Extreme
Connect Beyond the Network

Customer Release Notes

ExtremeWireless™ Convergence Software

Software Version 10.01.01.0129
December 11, 2015

INTRODUCTION:

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

> **Extreme Networks recommends that you thoroughly review this document prior to installing or upgrading this product.**
>
> **For the latest firmware versions, visit the download site at:**
> www.extremenetworks.com/support/

FIRMWARE SPECIFICATION:

Status	Version No.	Type	Release Date
Current Version	10.01.01.0129	Major Feature Release	December 11, 2015

SUPPORTED CONTROLLERS AND ACCESS POINTS

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

Product	Image
ExtremeWireless Controller C4110	AC-MV-10.01.01.0129-1.gxe
ExtremeWireless Controller C5110	AC-MV-10.01.01.0129-1.txe
ExtremeWireless Controller C5210	AC-MV-10.01.01.0129-1.rue
ExtremeWireless Controller C25	AC-MV-10.01.01.0129-1.pfe
ExtremeWireless Controller C35	AC-MV-10.01.01.0129-1.cwe
ExtremeWireless Virtual Appliance V2110 VMware	AC-MV-10.01.01.0129-1.bge
ExtremeWireless Virtual Appliance V2110 MS Hyper-V	AC-MV-10.01.01.0129-1.ize
Wireless AP3935	AP3935-10.01.01.0129.img
Wireless AP3801i	AP3801-10.01.01.0129.img
Wireless AP3805	AP3805-10.01.01.0129.img
Wireless AP3865	AP3825-10.01.01.0129.img
Wireless AP3825	AP3825-10.01.01.0129.img
Wireless AP3715	AP3715-10.01.01.0129.img
Wireless AP3710	AP3710-10.01.01.0129.img

Wireless AP3705i	AP3705-10.01.01.0129.img
Wireless AP3765	W78XC-2-10.01.01.0129.img
Wireless AP3767	W78XC-2-10.01.01.0129.img

INSTALLATION INFORMATION

Note:

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

Installation Notes

- The minimum system software version is 09.21.01 to upgrade to this software version.
- Rogue AP detection, countermeasures and Prevention for Guardian mode for AP3935 have been disabled in release V10.01.01.
- It is possible that some client devices will not handle frames properly when the L2 MAC is unicast and the L3 IP address is multicast in which case the "Multicast to Unicast Delivery" option should be disabled.
- The V2110 is supported on ESXi version 5.5 and 6.0. For best performance and lowest latency, the MMU and CPU should support hardware virtualization such as the Intel EP-T & VT-x or AMD AMD-V & RTI.
- The following advanced features are supported on vSphere 5.5:
  - vSphere High Availability (HA). Release 9.12.01 adds support for vSphere application level HA monitoring. This provides protection comparable to that offered by the hardware watchdog timer on the hardware wireless controllers.
  - vSphere vMotion. vMotion involves moving a running virtual machine (VM) from one host to another within a cluster with minimal or no service interruption.
  - vSphere Dynamic Resource Scheduling (DRS) and Dynamic Power Management (DPM). These features monitor host utilization and use vMotion to migrate VMs to different hosts based on power management and resource utilization goals.
  - Storage vMotion. Storage vMotion allows the administrator to move a VM's disks to different host servers while the VM is running.
  - Cold migration – The V2110 supports cold migration subject to the requirement that the V2110 is migrated in a shutdown state not in a suspended state.
  - Distributed Virtual Switches (DVS). A DVS is a virtual switch that spans multiple physical hosts. VMs migrated between hosts sharing a DVS retain their network point of presence and addresses. Customers who expect to vMotion V2110s frequently should deploy DVSs if possible.
  - The V2110 has supported the virtual serial port and virtual serial port concentrator features since its first release. This support continues in release 10.01.01. VMware requires the customer to purchase licenses in order 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.
- If configuring a service that will incur topology changes after user gets an IP address via DHCP, for example due to authentication state, it is recommended to use short lease times on the initial topology (un-auth topology) so that clients automatically re-negotiate a new address faster (typically at half-lease) . Alternatively, it may be required to manually renew the DHCP lease from the client.

- Please add filter rule "In Filter:dest, Out Filter:src, 0.0.0.0/0, port:BootP(67), Protocol:UDP, allow" in non-authenticated policy for captive portal WLAN Service if you intend to allow wireless clients to get an IP address through DHCP.
- If the filters used by controllers are managed by Policy Manager (PM), PM should include the DHCP allow rule in the policies where that is appropriate. If PM has not done this then it will need to explicitly add the rule to policies that are pushed to the controller and that need to support DHCP.
- IP Broadcast Multicast traffic will apply catch-all role action. If users would like to allow specific multicast, broadcast, and subnet broadcast traffic with the deny-all catch-all filter rule for global default policy, they need to explicitly add specific multicast, broadcast and subnet broadcast rules one by one to allow that traffic.
- \, ', " characters are not supported in WLAN/VNS fields.
- In case of upgrade to V10.01, 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.
- Configuration of the AP3935 is not yet supported via Network Management.

Upgrading Virtual Appliance V2110 VMware to the Current Release

You only need to install the ".ova" file when you first install the V2110 VMware. The latest .ova file is V2110-09.21.01.0179.ova. All subsequent upgrades can be performed using the standard controller upgrade procedure to apply a ".bge" file to the V2110 VMware.

For more information about installing the V2110 VMware refer to the "ExtremeWireless V2110 Virtual Appliance Installation Guide VMware platform".

For more information about upgrading the V2110 VMware refer to the "ExtremeWireless Convergence Software Maintenance Guide".

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

You need to install the ".zip" file when you first install the V2110 Hyper-V. All subsequent upgrades can be performed using the standard controller upgrade procedure to apply a ".ize" file to the V2110 Hyper-V.

For more information about installing the V2110 MS Hyper-V refer to the "ExtremeWireless V2110 Virtual Appliance Installation Guide MS Hyper-V platform".

For more information about upgrading the V2110 MS Hyper-V refer to the "ExtremeWireless Convergence Software Maintenance Guide".

Configuring the Shared Secret for Controller Communication

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

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

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

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

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

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

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

NETWORK MANAGEMENT SOFTWARE SUPPORT

Network Management Suite (NMS)	Version
etSight and Wireless Manager	6.3 or higher
NetSight Wireless Advanced Services	4.4
Extreme Control Identity and Access Management	6.3 or higher

IMPORTANT: EXTREMEWIRELESS V10 LICENSING CHANGES

Consolidated the regulatory domains to FCC, ROW, Base (for no domain specified). The FCC domain is limited to the US (and US territories), Puerto Rico, and Colombia. All other countries where an AP is certified falls under the Rest-Of-World (ROW) regulatory domain including countries previously under the NAM domain (e.g. Canada). Due to the regulatory compliance requirements, there is no grace period for installing a V10 license when a customer upgrades from V9.21. However, to help transitioning legacy NAM countries to ROW, V10 FCC licenses will support previous NAM countries. Customers that have a valid maintenance contract must request a V10.01 upgrade license (available through the Extranet Licensing Site) before upgrading the appliance to V10.01.

EXTREMEWIRELESS V9 TO V10 REQUESTS FOR NEW LICENSE KEYS

A new activation license key needs to be requested whenever the Wireless Controller software is upgraded from one major version to another (e.g., version 9 to version 10). Old activation keys will not carry over in the upgrade process, but feature licenses (incremental AP licenses, Radar, etc.) are carried over on the same controller.

After upgrade, you are given a 7 day grace period to activate an upgraded system or you lose the ability to manage VNS configuration and Radar scanning. Logs are also recorded every 15 minutes to remind you to install a valid 10.01 activation key.

To request a new V10 license key:

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

Select the Product Licensing link (https://extranet.extremenetworks.com/mysupport/licensing).

Select the **ExtremeWireless Upgrade Licenses** option from the list of tasks on the right-hand menu.

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

Click **Submit.**

Once the form has been submitted, it will be reviewed by Order Management to confirm the contract is valid for a version 10 upgrade.

Upon approval, you will be notified via email and given an Entitlement ID that must be redeemed though the user's Extranet account (follow the instructions in the email).

Once the Entitlement is redeemed, an activation key will be emailed to you (or it can be directly copied).

Configure the activation key into the ExtremeWireless Controller.

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

NEW FEATURES, SOFTWARE CHANGES, AND ENHANCEMENTS

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

Enhancements in 10.01.01.0129
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.
Legacy AP26XX, AP36XX, AP4102 Series access points are not supported with V10.01 or later, however, these legacy APs will continue to be supported in maintenance mode only with V9.21 until they reach End-of-Support.	N/A
Radar countermeasures are not available on the 39XX Series in V10.01.01; countermeasures will be available in a future maintenance release.	wns0013401– Info
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.	wns0013397– Info
Due to changes to the SNMP agent in V10.01.01, "counter64" type OIDs is no longer supported. To get support for this type OIDs use SNMP V2c or V3.	wns0013536– Info
802.11v is not supported	wns0012730– Info
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 any Capture Filter and also disable "Do not capture own RPCAP traffic" in Remote Settings. In v1.12.3, this option is found by going to **Capture** > **Option** > Double-click **Interface Row** > **Remote Settings**.	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, and in site configuration all topologies get pushed to all APs, which effectively limits the maximum per-controller topologies to 128	wns0012793 – Info
Counter measures for honeypot AP threat may be less effective for iPhone (with version 8.3) client device than other device types.	wns0012678 – Info
For AP3935, real capture tool is not available. For all other APs, see	N/A

How **TO USE THE REAL CAPTURE TOOL** on page 8.	
We recommend that you do not enable 802.11k along with the Quiet IE option for installations with Ascom i62 phones.	wns0012567– Info
Enforcement of Rogue AP countermeasures requires AP in Guardian mode.	wns0012296– Info
Instability issues observed on the network with Intel AC-7260 based clients. **Workaround**: Update the Intel AC-7260 driver and disable Throughput Boost setting in client driver Advanced option. This issue is not present if the client driver is running18.20.0.9 or above.	wns0011519 – 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.	wns0011589 – Info
RADIUS attribute-value pair limits the location data size to 251 characters. When the location data size is more than 251 characters, then 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 set to 'Z'	wns0011008– Info
Chrome autocomplete 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

Topology groups – Info

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

Info

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

HOW TO USE THE REAL CAPTURE TOOL

1. 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.

2. From the Wireshark GUI, set the capture interface to the selected AP's IP address and select **null authentication**.

3. 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 5 Ghz interface, and wlan1 is the 2.4 Ghz interface.

   You have the option to capture bidirectional traffic on eth0, wifi0 and wifi1. The capture on wifi0 and wifi1 will not include internally generated hardware packets by the capturing AP. The capturing AP will not report its own Beacons, Retransmission, Ack and 11n Block Ack.

4. If the bidirectional traffic information is needed, then the real capture should be done from a close-by second AP. To do this, change the 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.

SUPPORTED WEB BROWSERS

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

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

The Wireless Clients (Captive Portal, AAA):

Browsers	Version	OS
Chrome	47.0.2526.80 m	Windows 7
	46.0.2490.71 dev-m	Windows server 2012
	38.0.2125.111m	Windows server 2012
Firefox	41.0.1	Windows server 2012
	38.0.5	Windows XP
IE 11	11.0.9600.18059	Windows 7
IE 8	8.0.6001.18702	Windows XP
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 is a list of ports that may be required to be open so the controllers/APs will work properly on a network. Firewall protection may also be required..

ExtremeWireless TCP/UDP Port Assignment Reference

Comp. Source	Comp. Dest	Protocol (TCP/UDP)	Src Port	Dest Port	Service	Remark	Open Firewall Req'd
Ports for AP/Controller Communication							
Controller	Access Point	UDP	Any	13910	WASSP	Management and Data Tunnel between AP and Controller	Yes
Access Point	Controller	UDP	Any	13910	WASSP	Management and Data Tunnel between AP and Controller	Yes
Controller	Access Point	UDP	4500	Any	Secured WASSP	Management Tunnel between AP and Controller	Optional
Access Point	Controller	UDP	Any	4500	Secured WASSP	Management Tunnel between AP and Controller	Optional
Access Point	Controller	UDP	Any	13907	WASSP	AP Registration to Controller	Yes
Access Point	Controller	UDP	Any	67	DHCP Server	If Controller is DHCP Server for AP	Optional
Access Point	Controller	UDP	Any	427	SLP	AP Registration to Controller	Optional
Controller	Access Point	TCP/UDP	Any	69	TFTP	AP image transfer	Yes[1]
Access Point	Controller	TCP/UDP	Any	69	TFTP	AP image transfer	Yes[2]
Controller	Access Point	TCP/UDP	Any	22	SCP	AP traces	Yes
Any	Access Point	TCP	Any	2002, 2003	RCAPD	AP Real Capture (if enabled)	Optional
Any	Access Point	TCP/UDP	Any	22	SSH	Remote AP login (if enabled)	Optional
Ports for Controller Management							
Any	Controller	TCP/UDP	Any	22	SSH	Controller CLI access	Yes
Any	Controller	TCP/UDP	Any	5825	HTTPS	Controller GUI access	Yes
Any	Controller	TCP/UDP	Any	161	SNMP	Controller SNMP access	Yes

---

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

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

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

IETF STANDARDS MIB SUPPORT:

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

EXTREME NETWORKS PRIVATE ENTERPRISE MIB SUPPORT

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

Proprietary MIBs

Title	Description
enterasys-configuration-management-mib.txt	Used to perform configuration backup and restore
ENTERASYS-CLASS-OF-SERVICE-MIB	Used for configuration/monitoring CoS and rate control
ENTERASYS-POLICY-PROFILE-MIB	Used for configuration/monitoring policy and rules assignments
ENTERASYS-RADIUS-AUTH-CLIENT-MIB	Used for configuration of RADIUS Authentication servers
ENTERASYS-RADIUS-ACCT-CLIENT-EXT-MIB	Used for configuration of RADIUS Accounting servers
ENTERASYS-IEEE8023-LAG-MIB-EXT-MIB	Used for configuration/monitoring LAG port

Standard MIBs

Title	Description
IEEE802dot11-MIB	Standard MIB for wireless devices
RFC1213-MIB.my	Standard MIB for system information
IF-MIB	Interface MIB
SNMPv2-MIB	Standard MIB for system information
BRIDGE-MIB	VLAN configuration information that pertains to EWC
P-BRIDGE-MIB	VLAN configuration information that pertains to EWC
Q-BRIDGE-MIB	VLAN configuration information that pertains to EWC
IEEE8023-LAG-MIB	LAG configuration information. Set is permitted for LAG L2 port configuration only.

Siemens Proprietary MIB

Title	Description
HIPATH-WIRELESS-HWC-MIB.my	Configuration and statistics related to EWC and associated objects
HIPATH-WIRELESS-PRODUCTS-MIB.my	Defines product classes
HIPATH-WIRELESS-DOT11-EXTNS-MIB.my	Extension to IEEE802dot11-MIB that complements standard MIB
HIPATH-WIRELESS-SMI.my	Root for Chantry/Siemens MIB

802.11AC AND 802.11N CLIENTS

The following 802.11ac and 80211n clients are known to work with V10.01 software release:

11ac MU-MIMO

Due to limited availability of the real clients, the most of 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
AirPort Extreme (0x14E4, 0x117)	Broadcom BCM43xx 1.0 (6.30.223.74.22)	11ac Strict mode		Pass
ASUS PCE-68ac	6.30.223.75	11ac Strict mode		Pass
Broadcom 802.11 ac	6.30.223.102	11ac Strict mode		Pass
Cisco AE6000	AE6000_v5.0.7.0_Driver_Win7	11ac Strict mode		Pass
iPhone 6 - iOS 9.1	Modem firmware 2.23.03	11ac Strict mode		Pass
iPhone 6 - iOS 9.1	Modem firmware 4.32.00	11ac Strict mode		Pass
MacBook Air	Broadcom BCM43xx 1.0 (6.30.223.154.65)	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	iPad	IOS 7.1.2	
Apple	iPad (4th generation)	iOS9.1	a/b/g/n
Apple	iPad Air 2	IOS9.1	a/b/g/n
Apple	iPad Mini	iOS 8.4.1	
Apple	iPad2 A1396	iPad OS	11abgn
Apple	iPad3	iOS 8.4.1	a/b/g/n
Apple	iPhone 5	iOS	11abgn
Apple	iPhone 5	iOS 9.1	a/b/g/n/
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 build 10586	11 abgnac
Nexus 9	Nexus 9	Android	a/b/g/n/ac
Nokia 830		Win8.1	802.11abgnac
Polycom Spectralink	8440		
Samsung	Galaxy Note4	Android v5.0.1	a/b/g/n/ac
Surface 3 Pro		Win 8.1	Marvel Avastar 802.11 ac

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)

Vendor	Model OS	Version
Wireless Zero	Windows 7, 8, 8.1 Pro, 10 Pro Windows Phone 8.1	provided with Windows®

LAN SWITCHES

Vendor	Model OS	Version	Tested with
Cisco	Catalyst 3550	12.1(19)EA1c	AP 802.1x
Extreme	G3	01.00.02.0001	For PoE
	G3	06.11.01.0040	
	C20N1	Version 12.1(19)EA1c	No PoE
	B3G124-48P	06.61.03.0004	for AP 802.1x, PoE
	B3	01.02.01.0004	10480068225P
	C5	06.42.06.0008	11511205225K
	B3G124-48P	06.61.03.0004	for AP 802.1x, POE
	X460-24P	12.5.4.5	for AP 802.1x, POE
	B3	06.61.08.0013	Lab switch - sn 10480062225P
	B3	06.61.08.0013	Veriwave switch - sn 10480075225P
	X-460-G2		802.3at interoperability with AP3935
Extreme	Summit 300-24	7.6e.4.4	
	Summit 300-24	System Serial Number: 800138-00-03 0443G-01236 CP: 04	for AP 802.1x, POE
	Summit 300-48	7.6e1.4	AP 802.1x, PoE
	Summit 300-48	7.6e1.4	
	Summit 300	Software Version 7.4e.2.6	Lab switch
H3C	H3C S5600 26C	Bootrom Version is 405	for PoE
HP	ProCurve 4104GL	#G.07.22	Lab switch

CERTIFICATION AUTHORITY

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

RADIUS ATTRIBUTES SUPPORT

RADIUS Authentication and Authorization Attributes

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

RADIUS Accounting Attributes

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

GLOBAL SUPPORT:

By Phone: +1 877-801-7082 (toll-free in U.S. and Canada)

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

By Email: support@extremenetworks.com

By Web: www.extremenetworks.com/support/

By Mail: Extreme Networks, Inc.
145 Rio Robles
San Jose, CA 95134

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