Extreme Networks® IdentiFi ™ Wireless Convergence Software

Software Version 9.15.05.0007

March 27, 2015

INTRODUCTION:

This document provides specific information for this version of software for the Extreme Networks® IdentiFi ™ Wireless Convergence Software.

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

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

Firmware Specification:

Status	Version No.	Type	Release Date
Current Version	9.15.05.0007	Maintenance Release	March 27, 2015
Previous Version	9.15.04.0011	Maintenance Release	February 27, 2015
Previous Version	9.15.03.0005	Maintenance Release	January 23, 2015
Previous Version	9.15.02.0009	Maintenance Release	December 15, 2014
Previous Version	9.15.01.0121	Feature Release	November 17, 2014
Previous Version	9.12.04.0003	Maintenance Release	October 09, 2014
Previous Version	9.12.03.0009	Maintenance Release	September 12, 2014
Previous Version	9.12.02.0006	Maintenance Release	July 25, 2014
Previous Version	9.12.01.0067	Feature Release	June 26, 2014
Previous Version	9.01.03.0008	Maintenance Release	May 30, 2014
Previous Version	9.01.02.0017	Maintenance Release	April 25, 2014
Previous Version	9.01.01.0228	Feature Release	March 31, 2014

SUPPORTED CONTROLLERS AND ACCESS POINTS

This Extreme Networks® IdentiFi ™ Wireless Convergence Software version supports the following controllers and access points:

Product	Image
IdentiFi Wireless Controller C4110	AC-MV-09.15.05.0007-1.gxe
IdentiFi Wireless Controller C5110	AC-MV-09.15.05.0007-1.txe
IdentiFi Wireless Controller C5210	AC-MV-09.15.05.0007-1.rue
IdentiFi Wireless Controller C25	AC-MV-09.15.05.0007-1.pfe
IdentiFi Wireless Virtual Appliance V2110 VMware	AC-MV-09.15.05.0007-1.bge

IdentiFi Wireless Virtual Appliance V2110 MS Hyper-V	AC-MV-09.15.05.0007-1.ize
Wireless AP3805i – internal antenna model only	AP3805-09.15.05.0007.img
Wireless AP3865	AP3825-09.15.05.0007.img
Wireless AP3825	AP3825-09.15.05.0007.img
Wireless AP3715	AP3715-09.15.05.0007.img
Wireless AP3710	AP3710-09.15.05.0007.img
Wireless AP3705	AP3705-09.15.05.0007.img
Wireless AP3765	W78XC-2-09.15.05.0007.img
Wireless AP3767	
Wireless AP3605	AP3600-09.15.05.0007.img
Wireless AP3610	
Wireless AP3620	
Wireless AP3630 (thin mode)	
Wireless AP3640 (thin mode)	
Wireless Outdoor AP3660	
Wireless AP2605	AP200-09.15.05.0007.img
Wireless AP2610	
Wireless AP2620	
Wireless AP2630 (thin mode)	
Wireless AP2640 (thin mode)	
Wireless Outdoor AP2650	AP2650-09.15.05.0007.img
Wireless Outdoor AP2660	
Wireless AP4102 (thin mode)	AP4102-09.15.05.0007.img

INSTALLATION INFORMATION

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

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

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

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

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

- vSphere High Availability (HA). Release 9.12.01 adds support for vSphere application level HA monitoring. This provides protection comparable to that offered by the hardware watchdog timer on the hardware wireless controllers.
- vSphere vMotion. vMotion involves moving a running virtual machine (VM) from one host to another within a cluster with minimal or no service interruption.
- vSphere Dynamic Resource Scheduling (DRS) and Dynamic Power Management (DPM). These features monitor host utilization and use vMotion to migrate VMs to different hosts based on power management and resource utilization goals.
- Storage vMotion. Storage vMotion allows the administrator to move a VM's disks to different host servers while the VM is running.
- Cold migration – The V2110 supports cold migration subject to the requirement that the V2110 is migrated in a shutdown state not in a suspended state.
- Distributed Virtual Switches (DVS). A DVS is a virtual switch that spans multiple physical hosts. VMs migrated between hosts sharing a DVS retain their network point of presence and addresses. Customers who expect to vMotion V2110s frequently should deploy DVSs if possible.
- The V2110 has supported the virtual serial port and virtual serial port concentrator features since its first release. This support continues in release 9.15.01. VMware requires the customer to purchase licenses in order to use this feature.

The release 9.15.01 V2110 does not support the vSphere Fault Tolerance feature. This feature is only available to VMs that require only one virtual core. This is a VMware restriction.

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

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

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

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

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

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

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

Note: Upgrading Virtual Appliance V2110 VMware to the current release

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

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

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

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

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

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

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

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

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

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

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

Note: In case of upgrade to V9.15, if an existing VNS has WMM disabled only legacy clients will be serviced until WMM is enabled.

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

Note: During the first upgrade from pre-v9.01 to V9.15 all filtering rule will fail the Policy Manager verification. The newly upgraded controller will require a policy enforcement from Policy Manager to fix it. After this, any additional verification and enforcement will be always handled normally. Upgrades from v9.01 or later version will not have this problem.

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

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

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

Note: Deployment and configuration advice for AP2660

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

NETWORK MANAGEMENT SOFTWARE SUPPORT:

Network Management Suite (NMS)	Version No.
Extreme Networks NetSight and Wireless Manager	6.1 or higher*
Extreme Networks NetSight Wireless Advanced Services	4.4
Extreme Networks NAC	6.1 or higher

* You can use NetSight 6.1 or higher to manage your V9.15 controllers, but to take advantage of any V9.15 specific features, NetSight 6.2 is required.

EXTREME NETWORKS WIRELESS V8 TO V9 REQUESTS FOR NEW LICENSE KEYS

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

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

To request a new V9 license key:

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

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

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

NEW FEATURES, SOFTWARE CHANGES, AND ENHANCEMENTS

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

Enhancements in 9.15.04.0011
wns0010732 Added country support for Philippine for AP3705i, AP3715i/e and AP3825i/e
wns0011161 Add support for FCC UNII bands 1 & 4 to AP3865e model
wns0011762 Added country support for Chile for AP3825i and AP3825e
wns0011763 Added country support for Singapore for AP3805i/e
wns0011771 Added country support for Philippines for AP3805i
wns0011772 Added country support for Philippines for AP3865e
wns0011776 Added country support for India for AP3805i/e

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

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

Changes in 9.15.03.0005	
wns0011239	Corrected an issue with the Radius accounting process which causes excessive logs for clients with multiple sessions.
wns0011455	Improved editing of the guest user UI page by creating a drop down menu for year selection.
wns0011517	Corrected an issue with the Guest splash page to prevent users from entering any embedded code in the username field.
wns0011626 wns0011523	Corrected a memory management issue in certain high-density deployments with the AP37xx or AP36xx
wns0011543	Corrected an issue that caused under reporting of topology data traffic volume.
wns0011574	Corrected an issue causing a stale NAS-IP address field to be used in Radius authentication messages after a change in the controller IP address.
wns0011595	Corrected an issue that allowed policy incapable AP26xx to pass all traffic in a policy enabled environment
wns0011612	Corrected an issue that was causing the Ekahau server IP address to display incorrectly for location services.
wns0011620	Improved the handling of https redirection for authentication by auto updating required policy parameters.
wns0011642	Improved handling of Unicode characters in the username field
wns0011647	Corrected an instability issue in 9.15.02.0009 with AP36xx caused when a corrupted frame is received.

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

Enhancements in 9.15.02.0009
wns0011501 Add support for Hong Kong in ROW regulatory domain for the AP3865e
wns0011502 Add support for UAE in ROW regulatory domain for the AP3865e
wns0011527 Add Support for Barbados in NAM regulatory domain for the AP3825i/e and the AP3865e
wns0011528 Add support for Jordan in ROW regulatory domain for the AP3825i
wns0011529 Update channels and power settings for AP3765 and AP3767 models for Macau

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

Enhancements in 9.15.01.0121
Introducing support for the IdentiFi Wireless AP3805i, 2x2:2, dual-radio 802.11ac + abgn, indoor access point. This entry-level 802.11ac access point extends all the performance benefits of the new 802.11ac without the premium price.
Introducing support for the V2110 Virtual Appliance running on Microsoft Hyper-V platform; reduces the deployment costs of an enterprise-grade wireless network for customers that already have an investment in Microsoft Hyper-V data centers.
High-availability for location services ensures that devices, users, and threats are always visible in the network to ensure maximum up-time and performance.
High-Availability for IdentiFi Radar ensures continuous protection on the wireless networks, even in the event of WAN or hardware failures.
New enhancements for primary / backup Radius deployments allow the administrator to configure Radius authenticaton so that after a primary server failure and request are forward to the backup server, new authentication requests will revert back to the primary Radius sever after the primary server is back online.
A new area notification feature is designed to track client locations within pre-defined areas using either the Location Engine or the AP Location field. When the clients change areas, a notification is sent; this feature is useful to apply policies to clients based on their physical area.
New features for Radar including: 1. Passive monitoring of DFS channels 2. Passive monitoring of regulatory prohibited channels 3. Scanning 80MHz wide channels on the 38xx series
Periodic push of location data over the web for Third Party Location Services and Analytics solution (e.g. Purple WiFi).
Adds a new feature to improve the deployment flexibility of an External Captive Portal (ECP) securely across firewall boundaries. The new feature implements a comparable level of control and trust via the use of HTTP

Enhancements in 9.15.01.0121
redirections between the ECP and EWC that can be 'proxied' by the user's browser. These messages do not require additional ports be open on the firewall.
Increases Location Engine Limits to match the maximum clients limit of the wireless appliance.
Guest Portal redirection has been enhanced to redirect HTTPS requests to the Guest Portal page. The redirection will result in a security warning from most modern browsers because the original HTTPS request has been redirected to either an insecure open portal or to an HTTPS portal that is using a different SSL cert than the original request. If the user selects continue after the warning, the Guest Portal will come up so that they can sign into the network.
Adds country support for Iraq to the WS-AP3705 under ROW regulatory domain.
Adds country support for Taiwan to the WS-AP3825i/e under the ROW regulatory domain.
Adds country support for Zambia to the WS-AP3715i only under the ROW regulatory domain.
Adds country support for Singapore to the WS-AP3825i/e and WS-AP3865e under the ROW regulatory domain.
Adds country support for Angola to the WS-AP3765i under the ROW regulatory domain.
Adds support for the WS-AO-DX07025N & WS-AO-5D23009N for ETSI to the AP3865e.
Adds country support for all the 3700 and 3800 Series access points for Georgia under the ROW regulatory domain.
Adds country support for Armenia to WS-AP3705i, WS-AP3715i, WS-AP3825i, WS-AP3865e under the ROW regulatory domain.
Adds country support for Trinidad and Tobago for the AP3825i/e under the ROW regulatory domain.
Adds country support for Kuwait to the AP3825i/e under the ROW regulatory domain.
Adds country support for Angola to WS-AP3705i, WS-AP3715i/e, WS-AP3765i/e, WS-AP3767e, WS-AP3825i/e and WS-AP3865e under the ROW regulatory domain.
Adds country support for India to the WS-AP3865e under the ROW regulatory domain.
Adds country support for Qatar to the WS-AP3825i/e under the ROW regulatory domain.
Adds country support for Saudi Arabia to the WS-AP3825i/e under the ROW regulatory domain.
Adds country support for Mexico under the ROW and NAM regulatory domains.
Support for HTTPS Traffic redirect to the Captive Portal.
Support for using Individually assigned MAC Address per Ethernet Port.
Extend auto-login captive portal detection to Android, Windows and Blackberry.
Remove need for administrator to approve certificates for maintenance releases.
Update NAC VNS Wizard to include Default VSAs.

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

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

Enhancements in 9.12.04.0003
wns0011141 Adds country support for Angola to WS-AP3705i, WS-AP3715i/e, WS-AP3765i/e, WS-AP3767e, WS-AP3825i/e and WS-AP3865e under the ROW regulatory domain.

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

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

Changes in 9.12.03.0009	
wns0010604 wns0010923	Corrected an issue that could cause new or re-authenticated client sessions to not connect due to a synch issue between local and foreign controllers in a mobility domain.
wns0010916	Corrected an issue that would cause the channel setting to be changed from custom to auto when upgrading from V9.01.03 to V9.12.01.
wns0010964	Corrects an issue that could cause legacy 3600 Series to reboot.
wns0010969	Improved the cleanup algorithms to recover resources from disassociated client sessions faster increasing resiliency of the APs in high-density deployments.
wns0010994	Added an enhancement to allow Guest Portal Admin to search for user accounts by both user name and user ID.
wns0011010	Added an enhancement to preserve the previously configured default gateway if the change to an IP address on the controller is still in the same subnet as the default gateway.
wns0011014	Corrected an issue that prevented V9 policies configured on the controller from being imported into Policy Manager.
wns0011026	Corrected an issue that could cause APs to reboot when there is a large deployment of APs (500+) on the same multicast domain.
wns0011027	Addressed a corner-case race condition whereby a captive portal user could get a "refresh" browser message before the system had changed their topology from an unauthenticated to an authenticated state.
wns0011038	Improved the resiliency of the AP in very high-density user environments that results in heavy log event generation.

Changes in 9.12.03.0009	
wns0011041	Corrected a corner condition whereby the last fragment of a certificate chain was incorrectly fragmented by the AP to the controller if the certificate size caused the frame size to exceed the MTU size.
wns0011093	Corrected an issue that would prevent jumbo frames from working correctly when configured in conjunction with link aggregation on the controller.

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

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

Enhancements in 9.12.01.0067
Introducing support for the IdentiFi Wireless AP3865e, a high-performance, high-availability IEEE802.11ac 3x3:3 MIMO outdoor access point for high-density deployments in extreme weather conditions.
Adds support for “application” policy rules enabling granular control of Bonjour/LLMNR service requests and service advertisements.
Adds support for Guardian mode to the AP376X and AP3865 as well as in-service mode for the AP3865e.
Adds support for Rogue AP detection in Guardian mode to the 3800 Series.
Adds support for scheduled AP Log Collection for the 3000 Series. The AP log collection feature does not work if the APs are deployed on the secure side of a firewall and the controller is deployed on the unsecure side.
Increases the number of MUs tracked by the location services engine to 2,500 for the C5110, C4110, and V2110 and to up to 1,024 MUs for the C25.
The AP3825 and AP3865 became WiFi Alliance compliant and received the “WiFi certified” status from TUV.

Changes in 9.12.01.0067	
wns0010129	Corrected a memory management issue on 11n APs that could cause the AP to reboot.
wns0010481	Corrected an issue whereby a transient RF event could result on a false positive and subsequent AP reset on the 3710s.
wns0010826	Corrected an issue that could generate an intermittent debug message if the GUI application could not collect the necessary data to render a configuration screen.
wns0010034	Corrected a memory management issue that could cause the AP36XX Series APs to reboot.

Changes in 9.12.01.0067	
wns0010174	Corrected a memory management issue with the LLDP service on the APs that could cause the AP to reboot.
wns0010056	Corrected an issue that prevented some Apple devices from connecting to a hidden SSID.
wns0010645	Corrected an issue with broadcast/multicast filtering that could result in DHCP packets being dropped intermittently when using DHCP relay and routed topologies.
wns0010581	Corrected the DFS algorithm used for the AP3710i/e for Mexico in the regulatory tables.
wns0010575	Corrected regulatory tables for channels 149-165 for Korea.
wns0010553	Added a GUI enhancement to prevent an administrator from entering a bad ICP non-auth configuration.

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

Changes in 9.01.03.0008	
wns0008388	Improved the resiliency of the AP3600 Series when a malformed E/N packet is received on the wired port.
wns0010034	Corrected a memory management issue that could cause the AP36XX Series APs to reboot.
wns0010473	Corrected a memory management issue that could cause a controller to reset
wns0010551	Corrected an issue with the ECP interface whereby the controller was not returning the correct topology name for an MU associated to an unauth policy.
wns0010585	Corrected an issue whereby the AP would continue to send packets to a mobile device that was in sleep mode causing the loss of data packets.
wns0010638	Increased the length of the SNMP password parameter to account for protecting the password via encryption in the configuration file.
wns0010645	Corrected an issue with broadcast/multicast filtering that could result in DHCP packets being dropped intermittently when using DHCP relay and routed topologies.
wns0010763	Corrected the power settings for Kuwait for the AP376X Series; removes channels 36-64 for outdoors.
wns0010756	Corrected the power settings for Taiwan for the AP3705i.

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

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

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

Enhancements in 9.01.01.0228
Introducing support for the IdentiFi Wireless AP3825i and AP3825e, two new high-performance, high-availability IEEE802.11ac 3x3:3 MIMO indoor access points for mission critical deployments.
Enhanced IdentiFi Guardian to detect the presence of Rogue APs via a closed-loop wired/wireless mechanism thereby reducing false positives (unauthorized APs attached to an authorized network).
Adds support for automatically provisioning the power settings for professionally installed external antennas based on installer configurable attenuation levels.
The internal Captive Portal can now be configured to use either http or https.
Adds the ability to encapsulate mini-Jumbo frames for tunneled data traffic from the AP to the controller without the need to fragment and reassemble larger packets. Supported on the C5210, C5110, C4110, AP3710, AP3715 and AP3825
Adds support for the ETS Resource Utilization MIB enabling SNMP management systems to query the CPU/memory utilization of a controller.
Adds support for backing up a controller configuration to a USB key.
Adds support for dynamic LAG via LACP enabling active/active dual-Ethernet data paths to the AP3825.
Adds support for ESXi Application Monitoring to the V2110.
Increased the AP capacity of the V2110 by two APs to 250 APs in normal mode and 500 APs in failover mode, matching the C4110 for HA deployments.
Adds support for license pooling of AP and Radar capacity licenses within an HA pair and simplifies the load-balancing of APs between controllers in the HA pair.
Adds country support for Singapore to the WS-AP3710i/e under the ROW regulatory domain.
Adds country support for Aruba to the WS-AP3705i and WS-AP3715i/e under the NAM/FCC regulatory domain.
Adds country support for Curacao to the WS-AP3705 and WS-AP3715 under the NAM/FCC regulatory domain.
Adds country support for Barbados to the WS-AP3705i, WS-AP3715i/e under the NAM/FCC regulatory domain.
Adds country support for Kuwait to the WS-AP3715i under the ROW regulatory domain.
Adds country support for Egypt to the WS-AP3715i under the ROW regulatory domain.
Adds country support for Saudi Arabia to the WS-AP3715i/e under the ROW regulatory domain.
Adds country support for Angola to the WS-AP3715i under the ROW regulatory domain.
Adds country support for South Africa to WS-AP3715i/e under the ROW regulatory domain.
Adds country support for Jamaica to the WS-AP3705, WS-AP3715 under the NAM/FCC regulatory domain.
Adds country support for Trinidad and Tobago to the WS-AP3705i, WS-AP3715i/e under the ROW regulatory domain.
Adds country support for South Africa to the WS-AP3710e under the ROW regulatory domain.
Adds country support for Colombia to the WS-AP3715e under the NAM/FCC regulatory domain.
Adds country support for China to the WS-AP3715i under the ROW regulatory domain.

Enhancements in 9.01.01.0228
Adds country support for Mexico to the WS-AP3715i/e under the NAM/FCC regulatory domain.
Adds country support for Singapore to the WS-AP3715i/e under the ROW regulatory domain.
Adds support for the 2.4GHz spectrum for Macau to the WS-AP3705i, WS-AP3715i and WS-AP3715e under the ROW regulatory domain.
Adds support for the WS-AO-DX10055, a new outdoor service antenna, to the WS-AP376Xe.
Adds country support for Egypt to the WS-AP3715e under the ROW regulatory domain.
Corrects the regulatory compliance table for Taiwan for on the WS-AP3705i to allow channels 149-165.
Adds support for Macau to the WS-AP3610, WS-AP3710i/e and WS-AP376X under the ROW regulatory domain.
Adds support for Hong Kong to the WS-AP3710i/e under the ROW regulatory domain.
Adds support for DFS channels to the WS-AP3710e under the NAM/FCC regulatory domain.
Adds support for DFS channels to the WS-AP3715i/e under the NAM/FCC regulatory domain.

Changes in 9.01.01.0228 (ported from 8.32.05.0007)	
wns0010126	Corrected an issue that would cause a device to see their own MAC address when querying for duplicate addresses due to a malformed gratuitous ARP request from the originating client.
wns0010104	Corrected an issue that would cause a “no change” topology to be added to the “Active Clients by VNS” report.
wns0009915	Corrected an issue that prevented a certificate from being loaded if the certificate file matched the CSR file name of the controller.
wns0009903	Corrected an issue that was causing roaming instability with Motorola HDT scanners due to a 0 length EAP packet.
wns0009866	Corrected an issue that could result in the configuration file being corrupted during an upgrade of a V2110 in the presence of a large CDR database.
wns0009850	Corrected an issue that prevented the Traffic Summary to be reported accurately in the Active Clients By VNS report.
wns0009837	Corrected an issue that prevented Guest user accounts from being synchronized in a high-availability pair.
wns0009836	SNMP queries to ifOperStatus, ifAdminStatus, and IfDescr tables are now working correctly.
wns0009815	Corrected an issue that was preventing SNMP queries to the ipNetToMediaPhysAddress from working.
wns0009811	Corrected an issue that could result in a mis-configuration when changing the configuration of an AP from a 20MHz channel to Auto.
wns0009806	Corrected regulatory settings for China on the 3610s for the 5.7-5.8 band.
wns0009803	Corrected an issue with the export of “All Clients” report which prevented XML parsers from reading the report.
wns0009761	Corrects an instability issue that could cause an intermittent reset on certain APs.
wns0009743	Correctly disables channels 120, 124, and 128 for AN-HT20 for the AP3620 with the WS-ANT02 due to regulatory requirements. Unlike the AP3610, the AP3620 can be deployed outdoors and thus it is not able to operate within the DFS/weather channels.
wns0009731	Corrected an issue that resulted in traffic being blocked when a rule matched on QoS settings.
wns0009728	Corrected an issue that could result in instability when trying to apply advanced filter rules in V8.31 to legacy APs.
wns0009723	Corrected an issue that resulted in the controllers reporting an inaccurate user count.

Changes in 9.01.01.0228 (ported from 8.32.05.0007)	
wns0009708	Added a new configuration option via the CLI to overwrite the default timing for key exchange retries. The default retry setting of 100ms may be too aggressive for some legacy clients to respond in time.
wns0009707	Corrected an issue that could cause instability issues with legacy 26XX Series APs when applying configuration changes.
wns0009706	Increased the timeout timer for EAP re-transmissions to minimize connectivity issues with slower clients.
wns0009704	Corrected an issue that prevented a Guardian sensor from accepting a deny list configuration update after detecting a threat.
wns0009698	Corrected a timing issue between the AP and the controller with Guest Portal redirection that could cause the end-user to have to press the submit button twice to continue to their intended page.
wns0009689	Corrected a memory management issue that could result in stability problems when saving configuration changes.
wns0009632	Corrected a statistics counter which was incorrectly reporting an excessive amount of duplicate frames after a radio reset on the 3700 Series.
wns0009610	Corrected the amount of the memory allocated for internal structures to ensure there are enough resources available on the controller for high-density deployments.
wns0009520	Updated the SSH service on the APs to the latest version.
wns0009489	Corrected an issue that prevented Guest users from seeing custom Guest Portal images after an upgrade.
wns0009481	Corrected an issue with the registration service that prevented Scalance W788-2RR from connecting to a controller running V8.21 or higher.
wns0009480	Corrected an issue that caused persistent mode feature to not work.
wns0009476	Corrected an issue that caused foreign controller in the mobility zone to reboot when configuration for active client session is changed on the home controller.
wns0009466	Fixed memory leak when operating as WDS parent with no client WLAN service on AP3660
wns0009465	Corrected an interface synchronization issue after an upgrade that prevented the NTP service from synchronizing the time on the controller.
wns0009459	Corrected an issue that causes instability on the controller under certain scenarios where a user roams from one VNS to another.
wns0009435	Fixed corner case instability caused by synchronization issues on 3710 AP.
wns0009417	The system now rejects administrative RADIUS login passwords and login attempts using Unicode characters.
wns0009342	Fix the instability caused by unused Ethernet interface timer on AP3715
wns0009312	Corrected an issue that allowed station to roam without performing MAC authentication after initial authentication.
wns0009306	Corrected a connectivity issue between the SEN WL2 and 3600 Series introduced in 8.31.01.
wns0009262	Improved interoperability with legacy wireless devices that exclusively use old power save method
wns0009252	Removed channel 120, 124, 128 from AP default settings.
wns0009107	Corrected an issue whereby clients using bridge at controller topology stayed connected when link-persistence was enabled even though the AP-controller link was down due to a physical link layer problem with the cable.
wns0008894	Corrected an issue that causes instability when frame aggregate deletion is requested by wireless client.

KNOWN RESTRICTIONS AND LIMITATIONS:

How to use Real capture tool - Click Start to start real capture server on the AP. This feature can be enabled for each AP individually. Default capture server timeout is set to 300 seconds and the maximum configurable timeout is 1 hour. While the capture session is active the AP interface operates in promiscuous mode. - From Wireshark GUI set the capture interface to the selected AP's IP address and select null authentication. Once Wireshark connects to the AP, the AP's interfaces will be listed as available to capture traffic. eth0 is the wired interface, wlan0 is the 5Ghz interface and wlan1 is the 2.4Ghz interface. - The user can selected to capture bidirectional traffic on eth0, wifi0 and wifi1. The capture on wifi0 and wifi1 will not include internally generated hardware packets by the capturing AP. The capturing AP will not report its own Beacons, Retransmission, Ack and 11n Block Ack. If this information is needed, then the real capture should be done from a close-by second AP. Change that second AP's wireless channel to match the AP that is being troubleshot. Let it broadcast a SSID so the radios switch on, but do not broadcast the same SSID you are troubleshooting, so that the clients do not connect to your second capturing AP.
wns0011707 – Info AP26xx family does not support advanced policy features such as CP redirection at the AP – contact GTAC for the full KB article.
wns0011519 – Info Instability observed on the network with Intel AC-7260 based clients. Workaround: Update the Intel AC-7260 driver and disable Throughput Boost setting in client driver Advanced option.
Wns0011589 – Info AP38XX supports TKIP but with the following restrictions due to new Wi-Fi Alliance certification requirements: 1. Only available for Legacy rates; not supported with 11n nor 11ac rates 2. Mix configuration of AES and TKIP on one radio is not supported; for example, configuring multiple VNS with mixed types of TKIP and AES on one AP radio is not allowed.
wns0011467– Info RADIUS attribute-value pair limits the location data size to 251 characters. In the case that the location data size is more than 251 characters then this data will be sent to the RADIUS server truncated to 251 characters.
wns0011008– Info The Location Batch Report file contains two timestamp attributes. Both of them are currently in local time, but the time zone indicator is missing. These fields should be reported as UTC time with the time zone set to 'Z'
wns0010904– fixed in 9.12.01 Corrected an issue that causes AP to stop advertising SSID when failing over to secondary controller in availability pair
wns0010885– Info Maintenance Guide mentions a RESET button on both AP3825 and AP3865. However, the AP3865 does not have a reset button. This issue will be corrected in the documentation in the next maintenance release.
wns0010642– Info Chrome autocomplete function fills in fields incorrectly. Users should disable password saving and password field auto completion in their Chrome configuration.
wns0010265 – Info In V9.12 the conversion from AP3630/40 “thin” mode to standalone mode is not supported. To convert an AP3630/40 from standalone mode to thin mode, first use V8.32 for the conversion. Once converted to V8.32 the AP becomes a 3610/20 and can then connect to a V9.12 controller.
wns0010168 – Info

"ac-strict" radio mode may not operate correctly with all clients. At release date (June 26, 2014) the Intel AC 7260 client does not operate if c-strict is set.

wns0008749 – Info

Enhancement to the authentication mechanism reduces the number of Radius authentication requests that are generated per user reducing the overhead on external authentication servers.

wns0008740 – Info

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

wns0008876 - Info

Issue: Reported WiFi degraded performance with Apple clients using 11n and Call Admission Control (CAC)
Apple clients running iOS 6.0.1 may experience degraded throughput when attempting to download media rich content such as video. Apple clients running iOS 5.x or earlier do not experience the issue under identical conditions. Apple support has observed and analyzed the issue, and has confirmed non-compliant CAC behavior with iOS 6.0.1 software. Apple intends to correct the issue in forthcoming firmware updates.
Conditions: Apple iOS 6.0.1 client connected to Unified Access Point at 802.11N data rates with Video Call Admission Control (CAC) enabled.
Workaround: Disable 802.11n support or disable Video Call Admission Control (CAC).

Info

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

wns0008979 - Info

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

wns0008035 - Info

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

wns0008023 - Info

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

wns0006968 - Info

The SNMP agent generates traps to notify the administrator of configuration changes, component failures, disconnection of Access Points or any other events that may need the administrator's attention. Administrators can configure the Agent and the Controller as to what level of trap they wish to receive. The traps type that are supported by the IdentiFi Wireless Controllers are:
1. Interfaces MIB (IF-MIB) linkDown (.1.3.6.1.6.3.1.1.5.3)
2. Interfaces MIB (IF-MIB) linkUp (.1.3.6.1.6.3.1.1.5.4)
3. HIPATH-WIRELESS-HWC-MIB apTunnelAlarm (.1.3.6.1.4.1.4329.15.3.19.4)
   • Sent by the controller when it detects that it has lost the connection to an AP. The trap identifies the AP that the controller can no longer contact
4. HIPATH-WIRELESS-HWC-MIB hiPathWirelessLogAlarm (.1.3.6.1.4.1.4329.15.3.9.6)
   • A trap containing one event that also is displayed in the controller's Event / Log report page. The trap is sent when the event is raised and recorded on the controller.
   • This trap accounts for the vast majority of traps messages sent by the controller at most sites.
   • The trap contains the trap severity, the component on the controller that raised the event and the text string associated with the event, just as it would appear in the controller GUI.
The item listed under #4 is a generic trap that contains specific information relevant to the event. The information varies from event to event and are all carried in the trap.

wns0007114 - Info

An 802.11n AP running on version 8.21 is being downgraded to an earlier pre 8.11 release. After the downgrade it may fail to convert to a sensor. The following downgrade procedure steps are required to address this issue:
11n AP:
1. Downgrade the AP firmware twice to the pre-8.11 version (8.01 or 7.41).
2. Convert the AP to sensor

11n AP running in sensor mode:
1. Convert the sensor to AP
2. Downgrade the AP firmware twice to the pre-8.11 version (8.01 or 7.41).

3. Convert the AP back to sensor

wns0007074 - Info

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

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

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

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

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

SUPPORTED WEB BROWSERS

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

- MS IE 7, IE 8.0, IE9, IE10
- FireFox 33.0

Note: Google™ Chrome currently is not supported for managing the EWC Controller.

Wireless Clients (Captive Portal, AAA):

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

PORT LIST

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

IdentiFi Wireless TCP/UDP Port Assignment Reference

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

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

Access Point	Controller	TCP/UDP	Any	69	TFTP	AP image transfer	Yes[2]
Controller	Access Point	TCP/UDP	Any	22	SCP	AP traces	Yes
Any	Access Point	TCP	Any	2002, 2003	RCAPD	AP Real Capture (if enabled)	Optional
Any	Access Point	TCP/UDP	Any	22	SSH	Remote AP login (if enabled)	Optional
Ports for Controller Management							
Any	Controller	TCP/UDP	Any	22	SSH	Controller CLI access	Yes
Any	Controller	TCP/UDP	Any	5825	HTTPS	Controller GUI access	Yes
Any	Controller	TCP/UDP	Any	161	SNMP	Controller SNMP access	Yes
Any	Controller	TCP/UDP	Any	162	SNMP Trap	Controller SNMP access	Yes
Ports for Inter Controller Mobility and Availability							
Controller	Controller	UDP	Any	13911	WASSP	Mobility and Availability Tunnel	Yes
Controller	Controller	TCP	Any	427	SLP	SLP Directory	Yes
Controller	Controller	TCP	Any	20506	Langley	Remote Langley Secure	Yes
Controller	Controller	TCP	Any	60606	Mobility	VN MGR	Yes
Controller	Controller	TCP	Any	123	NTP	Availability time sync	Yes
Controller	DHCP Server	UDP	Any	67	SLP	Asking DHCP Server for SLP DA	Yes
DHCP Server	Controller	UDP	Any	68	SLP	Response from DHCP Server for SLP DA request	Yes
Core Back-End Communication							
Controller	DNS Server	UDP	Any	53	DNS	If using DNS	Optional
Controller	Syslog Server	UDP	Any	514	Syslog	If Controller logs to external syslog server	Optional

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

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

IETF STANDARDS MIB SUPPORT:

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

ENTERASYS NETWORKS PRIVATE ENTERPRISE MIB SUPPORT

Enterasys Networks Private Enterprise MIBs are available in ASN.1 format from the Enterasys Networks web site at: http://www.enterasys.com/support/mibs/. Indexed MIB documentation is also available.

Enterasys Proprietary MIBs

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

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

2.11AC CLIENTS

The following 802.11ac clients are known to work with 9.15 software release:

Device	OS	Network adapter	Model
Notebook	Windows XP	Cisco	WUSB600N
Notebook	Windows XP	Netgear	WN511T
USB	Window 8	ASUS	AC1200
USB	Window 8	ASUSD-Link Corporation	AC1200
Onboard	Windows 7	Intel	Wireless WiFi Link 4965AGN
PCMCIA	Windows XP	Broadcom	Rangemax Next WN511B
USB	Windows 8	Dell	Wireless 1901
Onboard	Windows 8	Intel	Centrino Ultimate-N 6300 AGN
Onboard	Windows 7	Intel	Centrino Ultimate-N 6300 AGN
Notebook	Windows 7	Intel	AC 7260
USB	Windows 7	Asustek	USB N66
Notebook	Windows 8	Asus	USB-AC56
MacBook Air		Apple	AirPort Extreme
mini-PCI	Windows 7	Intel	AC-7260
Notebook	Windows 7	Intel	AC-7260
USB	Sindow 7		Cisco AE6000
Surface 3 Pro	Windows 8.1	Marvell	
Notebook	Windows 8.1	Intel	AC-7260

RADIUS SERVERS AND SUPPLICANTS

RADIUS Servers used during testing

Vendor	Model OS	Version
FreeRADIUS45	1.1.6	FreeRADIUS
FreeRADIUS21	1.0.1	FreeRADIUS
IAS	5.2.3790.3959	Microsoft Server 2003 IAS
SBR50	6.1.6	SBR Enterprise edition
NPS	6.0.6002.18005	Microsoft Server 2008 NPS
FreeRADIUS45	1.1.6	FreeRADIUS

802.1x Supplicants Supported

Vendor	Model OS	Version
Juniper Networks®/ Funk	Odyssey client	Version 5.10.14353.0
		Version 5.00.12709.0
		Version 4.60.49335.0
Microsoft®	Wireless Zero Configuration	Version Windows XP-4K-891859-Beta1
	Wireless Network Connection Configuration	Version Microsoft Window Server 2003, Enterprise Edition R2 SP2
	Wi-Fi Protected Access 2 (WPA2)/Wireless Provisioning Services Information Element (WPS IE) update for Windows XP with Service Pack 2	Version WindowsXP-KB893357-v2-x86-ENU.exe
Intel®	Intel PRO Set/Wireless	Version 13.0.0.x (with Windows® Intel® driver version 13.0.0.x)
Wireless Zero	Windows 7, 8, 8.1 Pro Windows Phone 8.1	provided with Windows®

LAN SWITCHES

Vendor	Model OS	Version	Tested with
Cisco	Catalyst 3550	12.1(19)EA1c	AP 802.1x
Enterasys	G3	01.00.02.0001	For PoE
Enterasys	G3	06.11.01.0040	
	C20N1	Version 12.1(19)EA1c	No PoE

Vendor	Model OS	Version	Tested with
	B3G124-48P	06.61.03.0004	for AP 802.1x, PoE
	B3	01.02.01.0004	10480068225P
	C5	06.42.06.0008	11511205225K
	B3G124-48P	06.61.03.0004	for AP 802.1x, POE
	Extreme X460-24P	12.5.4.5	for AP 802.1x, POE
	B3	06.61.08.0013	Lab switch - sn 10480062225P
	B3	06.61.08.0013	Veriwave switch - sn 10480075225P
Extreme	Summit 300-24	7.6e.4.4	
	Summit 300-24	System Serial Number: 800138-00-03 0443G-01236 CP: 04	for AP 802.1x, POE
	Summit 300-48	7.6e1.4	AP 802.1x, PoE
	Summit 300-48	7.6e1.4	
	Summit 300	Software Version 7.4e.2.6	Lab switch
H3C	H3C S5600 26C	Bootrom Version is 405	for PoE
HP	ProCurve 4104GL	#G.07.22	Lab switch

CERTIFICATION AUTHORITY

Server Vendor	Model OS	Version
Microsoft CA	Windows Server 2003 Enterprise Edition	5.2.3790.1830
Microsoft CA	Windows Server 2008 Enterprise Edition	6.0
OpenSSL	Linux	0.9.8e

RADIUS ATTRIBUTES SUPPORT

RADIUS Authentication and Authorization Attributes

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

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

RADIUS Accounting Attributes

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

GLOBAL SUPPORT:

By Phone: 603-952-5000
1-800-872-8440 (toll-free in U.S. and Canada)

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

By Email: support@enterasys.com

By Web: www.extremenetworks.com/support/

By Mail: Extreme Networks, Inc.
9 Northeastern Boulevard
Salem, NH 03079 (USA)

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