

AirDefense 10.0.0-14 Release Notes

AirDefense 10.0.0-14 Release Notes	2
1. New Features in AirDefense 10.0.0-14.....	2
2. Version Compatibility	3
WiNG Version Compatibility.....	3
Extreme Wireless Version Compatibility.....	4
ExtremeCloud Appliance Version Compatibility.....	4
Hardware Appliances.....	4
Virtual Platforms.....	4
Supported WiNG Wireless Access Points	4
Supported Extreme Wireless Access Points	4
Supported Browsers	4
Supported OS.....	5
3. Installation	5
4. Important Notes	5
5. SPR/Issues Fixed	8
6. Vulnerabilities Fixed	8
7. Known Issues and Recommendations	10
Issues specific to EW access points	10
Upgrade related.....	10
Platform	10
Network Assurance.....	12
Bluetooth Monitoring.....	13
8. AirDefense WiNG Feature Matrix.....	14
9. AirDefense Extreme Wireless Feature Matrix	15

AirDefense 10.0.0-14 Release Notes

1. New Features in AirDefense 10.0.0-14

The AirDefense 10.0.0-14 release introduces the following key features and functionalities:

- HTML 5 UI for Dashboard, Network and Alarms
- Bluetooth 4.0/ BLE 4.0 Security
- Cell phone hotspot detection
- Scalability enhancements
- Reporting engine enhancements
- Radioshare WIPS for Extreme Wireless AP 39xx and WiNG AP 76xx

Note that Locationing functionality supported with AD-PROX-P-1 license and associated reports have been removed from the firmware as it is EOL. This functionality has been migrated to the ExtremeLocation replacement product. This does not apply to locating rogue access points/ rogue clients – that functionality continues to be available in this release.

HTML 5 UI for Dashboard, Network and Alarms

A new HTML 5 based UI is being developed for AirDefense to eventually replace the current UI. The new UI will be released in phases over multiple releases. AirDefense 10.0 includes new Dashboard, Network and Alarms pages. The Flex based UI available in AirDefense 9.5 continues to be available in this release. The new UI is launched from the “New User Experience” button added in the top right hand corner of the AirDefense main screen. Detailed documentation on the new pages is available in the product manual. A new browser tab will open using the single sign-on capability that has been implemented.

Bluetooth 4.0/ BLE 4.0 Security

BLE based tags are increasingly being adopted to provide additional product information and to target sales promotions at shoppers in retail stores. As always, new technologies open up new avenues for attacks. A phishing attack can be launched from a malicious tag that can redirect a guest client device away to a harmful website. Likewise, a misconfigured tag can direct a customer to an incorrect website. This feature attempts to catch and report such events.

The feature works by detecting the URL advertisement in the Google Eddystone protocol using a BLE enabled sensor. Supported AP models are AP 8432, AP 8533, AP 7632, AP 7662 and AP 7612. The allowed URL list is configured in a file. The system generates a new alarm “Bluetooth Beacon using unauthorized URL” on detecting a violation.

Cell Phone Hotspot Detection

Cell phones typically connect to WLAN infrastructure as clients. However, they can also be configured to operate as mobile hotspots, where they operate as Wi-Fi access points. AirDefense 10.0 now classifies such devices as cell phone hotspots. A new alarm “Mobile Hotspot detected” has been added.

Scalability Changes

This release introduces scalability changes to improve UI responsiveness when a large number of devices are seen by the system. For this multiple parallel query executions have been added in the backend. Also, pre and post epoch rolls have been spread across 5 threads (previously 1) to parallelize processing for large numbers of clients. Unsanctioned devices are now aged-out after 6 hours to the forensics database. Additionally, for new installs, a default DAM rule has been added to age-out sanctioned devices not seen more than 5 days to forensics database.

Reporting engine enhancements

This release includes performance optimizations to the reporting engine to speed up report generation. In particular, wireless client inventory and retail analytics reports have been accelerated.

Radioshare WIPS for Extreme Wireless AP 39xx and WiNG AP 76xx

This was introduced post the 9.5 release and did not require changes to the AirDefense appliance or VM firmware. Support for AP 39xx requires EW release 10.41.07 or higher. Support for AP 7612, 7632, 7662 requires WiNG release 5.9.2.1 or higher. Please see the AirDefense 9.5 release notes – they have been updated with appropriate details.

Other Changes

- Older PCI 1.1, 1.2 and 2.0 reports have been removed.
- Locationing (licensed via AD-PROX-P-1) is now EOL and the replacement product is Extreme Location. As a result, the following reports have been removed from pre-defined reports - Presence Analytics, Proximity Region Analytics Legacy, Proximity Region Analytics. Only the reports have been removed, not the locationing engine. So, rogue access point/ rogue client location and location forensics continue to be supported.

2. Version Compatibility

The 10.0.0-14 SM version is upgradable from 9.5.0-11. Direct upgrade from any other version is not supported.

For existing customers who would like to upgrade to 10.0.0-14, AirDefense is an entitled Product and requires a support contract to be in place.

WiNG Version Compatibility

AirDefense 10.0.0-14 SM has been tested for compatibility against

- WiNG 5.9.2.x (see Section 4 - Important Notes)

Please see the section titled “DFS Tables, Sensor and Radio Share” in the corresponding WiNG release notes for a detailed matrix of sensor features supported for each access point in that WiNG release.

Extreme Wireless Version Compatibility

AirDefense 10.0.0-14 SM has been tested for compatibility against

- Extreme Wireless 10.41.08 & Extreme Wireless 10.41.09

ExtremeCloud Appliance Version Compatibility

AirDefense 10.0.0-14 SM has been tested for compatibility against

- ExtremeCloud Appliance 4.26.01

Hardware Appliances

- Model NX-9500
- Model NX-9600

Virtual Platforms

- Xen - Hypervisor 4.1.2 and higher
- VMWare EXSi Hypervisor 5.5, 6.0, 6.5

Supported WiNG Wireless Access Points

- AP 6522, AP 6562
- AP 7161
- AP 7522, AP 7532, AP 7562
- AP 8163
- AP 8533
- AP 8432
- AP 7602
- AP 7622
- AP 7612, AP 7632, AP 7662

For feature support by WiNG release, please refer to the section titled “DFS Tables, Sensor and Radio Share” in the WiNG release notes.

Supported Extreme Wireless Access Points

- AP 3915
- AP 3916
- AP 3917
- AP 3912
- AP 3935
- AP 3965

Supported Browsers

Note that, Flash Player 10.1 or later is required.

- Firefox 32 and higher
- Internet Explorer 9 and higher
- Chrome 37 and higher

Supported OS

- Windows 7 Enterprise
- Windows 10 Enterprise
- Linux
- Mac (Thin Client Applications Only)

3. Installation

Please follow the steps below to upgrade an AirDefense system that is currently running AirDefense 9.5.0-11 firmware. Direct upgrade from any other version is not supported.

- Copy the file AD-service-SM2-10.0.0-14.tar to the /usr/local/tmp folder on the AirDefense server using the smxmgr account. You can use any tool like scp, ssh secure file transfer client, putty etc. for this.
- Login to AirDefense as smxmgr. From the menu select Software and then Servmod and enter the location of the patch file /usr/local/tmp/
- The menu now shows available files. Enter the number corresponding to AD-upgrade-10.0.0-14 and press enter. AirDefense will now install 10.0.0-14.

For full instructions on how to upload the AirDefense image onto an NX and install it successfully please see the Users Guide.

4. Important Notes

1. Backup all config and forensics files prior to upgrade
2. Toolkit will need to be re-installed. Toolkits installed in prior versions should not be reused.
3. Anomalous Behavior Detection thresholds are lost when the system reboots or when services are restarted. Also, Live and Threshold values are shown in the alarm details page while the alarm is in the active state; when the alarm becomes inactive, these values are changed to “unknown”.
4. AirDefense VM – Note that the minimum virtual disk size must be 50GB for the VM solution.
5. Fast Termination with WING 5.9.2: Fast Termination was introduced for South Korea in release 9.4 together with special WiNG release 5.8.6.10. That functionality has been merged into WING 5.9.2 and is now available as GA together with AirDefense 9.5 (or higher) for AP 7522, AP 7532, AP 8432 sensors.
6. With AirDefense 9.4.0 (and higher) SSLv3 (and TLS 1.0, TLS 1.1) communication for sensor to server communication can be turned off completely. For all other communication (e.g. UI/ Toolkit etc.) SSLv3 was disabled in previous releases. By default, SSLv3 communication is left enabled in AirDefense 9.4 to permit communication with legacy sensors. To disable the SSLv3 communication entirely please follow the steps below. Also, note that WiNG 5.8.3 or higher firmware must be used on sensors when SSLv3 is turned off as only those releases support TLS v1.2
 - Login to AirDefense with smxmgr credentials
 - Select the “Config option” (type C)
 - At the end of the menu options, it will show “(SSLv3) Enable/Disable SSLv3 for Sensor-Server Communication”

- Type “SSLv3”
 - The system will display current status of SSLv3 in the system. If it is currently disabled, it will allow the user to enable it.
 - Type E to enable/ D to disable
 - Type Q to quit
 - System will now warn that AirDefense services will need to restart.
 - Type Yes to continue.
 - Once you exit of the WIPAdmin login, the AirDefense service will be restarted
7. With AirDefense 9.2.0 the sensor to AirDefense server communication has been switched to use 2048-bit key length and TLS 1.2. By default, AirDefense will use 2048 key length certificate. In order to fall back to 1024-bit key length (not recommended), please follow the following steps.
- Login to AirDefense as root (contact support for assistance)
 - Touch file /usr/local/smx/.k/key1024
 - Restart AirDefense services.
- Upon restarting AirDefense will now fall back to 1024 bit certificate for sensor-server communication.
- To switch back to 2048 bit certificates:
- Login to AirDefense as root (contact support for assistance)
 - Delete /usr/local/smx/.k/key1024 file
 - Restart AirDefense services.
8. Upgrade from AirDefense 9.0.3 to 9.1.0 (and higher) is not seamless. AirDefense architecture was significantly revised in 9.1 to improve scalability requiring changes to config. Some manual changes may be required to the config to upgrade successfully. It is recommended that upgrades from 9.0.3 be performed via 9.2.0 release – which has enhancements to ease the upgrade.
9. When upgrading firmware to 9.2.0 (from 9.0.3), a config restore MUST be performed using the 9.0.3 backup config file. In several cases, this will help restore config items that might be lost during the upgrade.
10. Alarm action manager profiles – exception option has been removed from GUI in 9.1.2 and added to the advanced filter.
11. By default, notification emails are sent once every 5 minutes. E.g. To increase this to one day emails - change the repetition periods as follows:
In file /usr/local/smx/notification/lib/notification.properties,
email.repetitionPeriod = 86400 // In seconds; Default = 300 seconds
syslog.repetitionPeriod = 86400 // In seconds; Default = 300 seconds
Restart AirDefense after the file is modified for the changes to take effect.
12. Bluetooth Beacon using unauthorized URL: EddyStone URLs are validated against the configured URLs in /usr/local/smx/etc/adbleurl.conf file. Advertised URLs from EddyStone BLE beacons are validated against these allowed URL list for checking whether authorized or not. AirDefense will check the sensed URL from beacons against the configured URLs and trigger an alarm if any violation is detected. There are two types of configurations allowed.
- a. List of allowed URLs
 - b. Allowed URLs for a specific BLE beacon mac address [Note: there is no short mac address and tiny URL's are not allowed]

5. SPR/Issues Fixed

The following SPRs/ CQs have been fixed in this release.

SPR/ CQ	Description
SPR-3413	Device Action rule filters reset when using "Not in" expression
SPR-3433	AirDefense - "station_pol_essid" filter not working correctly on custom reports
SPR-3449	"Redundant power supply failure" alarm is not triggered for NX9600
SPR-3466	Incorrect vendor name on wireless client csv export
SPR-3479	Cannot add temporary licenses to an active licensed system
SPR-3480	DeviceType filter in AAM incorrect BITMASK value

6. Vulnerabilities Fixed

Vulnerabilities Fixed in AirDefense 10.0

AirDefense 10.0 includes upgrades to several internal packages (including kernel to: 2.6.32-754.2.1, microcode_ctl: 1.17-33.1 and Java) to provide fixes for several vulnerabilities including:

- CVE-2018-10675
- CVE-2018-10872
- CVE-2018-1130
- CVE-2018-3639
- CVE-2018-3665
- CVE-2018-5803
- CVE-2017-1000111
- CVE-2017-1000112
- CVE-2017-1000251
- CVE-2017-1000253
- CVE-2017-1000364
- CVE-2017-1000410
- CVE-2017-11176
- CVE-2017-12190
- CVE-2017-13166
- CVE-2017-14106
- CVE-2017-15121
- CVE-2017-18017
- CVE-2017-18203
- CVE-2017-2636
- CVE-2017-2671
- CVE-2017-5715
- CVE-2017-5753
- CVE-2017-5754
- CVE-2017-6001
- CVE-2017-6214
- CVE-2017-7308
- CVE-2017-7541
- CVE-2017-7542
- CVE-2017-7616
- CVE-2017-7889
- CVE-2017-7895
- CVE-2017-8824
- CVE-2017-8890
- CVE-2017-9074
- CVE-2017-9075
- CVE-2017-9076
- CVE-2017-9077
- CVE-2016-7910
- CVE-2016-8650
- CVE-2015-8830
- CVE-2012-6701

Vulnerabilities Fixed in AirDefense 9.5

AirDefense 9.5 includes upgrades to several internal packages to provide vulnerability fixes (including kernel to 2.6.32-696.10.1, nss, bind, ca-certificates, glibc, jasper, openldap, rpcbind and sudo)

Vulnerabilities Fixed in AirDefense 9.4

AirDefense 9.4 includes upgrades to several packages (including bindlibs, bindutils, kernel, openssh, openssl) and fixes the vulnerabilities below.

- CVE-2017-6074
- CVE-2017-3136
- CVE-2017-3137
- CVE-2016-7545
- CVE-2015-8325
- CVE-2010-5107

Vulnerabilities Fixed in AirDefense 9.3

AirDefense 9.3 includes upgrades to several packages (including kernel, openssh, openssl, nss, ntp, glibc, perl etc.) and additionally fixes the vulnerability below.

- CVE-2016-2107

Vulnerabilities Fixed in AirDefense 9.2

AirDefense 9.2 includes upgrades to several packages (including openssh, openssl, Java and Tomcat) – fixing the vulnerabilities below:

- NTP Vulnerability CVE-2015-7871
- OpenSSL vulnerabilities - CVE-2015-3194, CVE-2015-3195, CVE-2015-3196, CVE-2015-3197
- OpenSSH vulnerability - CVE-2016-3115 (X11 forwarding)

Vulnerabilities Fixed in AirDefense 9.1.3-10b6

- glibc: getaddrinfo stack-based buffer overflow CVE-2015-7547

Vulnerabilities Fixed in AirDefense 9.1.3-10a8

- OpenSSL vulnerability – LOGJAM - CVE-2015-4000

Vulnerabilities Fixed in AirDefense 9.1.3-10

- GHOST CVE-2015-0235
- Unzip Multiple Heap Buffer Overflows Vulnerabilities - Zero Day CVE-2014-8139, CVE-2014-8140, CVE-2014-8141
- OpenSSL vulnerabilities security advisory dated - 11 Jun 2015 (see http://openssl.org/news/secadv_20150611.txt), CVE-2014-8176, CVE-2015-1789, CVE-2015-1790, CVE-2015-1791, CVE-2015-1792, CVE-2015-3216
- OpenSSH vulnerabilities - CVE-2014-2532, CVE-2014-2653

Vulnerabilities Fixed in AirDefense 9.1.2-17a6

- NTP vulnerabilities 2014-9293, 2014-9294, 2014-9295, 2014-9296
- Bash shellshock CVE-2014-6271, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187, CVE-2014-6277 and CVE 2014-6278

- Poodle SSLv3 CVE 2014-3566

7. Known Issues and Recommendations

General note for EW 39XX series access points:

- Support for Extreme Wireless Access Points has been added beginning with the AirDefense 9.5 release. Therefore, any upgrade issues from prior releases documented in the “Upgrade Related” section are not applicable.
- As features supported for EW 39xx access points are WIPS, Advanced Forensics and Liveview, known issues in the Network Assurance, Proximity and Bluetooth sections below are not applicable to these access points.
- As EW 39xx access points are only supported as dedicated sensors in this release, all issues related to radio-share are not applicable.
- Any WING sensor specific issues documented below are not applicable to Extreme Wireless access points.

Issues specific to EW access points

- The following alarms do not trigger on EW AP 39XX –Fake AP flood attack, AirSnarf (3912, 3915)

Upgrade related

- In 9.1.x Device/Alarm action manager, None(Any) filter and None(All) filters were reversed compared to 9.0.3. This is fixed in 9.2.
 - If upgrading from 9.0.3 – this conversion happens automatically when restoring the 9.0.3 config
 - If upgrading from 9.1.x - Any rules that were deliberately reversed by the administrator after upgrading from 9.0.3 to workaround such configs need to be reversed manually on upgrading to 9.2 (after restoring the config)
- Alarm action Manager: In AirDefense 9.1 and higher releases a maximum of 25 filters are supported in the filter list as well as in the expression filter list.
- Alarm Action Manager rule descriptions may not be preserved on upgrade to 9.1 and higher releases.
- Alarm Action Manager: In some cases, on upgrade from 9.0.3 to 9.2 you may see special characters in expression filters (e.g. ‘%’ or ‘)’) in the advanced filter expression editor. These characters are needed for internal operation. They do not impact end user functionality and can be ignored from an administrator perspective.
- Device and Alarm Action Managers: On upgrading from 9.0.3 to 9.2, an AAM profile that was left disabled at the global scope appears to be enabled. However, with 9.1 and higher releases, there is a separate “Enable Profile” checkbox to really enable the profile.

Platform

- Custom dashboards created in the old Flex UI will not show up in the new UI.
- The new UI is supported for the admin user in this release. Support for other user roles will be added in a future release.
- New UI - Unknown devices turned into rogue devices widget does not show data. Will be addressed in a future release.

- New UI – In the network snapshot grid, the total BT device count does not match the old UI. Sensor details are missing. Will be addressed in a future release.
- New UI - Radio Bands on WLAN do not show the correct count of WLANs.
- NEW UI: Search filter for the “polled devices” column does not work.
- New UI: BLE device classification widget doesn’t show correct counts.
- The following alarms do not trigger on AP 7612/ 7632/ 7662 - Airsnarf.
- The following alarms do not trigger on AP 7662 - Honeypot, Multipot, Hotspotter and Hunter-Killer.
- AirDefense Toolkit is only supported on Windows. It is not supported on Linux.
- “DeviceVendorprefix,AssociatedVendorPrefix and DeviceManufacturer should be used with the full name when used with =,!=,IN and NOT IN operators”. It is recommended that operators LIKE/ ILKE be used for DeviceVendorprefix,AssociatedVendorPrefix and DeviceManufacturer filters.
- WSP-8561 : CMC Server Unreachable message in tooltip - After adding the CMC appliance to Master AirDefense, it says "Server Unreachable" even though the server is reachable. After some time the “Server Unreachable” message disappears and “login failed” appears. Ignore the unreachable message - go ahead and share the certificate and restart the appliance to get the CMC working.
- NOT IN operator is not supported in AirDefense Alarm Action Manager.
- AirDefense does not generate the alarm "Frequency hopping interference detected" when using AP 7532 as a sensor.
- WIPS-OCS: LiveView does not display frames on channel 1 configured in OCS channel list.
- WIPS: Wipspd (on the AP) sometimes restarts when radio is changed from radio share to dedicated sensor.
- WIPS – Rogue AP Detection – In select cases like enterprise class rogue AP that is set up as a router (not an AP) and the BSSID of the wireless interface is completely unrelated to the MAC address of the wired interface, AirDefense uses a data pattern matching technique to classify the device as a rogue. For the sensor to see the wired side data from the AP, the port on the L2 switch should be configured as a SPAN port. If this is not done, the rogue AP will be marked as an unsanctioned device but AirDefense will not be able to classify it as a rogue.
- Forensics does not show the all of the data when the date range is long (15 days or longer). Workaround is to run multiple reports each of duration less than 15 days.
- Scheduled Configuration or Forensic Backup using TFTP protocol is not supported. Please use FTP or SFTP.
- “Wireless devices overload observed” alarm is only generated on NX 9500 in Standalone AirDefense (not supported on other appliances nor in Unified mode)
- Action Rules on demand discrepancy in Job Status, rules are not applied –Recommendation is - Admin needs to apply the Action Manager rule before running “Action Manager Rules on Demand” option. Action Manager Rule runs every minute by default.
- Job list in job status does not age out after 7 days
- Backup and Restore does not work when the profile name has a space at the end. Edit the profile to remove the extra “space” character.
- When Korean language is selected, the following do not work correctly
 - Cannot delete some SNMP Community settings when others are in use.
 - Unable to display “device name” correctly when number of characters exceeds 10.
- Port suppression fails on an RFS6000
- Backslash in LDAP authenticated user name causes loss of all user permissions on restart of services.

- The CMC slave authentication mechanism has been changed significantly in AirDefense 9.1.0. It is recommended that the user review the on-line help for CMC for a description of how to configure slave servers.
- After adding a Slave Server on a CMC Master Server, the user is not able to view configuration or other pages on the Slave Server from the Master Server because of a permission error. The workaround is to click the Reset button, log out of master server, and restart browser.
- 'Copy settings to all appliances' action in CMC results in GUI application error with numeric value as prefix in profile name.
- Data collection on WiNG 5.2.x devices was changed to occur over SNMP vs HTTPs. Data collection and configuration management requires the communication profile settings for SNMP timeout interval and retry to be set to 9999 milliseconds and 3 retries to avoid excessive timeouts which might disrupt connection resulting in incomplete data collection and device showing as offline when it is not actually offline to the network.
- Data collection set to a short interval may result in devices going offline; it is recommended to set the time between data collections to an interval longer than the time a complete data collection takes.
- SFTP is not supported with the internal relay server, it is only supported with an external relay server.
- The format of the folder for CLI variables must be:
`/<serverName>/<country>/<region>/<city>/<campus>/<building>/<floor>`
For example, `/AirDefense/USA/South/Atlanta/Alpharetta/Atlanta_main/Floor_2`
All other profiles accept the following folder format:
`<country>/<region>/<city>/<campus>/<building>/<floor>`
- CQ 201328 – AP 7532 device icons displayed incorrectly when device goes offline

Network Assurance

- Clearing configuration in Appliance Manager may prevent edits to Live-RF application configuration. If the system gets into this state, please contact the support team or re-install AirDefense.
- Changes to duty cycle field in the Advanced Spectrum Analysis window will cause all channel extensions to be set to 0 on the sensor. A manual stop and start of ASA fixes the issue.
- Cannot schedule Advanced Spectrum Analysis dedicated scan with default values – change atleast one value from default to turn on the OK button.
- The Advanced Spectrum Analysis on AP 6522 displays spurs when the frequency range is extended to cover Channel 14. These spurs cause the Advance Spectrum Analysis alarm "Utilization Exceeded Threshold" to be triggered.
- Spectrum Analysis – On changing chart options Duty cycle, Device count, Spectral density and Real time FFT data is lost. Do not change chart options to preserve existing data.
- AP Test – AP Test with Captive Portal is not supported. It requires a custom plugin to be created for the specific captive portal. Workaround: Use the ping test to verify reachability to the captive portal.
- AP Test – WEP keys entered in ASCII characters prevent successful testing of WEP networks when using M5x0 sensors. WEP keys entered as hex code work fine.
- AP Test – Due to hardware limitations AP testing using EAP-TLS or PEAP-TLS is not supported on the M5x0 sensor platforms.

- AP Test – The AP Test supplicant does not support certificates which are protected with a passphrase, only certificates which do not require a passphrase to access the key are supported.
- AP Test - AP Test scheduled using alarm action manager does not run according to the chosen profile
- AP Test - AP Test license does not get automatically applied when Auto Licensing is selected
- AP Test and Wireless Vulnerability assessment – works at a BSS level only and not at a floor/ scope level.
- AP Test – Scheduled AP Test disappears from menu despite the presence of a radio-share AP Test license. Support can issue an AP test license which will re-enable this functionality.
- AP Test – SPR 27984 - AP-Test with EAP-TLS fails with error message “Network
- AP Test – AP Test Downlink test fails for AP 7522 and AP 7532 with WiNG 5.8.4
- AP Test – AP 8432 and AP 6522 Uplink test fails while running AP test with WiNG 5.8.4
- AP Test – When using TKIP-CCMP , AP 622 acting as a client does not get an IP address via DHCP with WiNG 5.8.4
- Authentication: EAP authentication failed” – has been fixed in WiNG 5.8.1 & higher releases.
- Multiple Vlan IDs cannot be removed – they can only be removed one at a time.
- Live view: SSID and RSSI value do not appear in devices tab occasionally.
- Live RF with AP 75xx is only supported at 11n rates

Bluetooth Monitoring

- Bluetooth Devices imported via a csv file and with a selected folder are placed in unplaced devices folder. They are moved to the correct folder when the device is seen
- Some Eddystone tags have non-standard fields and may not be correctly recognized by the AP. Some tags do not advertise a URL in the beacon – such tags cannot be protected with the BT 4.0/ BLE security feature. The following tags have been tested against AirDefense:
 - Kartographer eddystone beacons – UFOBeacon Odyssey
 - Ibeacons – used Wing Devices as advertisers. Apple ibeacons were also sensed.
 - BLE simulator app – TxEddystone
 - BLE Scanning app -- Beacon simulator
- Some tags advertise additional “.com”'s in the URL field. This does not impact URL matching, however, they will show up in the alarm description text.

8. AirDefense WiNG Feature Matrix

This section defines features supported by access point/ sensor module.

As a dedicated sensor	WIPS & Advanced Forensics	Spectrum Analysis	Advanced Spectrum Analysis	Live RF	Live View	AP Test	Connecti on Troubles hooting	WVA
AP 6522/6562	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
AP 7161	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
AP 7532/7522/7562¹	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
AP 8163	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
AP 8533²	Yes	No	Yes	No	Yes	Yes	Yes	Yes
AP 8432²	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
AP 7602/7622	Yes	No	No	No	No	No	No	No
AP 7632/ 7662/ 7612¹	Yes	No	No	No	Yes	No	No	No

Notes:

¹AP 7522, AP 7532, AP 7562, AP 7632, AP 7662, AP 7612 radios are band-locked, entire AP needs to be dedicated as sensor

²Support is limited to the dedicated sensor (Radio 3) for AP 8533. For AP 8432 – either Radio 1 can be used as a dedicated sensor and Radio 2 for data or the entire AP can be dedicated as sensor.

3. Radio Share functionality (allows for enabling the Network Assurance toolkit in AirDefense, without dedicating a radio as a sensor) is available on the 802.11n/802.11ac APs with some caveats – please see details below:

In Radio Share mode	WIPS & Advanced Forensics	Spectrum Analysis ²	Advanced Spectrum Analysis ³	Live RF	Live View	AP Test ⁵	Connecti on Troubles hooting	WVA
AP 6522/6562¹	No	No	Yes	Yes	Yes	Yes	Yes	No
AP 7161	No	No	No	Yes	Yes	Yes	Yes	No
AP 7532/7522/7562⁴	Yes	No	No	Yes	Yes	Yes	Yes	No
AP 8163	No	No	Yes	Yes	Yes	Yes	Yes	No
AP 7502	No	No	No	No	No	No	No	No
AP 8533	No	No	No	No	No	No	No	No
AP 8432	Yes	No	No	No	Yes	Yes	Yes	No
AP 7602/7622	No	No	No	No	No	No	No	No
AP 7632/ 7662/ 7612⁴	Yes	No	No	No	Yes	No	No	No

Notes:

¹AP 6522, 6562 – The first radio is band-locked to 2.4Ghz. The second radio is capable of ABGN sensor operation.

- In Radio 1 = Sensor, Radio 2 = Wlan configuration, the sensor will only scan 2.4Ghz channels on Radio 1.
- In Radio 1 = Wlan , Radio 2 = Sensor configuration, the sensor will scan both bands on Radio 2

- In Radio 1 = Sensor, Radio 2 = Sensor configuration, the sensor will scan 2.4GHz on Radio 1 and 5GHz on Radio 2

²Spectrum Analysis is not supported with Radio share enabled.

³Advanced Spectrum Analysis in RadioShare mode may impact WLAN performance.

⁴AP 7522, AP 7532, AP 7562, AP 7632, AP 7662, AP 7612 radios are band-locked, both radios are required for sensing

⁵AP Testing in radio share mode - only single-cell/internal BSS AP testing is supported. AP Testing on remote BSS is not supported.

9. AirDefense Extreme Wireless Feature Matrix

For the EW 39xx series access points operating as dedicated sensors, AirDefense supports the following features:

- WIPS
- Advanced Forensics
- Liveview

AirDefense also supports the following features for AP 39xx operating as radio-share sensors.

- WIPS
- Advanced Forensics

© Extreme Networks. 2018. All rights reserved.