfigure the AP settings. |

| Changes in 10.51.01.0100 | |
|---------------------------------|---|
| wns0021917 | Improved boundary check in PSK for configuring long strings that may have prevented AP radio to come online (fix added in build 0100 on top of others) |

New features in V10.51.01.0097

Mesh Client Enhancements

- Improves stability for AP39xx with Mesh Client, 11k and Location Engine enabled.
- Added multi-edit functionality for Mesh configurations.
- Enhanced Mesh statistics reports with search function.

Increased Topology/Role limits for C5215

- The maximum number of the topology and role limits has increased to 4000 on C5215 only.

Purge Sessions Upon Client Disconnect (Wireless or Wired)

- This feature cleans up the client session upon DeAuth/DeAssoc received from the wireless client or link down on wired client.

Return to Original Channel after DFS when clients <= "X"

- This feature allows user to configure the client threshold number before the AP will return to the original channel prior to the DFS event.

Configuration of timeout for Location Entries

- This feature allows Location Entry "Idle Timeout" to be configurable between 5-1440 minutes (defaulted to 30 min).

Overwrite of Calibration setting for IoT Beacons

- This feature allows configuration for calibration setting on iBeacon and Eddystone-url Beacon.

Policy MIB update for NSI/ISID indication

- Policy MIB update for NSI/ISID indication for Fabric Attach Mode topology.

Added MIB OID for Called-Station-Id-SSID

- Added MIB OID support for Called-Station-Id-SSID.

Display 802.1X usernames in-lieu of device name

- This feature displays the 802.11x user names in-lieu of device name for 802.1x authenticated clients.

Append SSID to MAC in Called-Station-Id

- Added support in the AP RADIUS Client Called-Station-Id format XX-XX-XX-XX-XX-XX:SSID according to RFC3580.

| Changes in 10.51.01.0097 | |
|---------------------------------|--|
| wns0021401 | Radio driver code is “stuck” when commanded to scan the channel. |

| Changes in 10.41.13.0008 | |
|---------------------------------|--|
| wns0021208 | Corrected "Invalid configuration request" being shown in AP logs during a controller upgrade while APs failover to secondary Controller. |
| wns0021242 | Improved handling of Bonjour multicast traffic mapped to contain to VLAN while in Sites Mode. |
| wns0021325 | Improved handling of ARP tables when dealing with large number of devices on network. |
| wns0021358 | Resolved co-existence when AP subnets are in the same range of 1.1.0.0/16 while FFECF is enabled. |

| Enhancements in 10.41.13.0008 | |
|--------------------------------------|---|
| wns0021030 | Added country support of AP3912i-ROW for Russia. |
| wns0021335 | Added country support of AP3915i-ROW for Ukraine. |

| Changes in 10.41.12.0006 | |
|---------------------------------|---|
| wns0014094 | Completed 10.41 interoperability testing with AP38xx and SpectraLink handsets. |
| wns0021014 | Resolved AP not returning to original channel after DFS timeout with 11h enabled. |
| wns0021039 | Improved Guardian mode threat detection and prevention for “..DoS and password-cracking attacks”. |
| wns0021093 | Improved handling of session state tables when there are an influx of clients associating/disassociating at a given time. |
| wns0021104 | Corrected 2.4GHz rate selection on AP38xx for single 1x1 clients. |
| wns0021196 | Improved session state handling when clients are idle which may have introduced instability on the Controller. |

| Enhancements in 10.41.12.0006 | |
|--------------------------------------|--|
| wns0020571 | Added integration of AP38xx with ExtremeLocation. |
| wns0021200 | Added new metrics ‘Noise Floor’ and ‘Radio Channel’ under Reports > APs > AP Performance by Radio. |
| wns0021241 | Added country support of AP3912i-ROW for Brazil |

| Changes in 10.41.11.0009 | |
|--|---|
| wns0020759 wns0021113 wns0021084 | Addressed logic in Low Link Speed health widget incorrectly reporting # of APs with dual ethernet ports. |
| wns0020762 | Improved In-Service Radar spoof detection for AP3805 reporting each other as spoof APs. |
| wns0020966 | Addressed corner case while under client load where controller in HA failed to notify APs to failover to secondary controller and WLAN would become disabled. |
| wns0020142 | Improved client compatibility for AP38xx when MFP is enabled. <i>(only a specific corner case issue was fixed. Please see Known Issue section)</i> |
| wns0021051 wns0021163 | Improved configuration import logic for upgrades from 9.21.xx to 10.41.xx due to channel width setting not being preserved instead of halting import process. |
| wns0021090 | Corrected mal-formed LLDP packets for AP39xx |
| wns0021091 | Improved stability of Wireless Controller with Netsight. |
| wns0021114 | Improved configuration import logic for upgrades from 10.41.08 to 10.41.10 due to IPv6 default action of Deny would change to None after upgrade. |
| wns0021123 | Improved error handling of failed connections between Wireless Controller and Netsight. |
| wns0021149 | Improved compatibility of AP39xx for FA with ERS switch in v7.6007. |
| wns0021185 | Improved configuration import logic for upgrades from 10.41.01 to 10.41.10 due to encrypted FTP passwords being used in Remote FTP settings within the GUI. |
| wns0021193 | Removed incorrect Mobility log messages while Availability is enabled with Mobility disabled. |

| Enhancements in 10.41.11.0009 | |
|--------------------------------------|---|
| wns0020779 | Added country support of ALL AP3865e and AP39xx for Myanmar |
| wns0021068 | Added country support of AP3865e and ALL AP39xx for El Salvador |
| wns0021088 | Added country support of AP3917i-ROW for Mexico |
| wns0021166 | Added country support of AP3865e and ALL AP39xx for Guatemala |

| Changes in 10.41.10.0014 | |
|---------------------------------|---|
| wns0020630 | Improved AP38xx stability for spectrum scans when Guardian is enabled. |
| wns0020763 | Revised workflow for AP search tab by preserving the input value to allow for configuring the AP and returning to the search list. |
| wns0020801 | Improved AP search to include both Active and Inactive APs. |
| wns0020803 | Addressed failover scenario where client traffic would not egress from an AP on a secondary controller. |
| wns0020843 | Corrected GUI spelling error on Home screen when Application Visibility referenced "Datebases" instead of "Databases". |
| wns0020879 | Reverted Health widget on dashboard to display AP uptime instead of tunnel duration. |
| wns0020887 | Improved ACS algorithm to prevent APs from selecting only the first channel from a list of best four channels. |
| wns0020903 | Added DHCP fingerprint for Windows 10: Microsoft Surface. |
| wns0020933 | Improved data path logic for clients sending multicast/broadcast packets with Controllers in Mobility (no HA) where a storm could occur on client roam. |
| wns0020862 | Resolved default route being inactive from routing table upon upgrade from V10.31 to V10.41. |

| Enhancements in 10.41.10.0014 | |
|--------------------------------------|---|
| wns0020806 | Added country support of AP3915i-ROW and AP3915e-ROW for Argentina. |
| wns0020857 | Added country support of AP3915i-ROW for Tonga. |
| wns0020863 | Removed Band 4 from AP3935/AP3965 Indoors for Egypt. |

| Changes in 10.41.09.0008 | |
|---------------------------------|--|
| wns0020387 | Updated AP default settings logic to properly enforce channel width when an AP is adopted for the first time. |
| wns0020566 | Resolved synchronization re-keying which could prevent AP from establishing their backup tunnel. |
| wns0020637 | Corrected logic while in Sites Mode using B@AP Topology where DHCP traffic would be encapsulated in WASSP tunnel. |
| wns0020651 | Improved congestion control on the radio to prevent radio resets. |
| wns0020687 | Resolved corner case whereby if AP was previously configured with Auto Channel and fixed channel width, if a factory reset occurred the AP would be stuck on channel 36 @ 20MHz. |
| wns0020688 | Updated GUI dashboard to allow click-through for the Un-Authenticated Stations icon. |
| wns0020699 wns0020715 | Updated GUI dashboard to display properly where extents of Health widget would previously be cut off. |
| wns0020760 | Addressed handling of commas in Guest User description field where exporting the file and importing it back would generate an error. |
| wns0020763 | Revised workflow for AP search tab by preserving the input value to allow for configuring the AP and returning to the search list. |

| Enhancements in 10.41.09.0008 | |
|--------------------------------------|--|
| wns0020716 | Added country support of AP3915i-ROW, AP3917i/e-ROW, AP3935i/e-ROW and AP3965i/e-ROW for Serbia. |

| Changes in 10.41.08.0012 | |
|---------------------------------|---|
| wns0019972 | Resolved interoperability with Aeroscout tags to emit the correct tag report. |
| wns0020519 | Addressed client location showing incorrectly on Netsight. |
| wns0020544 | Improved packet buffer management protection logic and data plane affinity assignment updates to better align with latest kernel architecture |
| wns0020567 | Corrected logic with handling of Policy rules with flexible IP port-range definitions. |
| wns0020576 | Addressed issue with intermittent failure to collect and report interface statistics for the wireless appliance. |
| wns0020580 | Corrected active AccessPoint count mib to be consistent with GUI. |
| wns0020594 | Resolved configuration conflict when saving topologies in an availability pair could result in VLAN ID conflict. |
| wns0020603 | Addressed beacon sending on incorrect data rate for 2.4GHz radio on AP3805 despite being configured. |
| wns0020621 | Corrected scheduled upgrade to apply correct date when enforcing the upgrade. |
| wns0020652 | Improved 802.1x compatibility with Sites Mode on AP3710. |

| Enhancements in 10.41.08.0012 | |
|--------------------------------------|---|
| wns0019286 | Added Client Port support on second ethernet port for AP3965e and AP3865e. |
| wns0019287 | Replaced AP serial number with AP name in the formatted AP alarm log sent to syslog, SNMP trap and XMC. |
| wns0020584 | Added country support of AP3917i/e-ROW for Korea. |
| wns0020633 | Added three new searchable columns (Status, Managed, IP Address) to AP List view. |
| wns0020645 | Added country support of AP3917i/e-ROW for Vietnam. |
| wns0020646 | Added country support of AP3965i-ROW for Bermuda and Dominican Republic. |
| wns0020658 | Updated power settings of AP3915i/e and AP3917i/e for Korea. |

| Changes in 10.41.07.0014 | |
|---------------------------------|---|
| wns0019859 | Relaxed 11k scanning aggressiveness when AP has many clients associated or multicast-to-unicast is enabled. |
| wns0019860 | Corrected issue where adding an L7 filter rule to a policy could result in any TOS/DSCP classifications to be removed. |
| wns0019924 | Relaxed the timers to 30mins for sending Area Change events in case client cannot be triangulated or client is no longer probing. |
| wns0019985 | Addressed migrating of Guest Usernames with invalid/empty passwords which could prevent Controller to upgrade successfully. |
| wns0020048 | Further improved logic for spoofed AP detection where APs would incorrectly report its own APs as spoofed. |
| wns0020055 | Adjusted SNMP update period in ifxtable for accurate polling into XMC. |
| wns0020241 | Updated Health dashboard report to only show "802.3.at-capable APs" in Low Power Mode across the AP39xx. |
| wns0020281 | Corrected active AccessPoint count mib to be consistent with GUI. |
| wns0020345 | Improved AP38xx performance for 2.4GHz in noisy environments. |
| wns0020430 | Resolved reoccurring messages flooding AP logs causing them to rollover quickly. |
| wns0020468 | Improved input handling for RADIUS shared-secret which was causing instability for the RADIUS client. |
| wns0020533 | Addressed port statistics not properly being updated in EWC Reports. |

| Enhancements in 10.41.07.0014 | |
|--------------------------------------|---|
| wns0019878 | Added enhancement to ADSP RadioShare (In-Service-Only) for AP39xx. |
| wns0020266 | Added Tenant ID support to ExtremeLocation™ for AP39xx. |
| wns0020502 | Added country support of AP3915i/e-ROW for Mexico, Chile, Vietnam and Japan. |
| wns0020503 | Added country support of AP3917i/e-ROW for Chile, India, Qatar, Dominican Republic, Argentina, Japan. |
| wns0020504 | Added country support of WS-AP3865e for Vietnam. |
| wns0020505 | Added country support of ALL AP38XX models for Kenya. |
| wns0020506 | Added country support of ALL AP39XX models for Kenya. |

| Changes in 10.41.06.0013 | |
|---------------------------------|---|
| wns0019788 | Modified DHCP fingerprint for WiDi boxes to report correctly. |
| wns0019944 | Corrected query of apCertificateExpiry mib to return accurate information. |
| wns0020048 | Adjusted logic for spoofed AP detection where APs would incorrectly report its own APs as spoofed . |
| wns0020085 | Adjusted GUI and CLI to have consistent SNMP password-length of 32 characters. |
| wns0020097 | Addressed logic for captive portal redirection when in Sites mode while using tunneled topologies. |
| wns0020126 | Corrected issue with displaying Tool-tips for Multi-edit |
| wns0020173 | Improved consistency of Client Search function on contextual reports (AP, VNS) |
| wns0020205 | Addressed issue with Multi-Edit not allowing configuration of parameters for AP391x Series APs. |
| wns0020192 | Corrected issue with credentials management logic on firmware upgrade of Camera Module of AP3916 |

| Enhancements in 10.41.06.0013 | |
|--------------------------------------|---|
| wns0019578 | Added enhancement responsiveness metrics for key protocols (DNS, DHCP) for AP38xx and AP39xx. |
| wns0020167 | Added Support for 802.1x Reauth for Wired Clients on AP3912 and AP3917. |
| wns0020174. | Extended support for AP packet capture to CLI. |
| wns0020322 | Added country support of AP3917i-ROW and AP3917e-ROW for China, Hong Kong, Brazil, Indonesia, Kuwait. |
| wns0020323 | Added country support of AP3915i-ROW and AP3915e-ROW for Korea_ROC and Brazil. |
| wns0020324 | Added country support of AP3915e-ROW for China, Hong Kong and Serbia. |
| wns0020325 | Added country support of All AP39xxx-ROW for Albania. |

| Changes in 10.41.05.0010 | |
|---------------------------------|---|
| wns0019886 | Addressed instability on AP39xx where AP would not perform full 802.1x re-authentication. |
| wns0019920 | Addressed handling of mal-formed DNS packets by adding more protection when decoding DNS replies. |
| wns0019979 | Corrected issue with interpretation of policy/filter rules which could prevent enablement of services on AP radios. |
| wns0020024 | Enhanced logic for AP39xx where having a larger number of clients associated could impact AP service. |

| Enhancements in 10.41.05.0010 | |
|--------------------------------------|--|
| wns0019285 | Added support for 802.1x authentication on AP3912 and AP3917 Client ports. |
| wns0019289 | Added SSID and Encryption in "Reports - Active threats report". |
| wns0019290 | Added support for IOT: AP as Edystone Beacon. |
| wns0019939 | Added warning message when number of mobility domain users exceeds 48k. |

| Enhancements in 10.41.04.0002 | |
|--------------------------------------|--|
| wns0019955 | Added country support of AP3916ic for Saudi Arabia |
| wns0019956 | Added country support of AP3915i-ROW for Chile, China, Ecuador, Hong Kong, India, Indonesia, Kuwait, Malaysia, Peru, Philippines, Qatar, Russia, Saudi Arabia, Singapore, South Africa, Taiwan, Thailand and UAE |
| wns0019957 | Added DFS Channels for FCC based countries to AP3915i-FCC |
| wns0019958 | Added DFS Channels for FCC based countries to AP3915e-FCC |
| wns0019959 | Added country support of AP3915e-ROW for Chile, Ecuador, India, Indonesia, Kuwait, Malaysia, Philippines, Peru, Qatar, Russia, Saudi Arabia, Singapore, South Africa, Taiwan, Thailand and UAE. |
| wns0019960 | Added country support of AP3917i-ROW for Ecuador, Malaysia, Philippines, Russia, South Africa, Thailand and UAE |
| wns0019961 | Added DFS Channels for FCC based countries to AP3917i-FCC |
| wns0019962 | Added country support of AP3917e-ROW for Ecuador, Malaysia, Philippines, Russia, South Africa, Thailand and UAE |
| wns0019963 | Added DFS Channels for FCC based countries to AP3917e-FCC |
| wns0019964 | Added DFS Channels for FCC based countries to AP3917k-FCC |
| wns0019994 | Added country support of AP3917e-ROW for Peru, Saudi Arabia and Taiwan |
| wns0019995 | Added country support of AP3917i-ROW Hong Kong, Peru, Saudi Arabia and Taiwan |
| wns0019996 | Added country support of AP3916ic-ROW for India |

| Changes in 10.41.03.0012 | |
|---------------------------------|---|
| wns0017485 | Changing the VLAIN ID for an assigned B@AP topology requires rebooting of Access Points on which the topology is present |
| wns0019434 | Improved resilience in handling of timer expirations for 802.11r/Fast Transitions (FT). |
| wns0019704 | Updated logic to ensure that Client Limits are updated whenever limits are adjusted for an existing Radio Preference group. |
| wns0019827 | Corrected packet length calculations on interface to RNDIS driver interface for HyperV that could cause packet drop for VLAN tagged interfaces. |
| wns0019868 | Improved parsing of OUIs starting with an encoding equivalent to "0x" |
| wns0019876 | Removed "Service" account from Access Points |
| wns0019891 | Improved recognition of terminal characteristics from Customer's browser for AP Remote Shell feature to better support international keyboards |

| Enhancements in 10.41.03.0012 | |
|--------------------------------------|---|
| wns0017287 | Draeger Certification for AP3912i and AP3916ic. |
| wns0017963 | Added support to RADIUS Access-Request for username AVP longer than 253 characters. |
| wns0018777 | Add ability to 'Pause' a Remote Packet Capture session. |
| wns0019288 | Added "Export" option to Radar->Uncategorized APs report for XLS and XML. |
| wns0019292 | Updated RADAR logging events description to include channel numbers with the frequency. |
| wns0019293 | Enhanced logic for Topology Groups to sort by VLAN ID then re-index them in order to have symmetry between multiple Availability Pairs. |
| wns0019700 | Added country support of AP3912i for Mexico. |
| wns0019701 | Added country support of AP3916i for Mexico. |
| wns0019744 | Added country support of AP3916i for Brazil. |
| wns0019745 | Added country support of AP3916i for Serbia. |
| wns0019746 | Added country support of AP3916i for China. |
| wns0019747 | Added country support of AP3912i for Serbia. |
| wns0019832 | Added country support of AP3915i/e for Taiwan. |
| wns0019908 | Added AP Remote Diagnostics (Packet Capture/SSH) when in Availability Mode, allowing remote access to an AP even if the AP is actively connected to the peer appliance. |

New features in V10.41.02.0014

Introduces AP3917i/AP3917e/AP3917k (2x2 11ac wave 2) Access Point

- The AP3917 is a feature rich 802.11ac Wave 2 and 802.11abgn outdoor access point that extends affordable enterprise-grade mobility beyond the walls. These outdoor access points are designed to operate in harsh environments such as manufacturing plants, parks, practice facilities and budget conscious venues. The AP3917 offers multiple connectivity options including WiFi 2.4GHz, WiFi 5GHz, and BLE/802.15.4 (Thread, etc.) for location services or extended connectivity to Internet of Things (IoT) sensors and devices.
- AP3917i, AP3917e and AP3917k are 2x2 dual concurrent 5GHz/2.4GHz band APs. They support 11ac Wave 2 on the 5GHz radio and 11n on the 2.4GHz radio, and feature an integrated Bluetooth Low Energy (4.0)/802.15.4 sensor radio.
- AP3917e and AP3917k are equipped with the integrated GPS hardware, which provides the coordinate information of the access point location. The software support of the GPS is not available in V10.41.02. Software support will be available in a later release.
- AP3917k is a PCB board only model with no enclosure. This model is available only for specific partner integration and is not available for general resale.
- Interfaces:
 - 1 x 1 Gbps uplink port
 - 1 x 1 Gbps client port
 - 1 x RJ45 Console port

- There are six new models available:
 - AP3917i-FCC and AP3917e-FCC for the FCC region:
COLOMBIA, PUERTO_RICO, UNITED_STATES
 - AP3917i-ROW and AP3917e-ROW for the rest of the world region
AUSTRALIA, AUSTRIA, BELGIUM, BOSNIA_HERZEGOVINA, BULGARIA, CANADA, CROATIA, CYPRUS, CZECH, DENMARK, ESTONIA, FINLAND, FRANCE, GEORGIA, GERMANY, GREECE, HUNGARY, ICELAND, IRELAND, ITALY, KAZAKHSTAN, KOSOVO, LATVIA, LIECHTENSTEIN, LITHUANIA, LUXEMBOURG, MACAU, MACEDONIA, MALTA, MONTENEGRO, NETHERLANDS, NEW_ZEALAND, NORWAY, POLAND, PORTUGAL, ROMANIA, SINGAPORE, SLOVAKIA, SLOVENIA, SPAIN, SWEDEN, SWITZERLAND, TURKEY, UNITED_KINGDOM
 - AP3917k-FCC for the FCC region:
COLOMBIA, PUERTO_RICO, UNITED_STATES
 - AP3917k-ROW for the rest of the world region
CANADA

Introduces AP3912/AP3915/AP3916/AP3917Thread™ Gateway for IOT

- A Border Router is a specific type of router that provides connectivity from the Thread™(802.15.4) network to adjacent networks on other physical layers (for example, Wi-Fi and Ethernet).
- Devices in the Thread™ stack support IPv6 addressing. AP3912/AP3915/AP3916/AP3917 will act as border GW between Wi-Fi & Thread network. The Border Gateway function enabled Thread™ devices to communicate with internet entities (Application management, device control or data/state visibility) using IPv6.
- Thread™ Gateway leverages the IOT radio's capability for IEEE Standard 802.15.4 and operates on 2.4GHz band.

AP3900 Series Integration with AirDefense 9.5

- Extend availability of Extreme AirDefense™ as a WIPS/WIDS choice for ExtremeWireless™ installations.
- ADSP server will recognize and adopt AP3900 series APs.
- Automate provisioning by enabling Collection of ExtremeWireless™ SSID/BSSID mappings for deployment info, from wireless appliance via SNMP.
- Configuration of Sensor APs via HWC ADSP Server IP addresses and assign the AP into the ADSP Scan Group.
- APs can only operate as full-time sensors. Radio-Share function is not available in 10.41.02. It will be considered for a future release.
 - Note: Configuring an AP3916ic as an ADSP Sensor will disable the usage of the integrated camera.
- Requires AP Capacity license on ExtremeWireless. Does not require RADAR licenses.
- Adoption and feature licenses for Extreme AirDefense are required. Refer to the Extreme AirDefense Datasheet for details.

AP3900 Series Integration with ExtremeLocation 1.1

- Integration of ExtremeWireless™ AP3900 series with ExtremeLocation 1.1 system.
- AP establishes websocket connections (HTTPS with self-signed certificates) to the ExtremeLocation Server and reports RSS readings based on the ExtremeLocation configuration.
- In V10.41.02, Tenant information, Site information and AP (added/deleted from configuration) are not provided from the Controller to the ExtremeLocation. ExtremeLocation administrators must create and associate theTenant Id and Site with the AP MAC addresses reported over AP webSocket.

| Changes in 10.41.02.0014 | |
|---------------------------------|--|
| wns0018847 | Adjusted UI logic to correct logic for persisting configuration of Fast-Failover settings in RADIUS Accounting. |
| wns0019234 | When running in link persistence mode with B@AP, corrected logic to prevent duplicate L2 updates for new client associations to AP. This could cause invalid MAC addresses to show up on AP switch port. |
| wns0019326 | Corrected policy assignment for clients roaming with Fast Transition (802.11r/FT) services. |
| wns0019361 | Changed behavior for AP with link persistence mode disabled. If Ethernet link goes down, it now prevents the AP from rebooting. This behavior is consistent whether link persistence is enabled or disabled. |
| wns0019371 | Adjusted logic to prevent the requirement to change channel if configured as Auto when channel width is being changed. |
| wns0019397 | Corrected Controller MIB attribute "apPerformanceReportbyRadioAndWlanTable" to return accurate number of clients and WLANs being broadcast by AP radios when queried. |
| wns0019449 | Addressed corner case where enabling MBA and Accounting and then disabling MBA could result in MBA still being enabled. |
| wns0019479 | Adjusted radio state management logic to prevent race condition that could prevent radios from being disabled by administrator command for WDS setups with multiple SSIDs. |
| wns0019529 | Corrected logic when in Sites Mode where client session lifetime would not adhere to pre-auth idle, post-auth idle, or session timeouts. As a result, this could cause client sessions to be cleaned up prematurely. |

| Changes in 10.41.01.0082 | |
|---------------------------------|--|
| wns0019363, wns0019377 | <p>Addressed several vulnerabilities related to protection of key management and improved key re-installation protection for AP as Authenticator for WPAv2 (PSK or Enterprise) services and as supplicant for WDS/Mesh functions:</p> <p>CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13081, CVE-2017-13082, CVE-2017-13086, CVE-2017-13087, CVE-2017-13088</p> <p>Please refer to Vulnerability Notice 18005 KRACK, WPA2 Protocol Flaw (https://extremeportal.force.com/ExtrArticleDetail?n=000018005) for updates to release schedule.</p> |
| wns0019430 | <p>Addressed issue after an upgrade where if auto channel selection is used, it would re-request a new channel and channel width. The expected behavior has been corrected to preserve previous channel and channel width. Also adjusted UI logic when channel is set to 'Auto' to only allow channel widths of 'Auto' or '20MHz'.</p> |

New features in V10.41.01.0080

Introduces AP3915i/AP3915e (2x2 11ac wave 2) Access Point

- The AP3915 is a feature rich 802.11ac Wave 2 and 802.11abgn indoor access point that delivers enterprise-grade performance and security without the premium cost. The AP3915i is designed to blend into any office, carpeted enterprise, or classroom environment. The AP3915 offers multiple connectivity options including 2.4G, 5G, and BLE/802.15.4 (Thread, etc.) for location services and extended connectivity to Internet of Things (IoT) sensors and devices.
- AP3915i and AP3915e are a 2x2 dual concurrent 5GHz/2.4GHz band AP. It supports 11ac Wave 2 on the 5GHz radio and 11n on the 2.4GHz radio. It also features an integrated Bluetooth Low Energy (4.0)/802.15.4 sensor radio.
- Interfaces:
 - 1 x 1 Gbps uplink port
 - 1 x RJ45 Console port (optional)
 - 1 x External 12V Power Supply connector (optional)
- There are four new models available:
 - AP3915i-FCC and AP3915e-FCC for the FCC region:
COLOMBIA, PUERTO_RICO, UNITED_STATES
 - AP3915i-ROW and AP3915e-ROW for the rest of the world region
AUSTRALIA, AUSTRIA, BELGIUM, BOSNIA_HERZEGOVINA, BULGARIA, CANADA, CROATIA, CYPRUS, CZECH, DENMARK, ESTONIA, FINLAND, FRANCE, GEORGIA, GERMANY, GREECE, HUNGARY, ICELAND, IRELAND, ITALY, KAZAKHSTAN, KOSOVO, LATVIA, LIECHTENSTEIN, LITHUANIA, LUXEMBOURG, MACAU, MACEDONIA, MALTA, MONTENEGRO, NETHERLANDS, NEW_ZEALAND, NORWAY, POLAND, PORTUGAL, ROMANIA, SLOVAKIA, SLOVENIA, SPAIN, SWEDEN, SWITZERLAND, TURKEY, UNITED_KINGDOM

Introduces C5215 Wireless Controller Platform

- C5215 is a new ExtremeWireless Management platform, supporting up to 1000 APs and 16,000 users in Standalone or 2000 APs and 32,000 users in High Availability pair. This platform is equivalent to the existing C5210 and will serve as its effective replacement offering. (Note: Requires minimum of 10.41.01.)
- Configuration import for C5210 to C5215 is supported.
- Rescue image import from C5210 to C5215 (or vice versa) is NOT supported.
- The C5215 hardware platform will be released in November 2017.

Fabric Attach: Edge Automation

- Fabric Attach provides Edge Installation Automation with Zero-Touch User & Device Attachment
- Integrates Extreme Edge products & connection services with next-generation Fabric Core
- Fabric Attach extends Fabric Connect services to EXOS and ExtremeWireless™ Edge
- Facilitates clients network access via VLAN abstraction as Individual Service Identifier (I-SID)
- FA Client(AP), Server/Proxy (switches) elements exchange facilitate orchestration of points of presence and path
- Leverage Extreme's dynamic role based policy control and automation and orchestration to secure auto-attachment of users/devices to Fabric-based services
- Automates switch port provisioning for required topologies
- This feature is only supported on AP3912/AP3915/AP3916/AP3935/AP3965 families.

AP Upgrade with Minimized Service Impact

- This feature extends the rebooting APs on schedule without interrupting the service to upgrading the AP FW process.
- Under the control upgrade process, the AP FW will be upgraded when the AP has low traffic and/or is in consideration of channel plan to minimize impact to wireless service.

ExtremeAnalytics™ Signature Synchronization

- Support synchronization of Application signature sets from ExtremeManagement™ to propagate updates due to Custom signature definition or subscription updates.
- ExtremeManagement™ Center will sync changes to signature definitions (Custom, Updates) to ExtremeWireless™ and ExtremeAnalytics.

AP Diagnostics

- The feature provides the AP diagnostics capability via wireless controller. It includes the various remote tools on the wireless controller:
 - AP Remote Shell to provide remote command line access to each AP.
 - AP image upgrade via HTTP, which reduces AP image download time compared to the current TFTP method.
 - AP Remote Packet Capture provides real time traffic view on the AP for both the management and the data traffic.

Auto Channel Width Selection (ACWS)

- This feature enhances the channel selection algorithm by performing deployment density evaluation. For dense deployments, the 80 MHz channels will be split in two 40MHz or four 20MHz channels in order to increase the number of individual channels available for selection. The ACS algorithm will select the AP channels to ensure minimum co-channel interferences and avoid channel overlap.
- New and improved formula to calculate best channel based on channel cost, penalty for Noise, CCI /NCI and tie-breakers.
- Results are aggregated into Channel Inspector report facilitating easier validation of channel selection results.

DFS - Return to Original Channel

- This feature restores AP channel to the original DFS channel after a Radar event. It allows for a stable deployment channel plan.
- Post Radar / DFS event, the channel is flagged and should not be used for 30 minutes according (to the DFS standard). AP performs ACS and selects a new channel from the allowed channel list. After 30 minutes, the original channel can be used again and the AP will return to the original channel as soon as the AP does not service any clients.

Airtime Fairness Update

- This feature allows the user to define up to four WLANs that have configurable minimum air time reservation during periods of congestion. Up to 80% airtime can be configured. The other 20% airtime is reserved for other WLANs to prevent starvation.
- Flexible Client Access (FCA) was previously introduced during the transition from legacy WiFi to 11n. Modern 11ac WiFi interface supports client air time fairness by default. FCA is no longer needed.

IOT: iBeacon RTLS (listening) Reporting

- Extends RTLS capability to support use cases such as asset tagging - using standard (off the shelf) iBeacon tags. APs receive the presence of iBeacon messages from tags within range and report the corresponding signal strength to a defined application server implemented by the customer in real time.
- The iBeacon info is translated into JSON structure (to facilitate easier application programming) and transported to a configured recipient application server via the wireless Controller. The applications can correlate location context based on access point location via BatchLocationReport for additional context.

AP web server configured with commercial certificates to avoid captive portal browser HTTPS warning

- Upgraded the built-in certificate on the AP to the valid commercial certificate. This avoids the browser-generated warning during a captive portal redirect.

Layer 7 Application signature updates for V10.41

- The following signatures were added in this release:
 - AccountKit
 - Adobe IO
 - Answers Cloud Services
 - LawRoom
 - LiveChat
 - Livingly Media

- AppointmentPlus
- Assembla
- Autodesk
- Bidpath
- BidTheatre
- CADVault
- CareZone
- Cisco Meraki
- ComplianceDesktop
- Consumer Reports
- Continuum
- Conversica
- Customer.io
- DLNA Service
- Doctor On Demand
- Doximity
- Druva
- Endomondo
- Epic
- Epocrates
- Eyeota
- FastMail
- FollowMyHealth
- FSV Payment Systems
- GoodRx
- HealthTap
- inContact
- Kronos
- Mac App Store
- MathXL
- NE Journal of Medicine
- Nuance
- Nvidia
- Oracle Cloud
- Pearson VUE
- PEPID
- Piazza
- POLYV
- ReviewBoard
- Rise
- ROXIMITY
- SAP SuccessFactors
- Secure-24
- ServiceNow
- Signal
- Silverpeak GMS
- Skype for Business
- SocialChorus
- Strava
- Symplicity
- Teem
- Vengo
- Verizon Voice over WiFi
- Vertex
- vTuner
- Wishabi
- ZAM
- Zocdoc

| Changes in 10.41.01.0080 | |
|---------------------------------|---|
| wns0018612 | Fixed the implementation of filter search that had a redundancy that might generate a warning message. Data traffic was not impacted. |
| wns0018713 | Force the AP to use short GI when the AP is as Parent in the WDS/Mesh in order to improve the throughput performance between the Parent AP and the Child AP. |
| wns0018751 | Correct the warning message when the AP has a low speed Ethernet link other than 1GB. |
| wns0018798 | Stop sending the Radius Accounting Interim Update when the configured value for "Interim Accounting Interval" is zero. |
| wns0018833 | Correct the error that the AP radio will be stopped after the fast-failover if there is antenna setting is defaulted on the secondly wireless controller. |
| wns0018861 | Adding support for the case where a RADIUS server was back up after being down. And this scenario was for a WLAN Service with only 1 RADIUS server. And the RADIUS server was put in the down state from another WLAN Service where the RADIUS server was the primary server (and there is at least 1 backup server). |

| Changes in 10.31.06.0007 | |
|---------------------------------|--|
| wns0018025 | Resolved a corner case where creating a topology may have an invalid internal VLAN ID causing Controller instability. |
| wns0018713 | Addressed configuration not being applied for guard interval->Short in a Mesh/WDS deployment which resulted in link using Long guard interval. |
| wns0018751 | Changed GUI dashboard verbiage under Health to "APs with Low Link Speed" |
| wns0018798 | Resolved RADIUS Accounting sending interim accounting messages despite the interval set to "0" (disabled). |
| wns0018830 | Addressed floor plans being deleted between HA paired controllers when managed by ExtremeManagement. |
| wns0018833 | Corrected failover scenario for external antenna APs that would disable their radios while in a Mesh/WDS link. |
| wns0018861 | Addressed scenario for multiple WLAN services having common RADIUS servers configured. If the common RADIUS Server went down, the WLAN Service with only 1 primary RADIUS server would not accept new RADIUS requests as a consequence of it being marked as down. |

| Changes in 10.31.05.0003 | |
|---------------------------------|--|
| wns0018482 | Addressed corner case where ordering of WLAN Services assigned to AP could prevent clients from roaming. |
| wns0018613 | Corrected the ability to add multiple domains to Hotspot identification field. |

| Enhancements in 10.31.04.0009 | |
|--------------------------------------|--|
| wns0018137 | Added support for dual-2.4 GHz radio for SCALANCE W786C / W788C. |

| Changes in 10.31.04.0009 | |
|---------------------------------|---|
| wns0017368 | Readjusted change for improved stability for Load Balance Groups when many clients are within the same group |
| wns0017422 | Corrected Guest Account session lifetime to act as an upper bound on the session duration |
| wns0018026 | Resolved invalid link speed being reported by AP during LACP bonding negotiation |
| wns0018046 | Improved client roaming with Mobility enabled between HA pairs running V9 and V10 |
| wns0018057 | Modified Device fingerprint signature for HP Printer to show correct OS |
| wns0018375 | Corrected corner case where changing domain keys could prevent Radar from turning ON |
| wns0018446 | Adjusted radio configuration logic to ensure that changes to privacy for defined service are propagated correctly. |
| wns0018508 | Improved stability for handling Configuration of WLAN Services with RADIUS Accounting delivery without a defined RADIUS server. |
| wns0018524 | Improved protection against bad frames on AP38xx and AP39xx |
| wns0018545 | Resolved Location Engine showing multiple audit log entries that a floor plan has been deleted. |
| wns0018553 | Corrected logic for filtering rule when using an IP port of '0' which could cause Web traffic to be blocked. |
| wns0018556 | Improved cloud connector's state machine to protect against interrupted connections, for ExtremeCloud™ managed Access Points. |

| Enhancements in 10.31.03.0012 | |
|--------------------------------------|---|
| wns0017956 | Added existing reports for 'Clients by AP' and 'Clients by VNS' under the Reports > Clients menu. |
| wns0018087 | Added Country Support for Russia for AP3916ic-ROW. |
| wns0018088 | Added Country support for Dominican Republic for AP3916ic-ROW. |
| wns0018089 | Added Country support for Ecuador for AP3916ic-ROW. |
| wns0018090 | Added country support for South Africa for AP3916ic-ROW. |
| wns0018091 | Added Country support for Taiwan for AP3916ic-ROW. |
| wns0018092 | Added Country support for Indonesia for AP3912i-ROW. |
| wns0018093 | Added Channels 116-128 (DFS Channels) for Columbia for AP39xx-FCC. |
| wns0018094 | Added Channels 116-128 (DFS Channels) for Puerto Rico for AP39xx-FCC. |
| wns0018095 | Added Channels 116-128 (DFS Channels) for United States for AP39xx-FCC. |

| Changes in 10.31.03.0012 | |
|---------------------------------|--|
| wns0017164 | Improved AP3935 stability when Guardian Mode is enabled will all features set. |
| wns0017368 | Improved stability for Load Balance Groups when many clients are within the same group |
| wns0017377 | Addressed instability on AP37xx and AP38xx when convert multicast-to-unicast feature is enabled |
| wns0017478 | Improved Airtime Fairness algorithm for when only 1 WLAN Service has it enabled. |
| wns0017916 | Corrected Wireless Client reports not loaded due to special characters in hostname or username. |
| wns0018005 | Resolved LACP not working on AP3825 after upgrade to 10.31.01.0048. |
| wns0018008 | Addressed reporting inconsistency where AP39xx was showing incorrect noise floor levels |
| wns0018062 | Addressed Potential Vulnerability of AP/Controller in CVE-2016-10229 |
| wns0018078 | Resolved config restore for CLI command 'called-station-id-ssid disable' when upgrading from 9.21.x to 10.31.x |
| wns0018139 | Addressed memory leak on AP37xx and AP38xx when 11k enabled |

| Enhancements in 10.31.02.0007 | |
|--------------------------------------|---|
| wns0017991 | Added Country support for Kuwait for AP3916ic. |
| wns0017992 | Added Country support for Philippines for AP3916ic-ROW. |
| wns0017993 | Added Country support for Singapore for AP3916ic-ROW. |
| wns0017994 | Added Country support for Malaysia for AP3916ic-ROW. |
| wns0017995 | Added Country support for Hong Kong for AP3916ic-ROW. |
| wns0017996 | Added Country support for Peru for AP3916ic-ROW. |
| wns0017997 | Added Country support for Singapore for AP3912i-ROW. |
| wns0017998 | Added Country support for Trinidad & Tobago for AP3912i-ROW. |
| wns0017999 | Added Country support for Dominican Republic for AP3912i-ROW. |
| wns0018000 | Added Country support for Ukraine for AP3825i. |
| wns0018001 | Added Country support for Uganda for AP3800 models. |
| wns0018017 | Added FCC DFS Channel support for AP3916iC-FCC and AP3916ic-ROW models. |
| wns0017430 | Added a second configuration option for sending RADIUS accounting packets; send to only one server (round-robin). |
| wns0017611 | Added AP support for Pronto Captive Portal. |
| wns0017898 | Introduced a process to update AP Webserver certificate prior to expiration when using FFECP @ AP. |

| Changes in 10.31.02.0007 | |
|---------------------------------|--|
| wns0016226 | Improved configuration import logic to prompt user to re-enter corrupted Radius Secret values instead of halting import process. |
| wns0017126 | Enhanced logic in Background Scan and Quiet IE functions for 802.11k to better handle effect of devices in Power Save Mode |
| wns0017305 | Added new signature "APP: FACEBOOK-ZERO" to detect new Facebook flow. |
| 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 |
| wns0017752 | Addressed client connectivity issue with AP3805i-FCC and AP3935i-FCC when switching a WLAN privacy between WEP(128-bit) and WPA-PSK(AES) |
| wns0017926 | Improved stability on AP3935/AP3965 when SIAPP traffic is present. |
| wns0017968 | Addressed the RFC3580 support for RADIUS Access-Request Called-Station-Id to use format BSSID:SSID. |
| wns0018004 | Improved 11k stability during background scan when Radar is detected. |
| wns0017221 | Addressed TCP connection sessions still showing ESTABLISHED by purging MU and HOST tables after session timeout. |

New features in V10.31.01.0048

Introduces AP3916ic (2x2 11ac wave 2) with integrated infrared camera

- AP3916ic is a 2x2 dual concurrent 5GHz/2.4GHz band AP with an integrated 2MB camera. It supports 11ac Wave 2 on the 5GHz radio and 11n on the 2.4GHz radio. The onboard camera is equipped with a 2MB sensor which supports up to 1080p real time video streaming. The on-board camera is ONVIF certified enabling third party video management support.
- There are two new models available:
 - AP3916ic-FCC for the FCC region:
COLOMBIA, PUERTO_RICO, UNITED_STATES
 - AP3916ic-ROW for the rest of the world region
AUSTRALIA, AUSTRIA, BELGIUM, BOSNIA_HERZEGOVINA, BULGARIA, CANADA, CROATIA, CYPRUS, CZECH, DENMARK, ESTONIA, FINLAND, FRANCE, GEORGIA, GERMANY, GREECE, HUNGARY, ICELAND, IRELAND, ITALY, KOSOVO, LATVIA, LIECHTENSTEIN, LITHUANIA, LUXEMBOURG, MACAU, MACEDONIA, MALTA, MONTENEGRO, NETHERLANDS, NEW_ZEALAND, NORWAY, POLAND, PORTUGAL, ROMANIA, SLOVAKIA, SLOVENIA, SPAIN, SWEDEN, SWITZERLAND, TURKEY, UNITED_KINGDOM

AP3912/AP3916 IoT GW with iBeacon Support

- Both AP3912i and AP3916ic Access Points are equipped with a Bluetooth Low Energy radio, which now provides iBeacon (Apple based standard) support. When the iBeacon feature is enabled, an iBeacon is transmitted periodically by the AP that can be seen by mobile devices. For example, this feature can be used by way-finding mobile applications to get location information about the user.

Added a pre-defined Topology Multicast Filter for AP3916ic

- WS-Discovery multicast group available in drop down for policy definition of topologies. WS-Discovery is the base multicast group used by ONVIF device discovery.
- This multicast group policy must be applied to the default topology assigned to the CAM function of the AP3916ic in order to support the ONVIF discovery protocol.

Topology Independent Captive Portal @ AP

- In the captive portal support for the B@AP topology, the AP will use fixed IP address 1.1.1.1 for captive portal redirects. Extreme will register sub-domain "portal.ezcloudx.com" and populate public/Extreme DNS server with DNS mapping of 1.1.1.1 for FQDN "portal.ezcloudx.com".
- When MU is redirected to captive portal, AP will include in the URL the FQDN "portal.ezcloudx.com" as AP's address.
- Upgrade from pre v10.31 will require to insert new rules in both "non-auth" and "auth" policies.

Weather Channel Support on AP3916ic

- AP3916ic-ROW has obtained the certification of using the weather channels including 5600MHz-5650MHz sub-bands.
- The certification includes the DFS detection on the weather channels and the 10 mins CAC (Channel Availability Check) before providing the service on the weather channels.

Configurable WDS ACK Timeout

- A new AP configuration option is provided to allow indication of expected distance between two nodes. In particular, for WDS links, distance between WDS points can add significant delay to the roundtrip of control Acknowledgements. The Distance indicator automatically adjusts the timeout values of control functions of the 802.11 stack to improve link quality and reduce retries for links over large distances. It is applicable to all the AP38xx/AP39xx Access Point products.

ACS enhancements for Sites

- This feature allow user to issue "Site Auto Channel Selection" from the main site menu. The controller will forward the command to the 1st active site AP found. The selected AP will forward the command to all other members over SIAPP.
- All the AP in the site group will participate in the ACS operation.

AP LAN MAC address as Called-Station-ID

- This feature allows the user to configure Called-Station-Id overwrite flag with a newly added checkbox.
- When the above check box is enabled, the Called-Station-Id can be overwritten for both the wired and wireless client with the AP Management port MAC address in the Radius request.
- When the above check box is disabled, the wireless client Called-Station-Id uses the BSSID value for the wireless client as before and the AP Management port MAC address for the wired client.

Reporting of AP LAN Link speed and duplex

- The AP inventory report was enhanced to display the negotiated link speed and duplex information for the AP LAN ports.
- A new health check indicator will identify APs with link connections not matching their optimal configuration.

Created a new Regulatory Key to enforce only EGYPT Selection

- As of January 1st 2017, regulatory requirements in Egypt deployments are required to enforce/assert that deployed access points are only configured according to Egypt compliance regulations. Only Egypt is allowed as an available country.
- A new Regulatory License key (EGY) is now available (Parts: 30319 HW, 30320 Virtual). Once installed, the EGY key restricts the country selection for AP assignment to Egypt (and only Egypt).
- Egypt is no longer available for ROW or MNT keys.

Validation of V2110 with VMWare ESXi 6.5

- Added support for VMWare ESXi 6.5 to the V2110.

New AP configuration properties publisher

- The Push Publisher Report facility was enhanced to provide a new option to publish high-level AP configuration properties as a periodic XML report. The report includes AP name, Serial Number, BSSID, IOT configuration, Location XY coordinates, etc.

Layer 7 Application signature updates for V10.31

- The following signatures were added in this release:

| Signature | Display Name |
|--------------------|-----------------------|
| 360OVERSEAS | 360 Software |
| ADOBEDTM-COM | Adobe Marketing Cloud |
| AKISMET-COM | Akismet |
| ANY-DO | Any.do |
| AVAST-COM | Avast |
| AVIRA-COM | Avira |
| BEACONSINSPACE-COM | BeaconsInSpace |
| BITDEFENDER | Bitdefender |
| BITMOJI-COM | Bitmoji |
| CDC-GOV | CDC |
| CMCM-COM | Cheetah Mobile |
| CLOUDFLARESSL-COM | CloudFlare |
| COMODO-COM | Comodo Security |
| DOCKER | Docker |
| DROPBOXAPI-COM | Dropbox |

| | |
|----------------------|--|
| DUOLINGO-COM | Duolingo |
| LIVESEGMENTSERVICE | ESPN |
| EVERALBUM-COM | EverAlbum |
| SCDN-CO | Fastly |
| FIREEYE-COM | FireEye |
| FOODUCATE-COM | Fooducate |
| FOOTMARKS-COM | Footmarks |
| FOXSPORTSGO-COM | FOX Sports Go |
| FOXSPORTSGO-UA | FOX Sports Go |
| FSG-BAMCONTENT | FOX Sports Go |
| GETTYIMAGES | Getty Images |
| ULXIMG-COM | HotNewHipHop |
| HOUSTONTEXANS-COM | Houston Texans Football |
| HULU-DASH | Hulu |
| HULUEDGECAST | Hulu |
| BLOBSTORE-APPLE-COM | iCloud |
| IDRIVE-COM | IDrive |
| IFTTT-COM | IFTTT |
| CCOMRCDN-COM | iHeartRadio |
| LETGO-COM | Letgo |
| LIFESUM-COM | Lifesum |
| LSMDM-COM | Lightspeed Systems |
| MALWAREBYTES | Malwarebytes |
| MAYOCLINIC-ORG | Mayo Clinic |
| MAYO-EDU | Mayo Clinic |
| MSEDGE-NET | Microsoft CDN |
| MIMECAST-COM | Mimecast |
| MOXTRA-COM | Moxtra |
| MPARTICLE-COM | mParticle |
| MYFITNESSPAL-COM | MyFitnessPal |
| UA-MYRADAR | MyRadar |
| NR-DATA-NET | New Relic |
| CLOUDMAGIC-COM | Newton |
| NFL-MOBILE-AKAMAHD | NFL Mobile -(Android and IOS requests) to Akamai CDN |
| NFLRUSH-COM | NFL RUSH |
| UA-NFLRUSH | NFL RUSH |
| OCULUS | Oculus |
| PALOALTONETWORKS-COM | PaloAlto Networks |
| PANDASECURITY-COM | Panda Security |
| PIKSEL-COM | Piksel |

| | |
|---------------------------|----------------------|
| QRADAR-TCP | QRadar |
| XFORCE-SECURITY | QRadar |
| SAMSUNG-COM | Samsung |
| SAMUNG CLOUD-COM | Samsung Cloud |
| SHARINGBOX-COM | Sharingbox |
| SHOEBOXAPP-COM | Shoebox |
| SLING-SPSBXSMES | Slingbox |
| SMITHMICRO-COM | Smith Micro |
| PICTURELIFE-COM | SmugMug |
| SNAPADS-COM | Snapchat Advertising |
| SOPHOSUPD-COM | Sophos |
| SOPHOSUPD-COM | Sophos |
| SPACEMONKEY-COM | SpaceMonkey |
| SPINRILLA | Spinrilla |
| SPRINGER-COM | Springer |
| STEAMCONTENT-COM | Steam |
| GOAPPS-TCP | Sungy Mobile |
| GOFORANDROID-COM | Sungy Mobile |
| SWARMAPP-COM | Swarm |
| TEAMVIEWER-COM | TeamViewer |
| TELEGRAM-ORG | Telegram |
| THRIVEMARKET-COM | Thrive Market |
| VADIO-COM | Vadio |
| VEMBA-IO | Vemba |
| WFXTRIGGERS-COM | Weather Channel |
| WEBMD-COM | WebMD |
| WEBROOT | Webroot |
| WIBBITZ-COM | Wibbitz |
| WOLFRAMALPHA-COM | Wolfram Alpha |
| AMP-AVAI-COM | Super Bowl 51 |
| SUPER-BOWL51-FISHSOFTWARE | |
| UA-SUPER-BOWL-51 | |
| BRICKFTP | BrickFTP |
| IPERF-TCP | iPerf |
| IPERF-TCP1 | |
| PINGHD | Ping HD |
| SMOOTHSTREAMS | SmoothStreamsTV |
| STREAMRAIL | StreamRail |
| UNITY3D | Unity Game Engine |

- Changed the group name for the following Yinzcam fingerprints to Sports:

- YINZCAM
- YINZCAM-S3-STORAGE
- Changed the display name for the following Skydrive fingerprints to "Microsoft OneDrive":
 - MESH
 - UA-SKYDRIVE
 - SKYDRIVE-MSN-WEBAPP
 - SKYDRIVE-LIVEFILESTORE-WEBAPP
 - SKYDRIVESYNC-WEBAPP
 - SKYDRIVE-LIVE
 - SKYDRIVE-API
 - SKYDRIVE-SECURESHARE
 - SKYDRIVE-SKYGFX
 - SKYDRIVE-STORAGE
 - SKYDRIVE-STORAGE2

| Enhancements in 10.31.01.0048 | |
|--------------------------------------|---|
| wns0017227 | Enhanced channel plan logic such that changing the radio mode or channel width does not reset it to 'Auto'. |
| 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. |
| wns0017729 | Resolved 'AP Performance Report by Radio' columns sorting incorrectly. |
| wns0017631 | Added Country support for South Africa for the AP3912i-ROW |
| wns0017631 | Added Country support for South Africa for the AP3912i-ROW |
| wns0017632 | Added Country support for Chile for the AP3912i-ROW |
| wns0017633 | Added Country support for Philippines for the AP3912i-ROW |
| wns0017635 | Added Country support for China for the AP3912i-ROW |
| wns0017636 | Added Country support for Saudi Arabia for the AP3912i-ROW |
| wns0017637 | Added Country support for Jamaica for the AP3865e |
| wns0017680 | Added Country support for UAE for the AP3912i-ROW |
| wns0017715 | Added Country support for Antigua Barbuda for the AP3935i-ROW |
| wns0017716 | Added Country support for Antigua Barbuda for the AP3805i-ROW |
| wns0017717 | Added Country support for Kazakhstan for the AP3912i-ROW |
| wns0017913 | Added Country support for Uganda for AP3935i/e and the AP3965i/e models |
| wns0017730 | Added Antenna support WS-AO-DX07180N for the AP3965e |

| Enhancements in 10.21.03.0010 | |
|--------------------------------------|---|
| wns0017614 | Added support for Scalance W788C and W786C models |
| wns0017458 | Added support for AP3912i-ROW for Korea |

| Changes in 10.21.03.0010 | |
|---------------------------------|---|
| wns0015950 | Corrected debug statement that could create a stack overflow by printing a value out of bounds, resulting in instability of wireless appliance (controller). |
| 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. |
| 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. |
| 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. |
| wns0017218 | Corrected issue with importing of MAC Blacklists, by improving serialization logic to better handle special characters in MAC listings. |
| wns0017289 | Corrected WEP key initialization logic that could prevent correct establishment with clients using Key Index 4 |
| wns0017291 | Improved logic for handling of malformed small frames to protect from possible memory corruption leading to platform instability. |
| wns0017306 | Updated device fingerprint signature to correctly identify "Unify OpenStage WL3" phones |
| wns0017380 | Improved session management logic to protect against possible incorrect radio references, which could result in system instability. |
| wns0016421 | Improved support for Policy MIB and etsysPolicyHttpRedirect to facilitate HTTP redirect policy definitions from ExtremeManagement™ 8.01 |

| Enhancements in 10.21.02.0017 | |
|--------------------------------------|---|
| wns0016942 | Update for AP3912 configuration and statistics modules to allow cloud support |
| wns0016891 | Improve Auto-Channel Selection coordination for ExtremeCloud™ deployments |
| wns0016943 | Enable support for MAC Based authentication and Captive Portal on AP3912i wired ports. Note: Support for 802.1x on the port will be provided into a later release. |
| wns0013138 | Added Country Support for AP3935 for Costa Rica |
| wns0017271 | Added Country support for Trinidad & Tobago for AP3935i-ROW |
| wns0017272 | Added Country support for Dominican Republic for AP3935i-ROW |
| wns0017273 | Added Country support for Trinidad & Tobago for AP3805i-ROW |
| wns0017274 | Added Country support for Philippines for AP3805i-ROW |
| wns0017275 | Added Country support for Costa Rica for AP3805i variants (AP3805i/e, AP3805i-ROW) |
| wns0017295 | Added Country Support for AP3965 for Costa Rica |
| wns0017265 | Added Country support for Taiwan for AP3912i-ROW |
| wns0017266 | Added Country support for Russia for AP3912i-ROW |
| wns0017267 | Added Country support for Qatar for AP3912i-ROW |
| wns0017268 | Added Country support for Kuwait for AP3912i-ROW |
| wns0017269 | Added Country support for Peru for AP3912i-ROW |
| wns0017270 | Added Country support for Malaysia for AP3912i-ROW |
| wns0017276 | Added Channels 52-144 (DFS Channels) for Colombia for AP3912i-FCC |
| wns0017277 | Added Channels 52-144 (DFS Channels) for Puerto Rico for AP3912i-FCC |
| wns0017278 | Added Channels 52-144 (DFS Channels) for United States for AP3912i-FCC |
| wns0017281 | Added Country support for Hong Kong for AP3912i-ROW |
| wns0017296 | Added Country Support for AP3912i-ROW for Costa Rica |

| Changes in 10.21.02.0017 | |
|--|---|
| wns0014750 | Adjusted client association management logic to improve buffer management for disconnecting devices. |
| wns0016281 | Optimized AP discovery method to account for low MTU links. |
| wns0016897 | Corrected issue with configuration of Band Preference/Load Control for Sites deployments. |
| wns0016947 | Addressed antenna port assignment logic on AP3805 for non-populated port configurations. |
| wns0017037 | Corrected the problem in the Edit AP dialog. After an auto channel selection, it was possible for the AP Radio to show as “scanning” for a long time and never exit this state. To resolve this, the AP had to be rebooted. |
| wns0017125 | Enforced inclusion of local reference address for NAS-IP-Address when doing local RADIUS authentication in Sites mode. |
| wns0017185 | Addressed AP Multi-Edit race condition for Auto-Channel Selection (ACS) configuration that could cause radio to become non-responsive. |
| wns0017187 | Corrected issued with propagation of AP tunnel state to peer Controller in High-Availability (HA). |
| wns0017217 | Improved performance for handling of fragmented frames in Secure Data tunnel. |
| wns0017279 | Improved compatibility with Ascom Phones i62 for power management frames when aggregation enabled. |
| wns0017179 wns0017301 wns0017318 wns0017228 | Improved performance of SNMP agent to handle large volume of configuration transactions. |

| Enhancements in 10.21.01.0065 | |
|--------------------------------------|---|
| wns014359 | <p>Introduce support for AP3912i, Wall-Plate, 802.11ac Wave 2, up to 1.17Gbps capacity, dual radio, 2x2:2, integrated BTLE/802.15.4 radio. 10.21.01 is the minimum release version of this access point.</p> <p>Extends foundational flow-based architecture to the AP3912i wireless AND wired ports, providing insight and control without impacting network performance in an easy to install package.</p> <p>Support default policy enforcement on wired ports. Policy assignment modeled as wireless service provides consistent enforcement for wireless and wired users.</p> <p>Ubiquitous reporting of wired and wireless clients. Same metrics capability for wired clients, including application visibility reporting and device fingerprinting</p> <p>Supports Control and Data encryption up to 150 Mbps.</p> |
| wns015804 | <p>Introduces IPFIX support for statistics reporting on network and application response times in distributed and centralized modes improving network efficiency and simplifying integration with ExtremeAnalytics</p> <p>Deprecates Mirror-N based method for ExtremeAnalytics integration. IPFix delivers metrics directly to Analytics engine via the Netflow feed. Requires ExtremeAnalytics 7.0.8.</p> |
| wns0015695 | <p>Refreshed client representation into full unified list with user definable criteria</p> <p>Visual indication of 802.11w/PMF capability for associated clients</p> <p>Provide per user Round Trip Time (RTT) metrics split for wireless and network contribution.</p> |
| wns0015822 | <p>Introduce per AP dashboard on operational metrics, including RF configuration, client load representation, channel occupancy and noise floor.</p> |
| wns0015803 | <p>Extends market-leading Extreme Policy with support for Domain Name System (DNS) based rules; reduces rule complexity, improves security, while simplifying integration with external Guest Service applications.</p> |
| wns0016211 | <p>Introduces support for fall through L7 deny rules as well as Wild Cards and Unknown Groups rule sets; reduces management complexity and provides greater flexibility for L7 based policies.</p> |
| wns0016148 | <p>Doubles the maximum session capacity of the V2110 on VMware to 8,192 concurrent sessions per appliance and a total of 16,384 sessions in high-availability mode.</p> |
| wns0014422 | <p>Introduces native integration with Centrak Real-Time Location System (RTLs) for value added location based services.</p> |
| wns005741 | <p>Channel inspector report provides RF assessment for channel configuration, including CoChannel, adjacency and overlapping SSID configurations for the wireless band from the perspective of a particular AP, helpful to determine congestion or other RF interference related diagnostics.</p> |
| wns0015801 | <p>Enhances Firewall Friendly Captive Portal (FFCEP) at AP to support user authentication via RADIUS from a response to FFCEP credentials. AP ETH MAC address and AP Location added as variables to FFCEP exchange.</p> |

| Changes in 10.11.05.0005 | |
|---------------------------------|--|
| wns0016280 wns0016353 | Enhanced power save mode logic to improve client wake-up. |
| 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. |
| wns0016584 | Improved configuration logic for deploying FFECF and 802.1x which could result in failure to redirect user. |
| wns0016592 | Corrected noise floor level reporting. |
| wns0016777 | Improved probe suppression logic for when RSS is low to release client instead of sending de-auth. |
| wns0016906 | Addressed Potential Vulnerability of AP/Controller in CVE-2016-5195. |
| wns0016955 wns0017019 | Addressed condition where small encrypted 802.11g frames could affect stability for AP3900. |
| wns0016986 | Improved SSH key management logic to regenerate keys on restart. |

| Changes in 10.11.04.0008 | |
|---------------------------------|--|
| wns0014331 | Addressed protection mode logic to improve compatibility with Motorola Scanner connecting to 2.4Ghz radio. |
| wns0016159 wns0016366 | Improved logic for client de-authentication that could affect stability during generation of 802.11k Neighborhood reports. |
| wns0016175 | Improved stability by adding prevention for invalid topology ID. |
| wns0016198 | Corrected issue that could cause AP to apply wrong role to client while in Site mode. |
| wns0016226 | Improved configuration import logic to prompt user to re-enter corrupted Radius Secret values instead of halting import process. |
| wns0016269 | Improved memory management in SNMPAgent to improve stability. |
| wns0016298 | Addressed race condition in client disassociating during a failover event that could corrupt session tables. |
| wns0016364 | Correct logic of multicast-to-unicast conversion to improve stability of AP39xx series APs when serving slow clients. |
| wns0016347 | Improved logic for logging function to prevent log file from being flooded. |
| wns0016390 | Addressed use case for VNS Wizard when using role based redirection. |
| wns0016450 | Improved stability for look up on missing rates. |

| Enhancements in 10.11.04.0008 | |
|--------------------------------------|--|
| wns0011752 | Log recommendation for user to change AP default Password every 30 days. |
| wns0012837 | Added support for AP3825i in Uganda. |
| wns0016453 | Added country support for Taiwan for AP3805i-ROW. |
| wns0016454 | Added country support for Argentina for AP3805i-ROW. |
| wns0016455 | Added country support for Korea (ROC) for AP3805i-ROW. |
| wns0016456 | Added country support for South Africa for AP3805i-ROW. |
| wns0016457 | Added country support for Serbia for AP3825i/e. |

| Enhancements in 10.11.03.0004 | |
|--------------------------------------|--|
| wns0015680 | Added Country Support for Kazakhstan for AP3965i/e_ROW. |
| wns0016062 | Added country support for Russia for AP3965i/e-ROW. |
| wns0016063 | Added Country Support for Brazil for AP3935i/e_ROW. |
| wns0016064 | Added Country Support for Brazil for AP3965i/e_ROW. |
| wns0016065 | Added Country Support for Mexico for AP3805i_ROW. |
| 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. |
| wns0016073 | Added country support for Brazil for AP3805i-ROW. |
| wns0016074 | Added Country Support for Nicaragua for AP3935i/e-ROW. |
| wns0016075 | Added Country Support for Nicaragua for AP3965i/e-ROW. |

| Changes in 10.11.03.0004 | |
|---------------------------------|--|
| wns0015352 | Adjusted parsing logic of RADIUS attributes to avoid stripping of domain name information for Captive Portal Authentication. |
| wns0015593 | Enhanced Guest account management interface to support multi-edit for Account lifetime. |
| wns0015807 | Improved packet processing logic for core assignment to address possible instability during high-rate flows on wave2 Access points. |
| wns0015880 | Corrected endianness conversion issue that could cause malfunction of Mac Based Authentication (MBA) for AP39xx models. |
| wns0015950 | Corrected debug statement that could create a stack overflow by printing a value out of bounds, resulting in instability of wireless appliance (controller). |
| wns0015963 | Corrected inclusion logic of Class attribute on Radius Accounting for 802.1x networks in 10.11.x software. |
| wns0015980 | Improved logic in Deep Packet Inspection (DPI) Engine to address possible instability when Application Visibility enabled for a WLAN service under high traffic loads. |

| | |
|------------|---|
| wns0016013 | Corrected issue with reporting of user statistics by Access Points, which could result in inadvertent idle timeout of registered devices. |
|------------|---|

| Enhancements in 10.11.02.0032 | |
|--------------------------------------|--|
| Software | |
| | Introducing IPv6 support for Bridge at Wireless Controller and Tunnel at Wireless Controller topology with IPv6 filter rules and IPv6 Proxy support. |
| | Added support for time-based subscription licenses when integrated with ExtremeManagement. |
| | Introducing the WS-AP3935i-IL, Indoor Wave 2 for Israel under the ROW regulatory domain. |
| | Introducing a GUI page for AP38xx/37xx to provide support for the Dräger Certification. |
| | Provide Warning in AP Grouping's WLAN Config quick action. |
| | Replaced throughput pie chart with historical throughput chart from user selectable application groups. |
| | Adding IGMP on AP37xx/AP38xx/AP39xx including support for IGMP V3 Multicast Group Registration and IGMP V2 Query/Report. |
| wns0013111 | Added country support for Korea for the AP3935i/e-ROW. |
| wns0015674 | Added country support for Kazakhstan for the AP3825i/e under ROW regulatory domain. |
| wns0015675 | Added country support for Kazakhstan for the AP3805i/e under ROW regulatory domain. |
| wns0015676 | Added country support for Kazakhstan for the AP3801i under ROW regulatory domain. |
| wns0015677 | Added country support for Kazakhstan for the AP3865e under ROW regulatory domain. |
| wns0015678 | Added country support for Kazakhstan for the AP3805i-ROW. |
| wns0015679 | Added country support for Kazakhstan for the AP3935i/e-ROW. |
| wns0015680 | Added country support for Kazakhstan for the AP3965i/e-ROW. |
| wns0015681 | Added country support for Chile for the AP3805i-ROW. |
| wns0015682 | Added country support for Russia for the AP3805i-ROW. |
| wns0015683 | Added country support for Georgia for the AP3805i-ROW. |
| wns0014684 | Added country support for Ecuador for the AP3805i-ROW. |
| wns0015685 | Added country support for Ecuador for the AP3965i-ROW. |
| wns0015748 | Added country support for Korea for AP3965i-ROW and AP3965e-ROW. |
| wns0015752 | Added support for DEMO for AP3935i-IL. |

| Changes in 10.11.02.0032 | |
|---------------------------------|---|
| wns0012777 | Optimized background scanning algorithm to improve stability of AP3800 series APs |
| wns0015281 | Addressed issue with limited connectivity for Intel Clients. See known issues for other cases |
| wns0012074 | Updated V2110 network device drivers to improve stability and host interoperability |
| wns0015550 | Improved logic to recover from possible radio stalling during configuration. |
| wns0014589 | Corrected user guide to correct description of CSV fields that carry user session lifetime. |
| wns0015121 | Addressed issue with packet fragmentation logic on AP3935 which could affect Client connections over VPN |
| wns0015715 | Corrected issue with handling of HTTPS for Captive Portal redirection |
| wns0014382 | Updated packet buffer handler to address message corruption for secure tunnel connections |
| wns0015436 | Adjusted radio logic handling to protect against aggressive client behavior of frequent changes in Power-Save mode for mixed client environments. |

| 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 | |
| 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 Added 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. |
| wns0015206 | Addressed possible instability for AP3800 series devices in handling of client connectivity management features (Steering, Balance, Probe Suppression) |

| 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 |

| Enhancements in 10.01.05.0008 | |
|--------------------------------------|--|
| 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. |

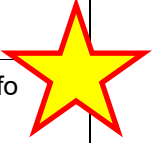
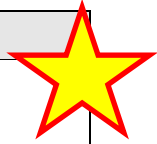
| Changes in 10.01.02.0038 | |
|---------------------------------|---|
| wns0011674 | Corrected a problem when the controller was no longer reachable via SMTPv3 if the user set a password with special characters. |
| wns0012997 | Restricted transmission of Ethernet pause frames on the AP3805i. |
| wns0012007 | 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. | |
| Added 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>Intel AC8265 client card sometimes fails to authenticate with AP (11r & MFP enabled) This is a Microsoft Windows 10 supplicant (Win Zero) issue. Will be fixed in Windows 10 – 19H1 release.</p> | <p>Info</p> |
| <p>If using Standard SSID->Hotspot->Enabled, prior to upgrading to 10.51 please ensure that the description fields for language configuration are not left blank in your Service Provider Settings.</p> | <p>wns0021808 -- Info</p> |
| <p>iPad clients may experience issues receiving IP address via DHCP as a result of 'Admission Control' being enabled within a WLAN Service. It is recommended to disable ALL 'Admission Control' options if iPad clients are expected to associate to the WLAN.</p> | <p>wns0021217 -- Info</p> |
| <p>Known Issue for AP3825: Disable MFP if clients are experiencing connectivity issues due to a poor signal (rule of thumb). Only a specific corner case issue was fixed in wns0020142. Different clients are behaving different when MFP is enable.</p> | <p>wns0020142 -- Info</p> |
| <p>Some wireless clients may experience connectivity issues with MFP and/or FT enabled. (They will not complete the 4-way handshake in order to complete the association process.)</p> <ul style="list-style-type: none"> • Qualcomm Killer Wireless 1535 -- driver Qualcomm Atheros Communication Inc., version 12.0.0.448 • Intel Dual Band Wireless-AC 8265 – driver Intel 19.50.1.5 • Intel Dual Band Wireless-AC 8260 – driver Intel 18.40.2.3 | <p>wns0020429 – Info</p> |
| <p>Vulnerability Notice: VN 2018-001 (CVE-2017-5715, CVE-2017-5753 - Spectre) VN 2018-002 (CVE-2017-5754 - Meltdown)</p> <p>ExtremeWireless controllers and Access Points are not vulnerable. User cannot execute externally crafted programs under normal operating conditions.</p> | <p>Info</p> |
| <p>IoT iBeacon Scan configuration</p> <p>If enabling the iBeacon Scanner function for AP391x models, it's not recommended to configure a Scanner Window (Dwell Time) that is larger than 80% of the configured Scan Interval. Doing so may lead to instability of the scanning function. This is a temporary restriction and will be addressed in an upcoming release.</p> | <p>Info</p> |
| <p>Vulnerability Notice 2017-005 - KRACK, WPA2 Protocol Flaw (client side responsibilities)</p> <p>The Software updates released with 10.41.01.0082 protect the infrastructure side (AP) from exploitation. However, wireless clients may still be vulnerable until their drivers are updated. Please contact the client software vendor for driver updates related to addressing these vulnerabilities related WPAv2 key management.</p> | <p>Info</p> |



| | |
|---|--|
| <p>Some Intel WiFi clients fails to obtain an IP address after 'Resume from Sleep' mode. Fixed in latest Intel driver (July 2017). For more information, see: https://downloadmirror.intel.com/26924/eng/ReleaseNotes_WiFi_19_70_0.pdf</p> | <p>Info</p> |
| <p>Some devices are not connecting to a WPA2-PSK service when Management Frame Protection (MFP) is enabled. See KB for more information: https://gtacknowledge.extremenetworks.com/articles/Solution/Certain-devices-not-connecting-to-WPA2-PSK-on-5ghz-radio-when-Management-Frame-Protection-is-enabled</p> | <p>Info</p> |
| <p>When using the CLI to configure the URL for the Hotspot, the command line only accepts the "https://". Use the GUI page to enter the URL of "http://".</p> | <p>wns0019160 - Info</p> |
| <p>The camera module for the AP3916ic operates under its own firmware. Camera firmware upgrade is integrated within ExtremeWireless™ firmware images and is managed by the ExtremeWireless™ appliance. If the firmware upgrade of an AP3916ic camera is deemed to have failed (see AP logs), remotely perform an admin reboot the AP (UI or CLI). The rebooting will re-start the camera's firmware upgrade process and the issue will be corrected. Camera firmware upgrade failures are uncommon, but could be experienced during the upgrade of an AP3916ic connected through mesh.</p> | <p>wns0019127 - Info</p> |
| <p>When the AP is configured on both availability pairs, the AP SSH password must be the same on both controllers. This is to endure that when the AP fails over to the secondary controller, the remote console will not be denied on the secondary controller.</p> | <p>wns0019148 - Info</p> |
| <p>When the AP is functioning as a WDS/MESH child/repeater, the remote packet capture function is not supported in V10.41.01.80.</p> | <p>wns0019188 - Info</p> |
| <p>L7 Policy does not block Sky Go on smartphones or tablets.</p> <p>Workaround:</p> <ul style="list-style-type: none"> • Create custom web filter for Sky Go. • Add the following URLs: <ul style="list-style-type: none"> • name = sky_go_1 matching pattern = .sky. • name = sky_go_2 matching pattern = skylivehls.cdn.fastweb. • name = sky_go_3 matching pattern = .skycdn. <p>Note: Periods must be included.</p> <p>See also the KB: https://gtacknowledge.extremenetworks.com/articles/Solution/L7-Policy-does-not-block-Sky-Go-on-smartphones-or-tablets</p> | <p>wns0018022 - Info</p> |
| <p>If the tagged VLAN ID of a "Bridge Traffic Locally at AP" VNS topology is changed, the associated WLAN Service forwards traffic for both the original and new VLAN ID.</p> <p>Workaround: AP needs to be rebooted after changing VLAN ID.</p> | <p>wns0017485 - Info</p> |
| <p>After upgrade to V10.31.01, the Locator may not display all the APs properly in an HA configuration. Restart the Locator by disabling and enabling the location engine. This will solve the issue and result is the APs displaying properly.</p> | <p>wns0017681 Fixed in 10.31.03.0012</p> |

| | |
|---|--------------------------|
| <p>For 802.11n/2.4 GHz clients LDPC will be disabled by the AP firmware even though the LDPC has been selected from the GUI and the LDPC bit is set in the association response packet sent by the AP. This has no known impact on connectivity and there will be no "L" in the client report's protocol column.</p> | <p>wns0017831 - Info</p> |
| <p>When the WDS or MESH service is configured on the radio and deployed as either a child or as a parent with active children, the on demand radio scan should not be performed on the radio under the Channel Inspector Report.</p> | <p>wns0017906 - Info</p> |
| <p>Even though users typically perceive a popular website or application as a unified destination, the reality is that most modern applications and websites utilize a web of service providers in the background to deliver their presentation layer and specific user experience. Often these websites rely on content that is being sourced from other established service providers such as content delivery networks. Most often, these engagements by the application or browser are interchanges with URLs that bear no resemblance to the application using them. As such, during a particular application interaction, only certain flows may be in reference to the well-known application name whereas others may be referring activity that is not generically associated with well-known service.</p> <p>L7 application filtering works by specifically fingerprinting a flow or set of flows based on its specific fingerprint, such as destination URL or authentication certificates. Some of those flows will be specifically addressed to the parent applications servers (such as Facebook.com) but other flows in the same exchange, relate to exchanges with other non-application specific service providers or content delivery networks (such as akamai.com). Each flow is identified on its own and the DPI is unable to correlate whether they're associated with the same presentation layer (user experience). Furthermore, these associations can vary for such considerations such as access geography or other business partnerships between application and content providers.</p> <p>As such, when defining and applying Layer 7 (L7) application or DNS based policy to allow or constrain specific applications (such as Facebook), in order to complete the user experience, user must be aware of the corresponding additional relationships that may need to be referenced by the that policy definition. For example, a definition to allow a typical Facebook experience, the user must craft policy that includes not only the traffic to the main site, but also the peripheral traffic for base content providers. For a North America's web login experience, the typical policy needs to allow:</p> <ul style="list-style-type: none"> • *.fbcdn.net (e.g. static.xx.fbcdn.net,scontent.xx.fbcdn.net,scontent.fsnc1-2.fna.fbcdn.net, ...) • *.facebook.com (www.facebook.com, m.facebook.com, staticxx.facebook.com) • cs.atdmt.com • *.doubleclick.net (googleads.g.doubleclick.net) • *.akamaihd.net (maybe obsolete) • *.facebook.net (maybe obsolete) <p>To determine full list on a per-application basis, customers should assess a network trace for their environment.</p> | <p>wns0017055 - Info</p> |

| | |
|--|---|
| <p>In a High Availability scenario when changing simultaneously two WLAN port assignments for two different AP ports, from the AP configuration page the WLAN assignment will not be synchronized for the second pair, resulting in a configuration mismatch. To prevent this situation, the assignment change must be done one WLAN at the time.</p> | <p>wns0017364 - Info</p> |
| <p>Old versions of FreeRadius are not working with Windows 8 and 10 clients. This is a FreeRadius limitation. To resolve this issue, a new version of FreeRadius is required to be installed. The problem was verified to be resolved with version 3.0.2 of FreeRadius.</p> | <p>wns0016966 - Info</p> |
| <p>For application filtering, a hostname based FQDN L7 has been identified as follows: If both a signature based L7 filter rule and a hostname based L7 filter rule match, the hostname based L7 filter rule will take precedence. If a hostname based FQDN entry is defined in "Custom Web Applications", even it's not used by any filter rules, it will still take precedence. Therefore, the corresponding regular L7 application will not match. This problem will be addressed in a future release.</p> | <p>wns0017012 - Info</p> |
| <p>Modern web pages are constructed using tools, scripts, and links from external sites. For example, loading the "extremenetworks.com" page involves loading from extreme networks domain plus 16 other external domains like (googleapis.com, cdn.optimizely.com, code.jquery.com, fonts.gstatic.com, ...).</p> <p>In order to write filters to allow "extremenetworks.com" page to load and block other pages, one must analyzes the web page contents carefully and add L7 filters to allow all other external domains that the page fetches data from, not just the extremenetowrks.com domain.</p> | <p>wns0017055 - Info</p> |
| <p>For an IPv6 topology, to ensure clients get DNS entry into their interface configuration, under Topology/multicast configuration IPv6multicast a rule has to be added; this could be added in the list of well-known multicast groups.</p> | <p>wns0015806 - Info</p> |
| <p>For the dpi-sensor to classify the flow properly, it is recommended that a filter rule to block QUIC protocol (udp port 443) is added.</p> | <p>wns0017040 - Info</p> |
| <p>For AP3912i the wired ports and the AP3916ic's CAM function are represented as radios. Service assignment is modeled on WLAN service assignment. Client reporting is unified in the same tabular format. Wired clients are differentiated in the client report by Radio=Port# and protocol=802.3</p> | <p>wns0016770 - Info</p> |
| <p>If Clients on the wired port are deployed on the IPv6 network, all client on the wired ports should be assigned Roles that have same VLAN (default PVID or Contain VLAN).</p> | <p>wns0016501 - Info</p> |
| <p>It is MANDATORY that before performing the upgrade to release 10.11.xx and 10.21.xx the setting for the "SCSI controller" for a VMware virtual controller (V2110) is set to "Paravirtual". (Note that the default value is "BusLogic Parallel".)</p> <p>See also the KB: https://gtacknowledge.extremenetworks.com/articles/Solution/V2110-large-upgrade-to-v10</p> | <p>wns0015953 – Info wns0016244 – Info</p> |

| | |
|--|--------------------------|
| <p>The following cipher-suites have been obsoleted in release 10.01 as compared with the 9.21 release:DES-CBC3-MD5RC2-CBC-MD5DES-CBC-MD5EXP-EDH-RSA-DES-CBC-SHAEXP-EDH-DSS-DES-CBC-SHAEXP-DES-CBC-SHAEXP-RC2-CBC-MD5EXP-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> | <p>wns0013172 - Info</p> |
| <p>The client of the Intel AC7260 wireless chipset with the latest 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.</p> <p>This issue is fixed in Intel drivers 18.33.3.1 or 18.33.3.2 and above.</p> | <p>Info</p> |
| <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> | <p>wns0014608 - Info</p> |
| <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, because redirection triggers directly off the first frame (SYN) in the flow. 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> | <p>wns0014726 - Info</p> |
| <p>When configured to 100% Airtime, the Flexible Client Access (Airtime Fairness) feature is limited to 50 simultaneously transmitting clients per radio on AP3900 series models.</p> | <p>wns0015037 - Info</p> |
| <p>ExtremeWireless Virtual Appliance V2110 MS Hyper-V</p> <p>Performance is affected when Hyper-V controller ports are mapped to virtual ports of their server. We recommend mapping controller ports to physical ports. Clustering Hyper-V is not supported and should not be configured.</p> | <p>Info</p> |
| <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). This is because the prefix used in the Engine ID has been changed from Siemens to Extreme Networks.</p> | <p>wns0013973 – Info</p> |
| <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> | <p>wns0013397– Info</p> |
| <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> | <p>wns0013536– Info</p> |

| | |
|---|-------------------|
| Some versions of Apple Mac Books might exhibit low throughput performance when Management Frame Protection (PMF) is enabled. | wns0012889– Info |
| 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. | wns0012862– Info |
| The Access Point Name field can be up to 23 characters and must start with alpha characters, not numeric. | wns0012722 – Info |
| 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. | wns0012793 – Info |
| Countermeasures for honeypot AP threat may be less effective for the iPhone (with version 8.3) client device than other device types. | wns0012678 – Info |
| We recommend that you do not enable 802.11k along with the Quiet IE option for installations with Ascom i62 phones. | wns0012567– Info |
| Rogue AP Detection applies only 'Open" hotspots. Countermeasures can be enforced against other link-protected hotspots if designated as a threat. | wns0012296– Info |
| 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. | wns0011519 – Info |
| 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. | wns0011589 – Info |
| 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. | wns0011467– Info |
| 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'. | wns0011008– Info |
| The Chrome auto-complete function fills in fields incorrectly. Disable password saving and password field auto completion in a Chrome configuration. | wns0010642– Info |
| APs advertising the SSIDs of administratively disabled WLAN Services are not detected as internal honeypots until the WLAN Service is enabled. | wns0008740 – Info |
| 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. | wns0008979 - Info |
| When the AP is used in a WDS or Mesh service, the AP name must be under 32 characters. | wns0008035 - Info |

| | |
|---|--------------------------------------|
| On C5210, status on interface without physical transceivers plugged reported Up and Down. | wns0008023 - Info |
| AP filter stats for unicast packets is 0 | wns0018782 Fixed in 10.51.04.0009 |
| <p>Topology groups – Info</p> <p>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</p> <p>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. It is corrected in SW 10.8.4.</p> | |
| <p>Info</p> <p>The client of the Intel AC7260 wireless chipset with the latest drivers 18.32.x or 18.33.x may become unresponsive 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.</p> <p>This issue is fixed in Intel drivers 18.33.3.1 or 18.33.3.2 and above (latest driver is 18.33.6.2)</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. <code>eth0</code> is the wired interface, <code>wlan0</code> is the 5Ghz interface, and <code>wlan1</code> is the 2.4Ghz interface. • You have the option to capture bidirectional traffic on <code>eth0</code>, <code>wifi0</code>, and <code>wifi1</code>. The capture on <code>wifi0</code> and <code>wifi1</code> 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 |
| 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

Note

- 1) Required when AP to Controller communication is over unsecured WASSP tunnel
- 2) Always required (used by IKEv2 during AP registration, regardless of WASSP being secured or not)
- 3) Required only for Version 10.11 or older. Version 10.21 or newer use IKEv2 over 4500 for AP registration
- 4) Required only for Version 10.31 or older. Version 10.41 does image upgrade using HTTP over WASSP (secure and unsecured)
- 5) Required only for Version 10.31 or older. Controller Version 10.41 does trace collection using scp over WASSP (secure and unsecured)
- 6) Required for Version 10.31 or older. Controller Version 10.41 does AP remote login using ssh over WASSP (secure and unsecured).

| 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(1) |
| Access Point | Controller | UDP | Any | 13910 | WASSP | Management and Data Tunnel between AP and Controller | Yes(1) |
| Controller | Access Point | UDP | 4500 | Any | Secured WASSP | Management Tunnel between AP and Controller | Yes(2) |
| Access Point | Controller | UDP | Any | 4500 | Secured WASSP | Management Tunnel between AP and Controller | Yes(2) |
| Access Point | Controller | UDP | Any | 13907 | WASSP | AP Registration to Controller | Optional (3) |
| 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(4) |
| Access Point | Controller | TCP/UDP | Any | 69 | TFTP | AP image transfer | Yes(4) |
| Controller | Access Point | TCP/UDP | Any | 22 | SCP | AP traces | Yes(5) |
| 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 (6) |

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 |
| Controller | Any | 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 |
| 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 |

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: <https://extremeportal.force.com/> . 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 V10.41 software release:

Windows 10

| Device | Model | Driver | Radio |
|-----------------|-----------------|----------------|------------|
| Intel | AC-7260 | 18.33.6.2 | a/b/g/n/ac |
| Microsoft Lumia | 950 xl dual sim | 10.0.10586.11 | a/b/g/n/ac |
| Microsoft Lumia | 830 | 10.0.15063.251 | a/b/g/n/ac |

List of New Mobile Devices Tested

| Model | OS | Driver Version | OPEN | WEP | WPA/P SK | WPA 2/PS K | OKC | 11r | 11k | 11ac strict | MU-MIMO | PMF |
|------------------------|-----------------------|----------------|------|-----|----------|------------|-----|-----|---------------|-------------|---------|-----|
| iPhone 8 | iOS 11.0.1 | | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| Samsung Galaxy S8 Edge | | | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Macbook Pro | macOS Sierra(10.12.6) | | Yes | Yes | Yes | Yes | n/a | n/a | Not Supported | Yes | No | Yes |

| | | | | | | | | | | | | |
|------------------------|------------|---------------|-----|-----|-----|-----|-----|-----|-----|-----|----|-----|
| Microsoft Surface Book | Windows 10 | 15.68.9046.79 | Yes | Yes | Yes | Yes | Yes | n/a | n/a | Yes | No | Yes |
| Microsoft Surface Pro | Windows 10 | 15.68.9114.29 | Yes | Yes | Yes | Yes | Yes | Yes | n/a | Yes | No | Yes |

11ac MU-MIMO

| Device | Model | Driver | 1x Support | Radio | 11ac Strict | MU-MIMO |
|-----------------|---|-------------------|------------|---------|-------------|-------------|
| Google Nexus | Nexus 5x | Android 6.0 | Yes | abgn+ac | Yes | 2x2 MU-MIMO |
| Microsoft Lumia | Lumia 950 | Windows 10 Mobile | Yes | abgn+ac | No | 2x2 MU-MIMO |
| Microsoft Lumia | Lumia 950XL | Windows 10 Mobile | Yes | abgn+ac | No | 2x2 MU-MIMO |
| Dell Alienware | Dell Alienware with Killer Wireless- 1535 | Windows 10 | Yes | abgn+ac | No | 2x2 MU-MIMO |
| Linksys | USB AC600 | | Yes | abgn+ac | No | 1x1 MU-MIMO |
| Acer PC | Acer Aspire E5 with Qualcomm Atheros QCA9377 | Windows 10 | Yes | abgn+ac | No | 1x1 MU-MIMO |
| Acer PC | Acer Aspire E15 with Qualcomm Atheros QCA9377 | Windows 10 | Yes | abgn+ac | No | 1x1 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 |

| Client | Driver Version | Test Case | Build | Result |
|--------------------|---|------------------|-------|--------|
| 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 Lumia 830 | | Win8.1 Win 10 | 802.11abgnac |
| Polycom Spectralink | 8440 | | |
| Samsung | Galaxy Note4 | Android v5.0.1 | a/b/g/n/ac |
| Surface 3 Pro | | Win 10 (all builds) | Marvel Avastar 802.11 ac |
| Surface 4 Pro | | 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 |

| Vendor | Model OS | Version |
|--------------------------|---|---|
| Intel® | Intel PRO Set/Wireless | Version 13.0.0.x (with Windows® Intel® driver version 13.0.0.x) |
| Microsoft® Wireless Zero | Windows 7, 8, 8.1 Pro, 10 Pro Windows Phone 8.1, Windows Mobile 10 | provided with Windows® |

LAN SWITCHES

| Vendor | Model OS | Version | Tested with |
|---------|---------------------------------|---|--------------------------------------|
| Avaya | VSP-4850GTS-PWR | (6.0.1.1_B003) (PRIVATE) HW Base: ERS 4850 | Fabric Attach |
| Avaya | VSP-4850GTS-PWR | ((6.1.0.0_B030) (PRIVATE) HW Base: VSP 4850 | Fabric Attach |
| Avaya | Ethernet Routing Switch 3626GTS | + HW:01 FW:6.0.0.3 SW:v6.0.0.007 BN:07 | Fabric Attach |
| 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 |
| Extreme | X-460-G2 | | 802.3at interoperability with AP3935 |
| | 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 |

| Attribute | RFC Source |
|--------------------|------------------------------|
| Service-Type | RFC 2865, RFC 3580 |
| Session-Timeout | RFC 2865 |
| State | RFC 2865 |
| Termination-Action | RFC 2865, RFC 3580 |
| Tunnel Attributes | RFC 2867, RFC 2868, RFC 3580 |
| User-Name | RFC 2865, RFC 3580 |
| Vendor-Specific | RFC 2865 |

RADIUS Accounting Attributes

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

GLOBAL SUPPORT:

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

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

By Email: support@extremenetworks.com

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

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

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/