

## AirDefense 10.3.0-05 Release Notes

<b>AirDefense 10.3.0-05 Release Notes</b> .....	<b>2</b>
<b>1. New Features in AirDefense 10.3.0-05</b> .....	<b>2</b>
<b>2. Version Compatibility</b> .....	<b>4</b>
Firmware Version Compatibility .....	4
Extreme Wireless Version Compatibility .....	4
ExtremeCloud Appliance Version Compatibility.....	5
Hardware Appliances.....	5
Virtual Platforms.....	5
Supported WiNG Wireless Access Points and Firmware version .....	5
Supported Extreme Wireless Access Points .....	5
Extreme Switch Compatibility .....	6
Supported Browsers .....	6
<b>3. Installation</b> .....	<b>6</b>
<b>4. Important Notes</b> .....	<b>6</b>
<b>5. SPR/Issues Fixed</b> .....	<b>9</b>
<b>6. Vulnerabilities Fixed</b> .....	<b>9</b>
<b>7. Known Issues and Recommendations</b> .....	<b>12</b>
Pre-requisites for multicore configuration .....	12
Issues specific to EW access points .....	12
Upgrade related .....	12
Platform .....	13
Network Assurance.....	14
Bluetooth Monitoring.....	15
HTML5 UI .....	15
WIPADMIN CLI .....	16
<b>8. AirDefense WiNG Feature Matrix</b> .....	<b>16</b>
<b>9. AirDefense Extreme Wireless Feature Matrix</b> .....	<b>17</b>

## AirDefense 10.3.0-05 Release Notes

### 1. New Features in AirDefense 10.3.0-05

The AirDefense 10.3.0-05 (service module) release introduces the following key features and functionalities:

- 802.11ax support for tri-radio access points - 400 series APs (410i/e & 460i/e)
- WPA3 support for legacy Broadcom based APs (based on WiNG 7.2.1 support)
- Support Auto-Sensor functionality for tri-radio APs
- Syslog enhancement

#### Tri-radio 802.11ax support - 400 series APs (410i/e & 460i/e)

- As part of WiNG 7.3.0 software release, 802.11ax support is further enhanced for tri-radio 400 series APs. This feature in AirDefense is to support WIPS functionality along with sensing devices operating in 802.11ax protocol for third radio which is utilized as dedicated sensor. The AirDefense server can detect and classify these devices that support the 802.11ax protocol. Also, this release enhances Liveview support with 802.11ax frames being parsed and then shown in detail.

#### WPA3 for legacy Broadcom APs (based on WiNG 7.2.1 support)

As part of 7.2 software release, the WPA3 support is introduced in 500 series APs (505i, 510i/e, 560i/h). Now this feature in sensor extended to legacy Broadcom WiNG APs. This feature in AirDefense is to support sensing devices operating in WPA3 environments. AirDefense Server is capable in detecting those devices and generate alarms related to that. The alarms supported are

- Device operating in WPA3-SAE without PMF
- Sanctioned WPA3 SSID name same as Unsanctioned WPA2 BSS
- WPA3 Client trying Association with WPA2 BSS
- WPA3 SAE Transition Mode Device
- WPA3 client roamed from WPA3 to WPA2/Open
- SAE Capable Device
- OWE Capable Device

#### Support Auto-Sensor functionality for Tri-radio APs

- This functionality enables automated assignment of sensor licenses without requiring customer intervention. System leverages RF environment knowledge to automatically provision ADSP Sensors (dedicate 3<sup>rd</sup> radio for tri-radio APs) in the given RF Domain using Smart-RF Neighbor reports
  - In AirDefense this will auto-assign sensor role to tri-radio APs during initialization
  - AirDefense server provides an additional option in license management to enable license auto re-assignment on demand. This feature should be enabled only if controller/sensor supports smart sensor functionality. Today this is manually enabled if user has selected smart sensor functionality in controller.

- For this feature to work admin should also enable auto-licensing feature on AirDefense UI.

In this release, this feature is supported only for tri-radio AP410i/e and 460i/e

#### Syslog Enhancement

- Activity logs in AirDefense stored in our internal database and provided through reports on-demand.
- Customer requested to send these activity logs as and when occurs to remote syslog feature
- Option to enable/disable this feature and add IP address of the syslog server is provided at appliance level.
- This feature is independent and not to be interlinked with Action Manager option. The action manager continues to be configured to report the alarms and devices as it was done before.

## 2. Version Compatibility

The 10.3.0-05 SM version is upgradable from 10.2.1-07. Direct upgrade from any other version is not supported.

For existing customers who would like to upgrade to 10.3.0-05, AirDefense is an entitled Product and requires an active support contract.

### Firmware Version Compatibility

AirDefense 10.3.0-05 SM has been tested for compatibility against

- WiNG 7.3.0
- WiNG 7.3.0.1 (with XCA)
- Identify 10.51.10
- XCA 4.76.01

### Supported Sensor Model and Interop Build version validated

Sensor Model	WING Interop build
AP 7522, AP 7532, AP 7562	WING 7.3.0/7.3.0.1
AP 8533	WING 7.3.0/7.3.0.1
AP 8432	WING 7.3.0/7.3.0.1
AP 7602/AP 7622	WING 5.9.5.0
AP 7612, AP 7632, AP 7662	WING 7.3.0/7.3.0.1
AP 505	WING 7.3.0/7.3.0.1
AP 510, AP 560	WING 7.3.0/7.3.0.1
AP 650/AP6532	WING 5.9.1.6/5.9.1.7
AP 7131	WING 5.9.3.3
AP 6522/AP 6562	WING 5.9.4.1
AP 7161	WING 5.9.3.3
AP 8132	WING 5.8.6.0
AP 8163	WING 5.9.6.0

Sensor Model	Identifi Interop build
AP 3915, AP3917	10.51.10
AP 3935, AP3965	10.51.10
AP 3912, AP3916	10.51.10

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 10.3.0-05 SM has been tested for compatibility against

- Extreme Wireless 10.51.10

### **ExtremeCloud Appliance Version Compatibility**

AirDefense 10.3.0-05 SM has been tested for compatibility against

- Extreme Cloud Appliance 4.76.01

### **Hardware Appliances**

- Model NX-9500
- Model NX-9600

### **Virtual Platforms**

- VMWare EXSi Hypervisor 5.5, 6.0, 6.5

### **Supported WiNG Wireless Access Points and Firmware version**

- 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
- AP 505, AP 510, AP 560
- AP 410, AP 460

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

## Extreme Switch Compatibility

- x440 Switch support summitX-30.4.1.2-patch2-6.xos

## Supported Browsers

Flash Player 10.1 or later is required.

- Firefox 65 and higher
- Chrome 72 and higher

Internet Explorer is not supported

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 10.2.1-07 firmware. **Direct upgrade from any other version is not supported.**

- Copy the file *AD-service-SM9-10.3.0-05.tar* file 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-service-SM9-10.3.0-05* and press [Enter]. AirDefense will now install 10.3.0-05.

For full instructions on how to upload the AirDefense image onto an NX and install it successfully please see the *Extreme AirDefense 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. 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 communications, (for example, UI/ Toolkit etc.) SSLv3 was disabled in the 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. Note that WiNG version 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) item.
  - At the end of the menu options, a “(SSLv3) Enable/Disable SSLv3 for Sensor-Server Communication” item is shown.
  - Type “**SSLv3**”.
  - The system will display current status of SSLv3 in the system. If it is currently disabled, this option 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 out of the WIPsadmin login, AirDefense service will be restarted.
6. From AirDefense version 9.2.0, the communication between sensors and AirDefense server is 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 fall back to 1024 bit certificate for sensor to server communication.
- To switch back to 2048 bit certificates:
- Login to AirDefense as *root* (contact support for assistance)
  - Delete the */usr/local/smx/.k/key1024* file
  - Restart AirDefense services.
7. Upgrade from AirDefense v 9.0.3 to v 9.1.0 (and higher) is not seamless. AirDefense architecture was significantly revised in v 9.1 to improve scalability requiring changes to *config* file. Some manual changes may be required to the *config* to upgrade successfully. It is recommended that upgrades from v 9.0.3 be performed via v 9.2.0 release – which has enhancements to ease the upgrade.
8. When upgrading firmware to v 9.2.0 (from v 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.
9. Alarm action manager profiles – exception option has been removed from GUI in 9.1.2 and added to the advanced filter.
10. 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.
11. 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





## 5. SPR/Issues Fixed

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

SPR/ CQ	Description
AD-11086	Termination not occur when AAM Advanced Filter put Associate Equal to True
AD-11108	CLI device import does not work
AD-10236	Custom Reports/Favorites/Edit Settings/E-mail and/or FTP not retaining Format HTML

## 6. Vulnerabilities Fixed

### Vulnerabilities Fixed in AirDefense 10.3

AirDefense 10.3 includes upgrades to internal packages (including kernel to: 2.6.32-754.25.1 and openssl: 1.0.1e-58) to provide fixes for several vulnerabilities including:

- CVE-2019-14821
- CVE-2018-12207
- CVE-2019-11135
- CVE-2019-0155
- CVE-2019-0154
- CVE-2019-1559

### Vulnerabilities Fixed in AirDefense 10.2

AirDefense 10.2 includes upgrades to several internal packages (including kernel to: 2.6.32-754.18.2, openssh: 5.3p1-124.el6\_10 and etc.) to provide fixes for several vulnerabilities including:

- CVE-2018-10902
- CVE-2018-12126
- CVE-2018-12127
- CVE-2018-12130
- CVE-2018-13405
- CVE-2018-17972
- CVE-2019-1125
- CVE-2019-11477
- CVE-2019-11478
- CVE-2019-11479
- CVE-2019-3896
- CVE-2019-5489
- CVE-2018-15473

### Vulnerabilities Fixed in AirDefense 10.1

AirDefense 10.1 includes upgrades to several internal packages (including kernel to: 2.6.32-754.10.1, openssh: 5.3p1-123.el6\_9 and etc.) to provide fixes for several vulnerabilities including:

- CVE-2018-14634
- CVE-2018-5391
- CVE-2018-5390
- CVE-2018-3693
- CVE-2018-10901
- CVE-2018-3620
- CVE-2018-7566
- CVE-2018-1000004
- CVE-2016-6210

#### 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](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

- AP5XX sensors do not show supported protocols as “ax” even though these access points are capable of supporting the protocol.

### 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.
- Any WING sensor specific issues documented below are not applicable to Extreme Wireless access points.

### **Pre-requisites for multicore configuration**

- All the floors in the same building should be created under one area of network tree structure
  - This is mandatory as not doing so will result in devices being seen multiple times and may result in undefined WIPS behavior
- Auto-placement rules are mandatory for network devices placement
  - Messages from sensors in unplaced folder will not be processed
  - Polled devices in unplaced folder will not be considered for any WIPS processing
  - Do not manually move Sensor/AP within your network tree if these devices were placed using auto-placement rules.
- 

### **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 filers (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

- BSS/WC termination is not happening on DFS channels using AP410 sensor
- AP Test is failing with WPA2 security mode using AP410 sensor
- Those sanctioned wireless clients not seen in your network for more than 10 days will not be shown in the UI till they sensed or polled again. This duration can be configured via *airids.conf* parameter.
- Import devices via CLI will not be able to place the devices based on firmware version filter in Auto placement rule.
- Moving BT\_Sensor between floors will not move the respective BT/BLE devices.
- Custom dashboards created in the old Flex UI will not show up in the new UI.
- 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: WipSD (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

- In AP505, liveview is not showing any data when it is enabled in radioshare mode
- 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.

### HTML5 UI

- Networks/Dashboard/Alarm tabs appear even though the licenses are removed
- In Network page, polled device count mismatch, neighboring bss/wireless client are not computed properly.
- In user management, custom profile permissions do not get updated in user associated with that custom template. The workaround for this issue to modify at individual user level

- In License management page, Delete Devices in License Assignment screen does not delete these devices as expected. The UI shows these devices as being deleted successfully. However, these devices are not deleted and their license will not get released. To work around this issue, use the legacy UI for releasing these licenses.
- In the new user work flow, creation of Discovery Profile with SNMP fails. Use the *Advanced Configurations* option to overcome this issue.
- The image is broken in Mozilla Firefox in the toolkit download page.
- 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.

#### WIPSADMIN CLI

- In CLI, execution of some commands throws some exceptions as file not found error for logs. This can be ignored, and the requested function will be executed and provide the results as expected.

## 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 7532/7522/7562 <sup>1</sup>	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
AP 8163	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
AP 8533 <sup>2</sup>	Yes	No	Yes	No	Yes	Yes	Yes	Yes
AP 8432 <sup>2</sup>	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
AP 7602/7622	Yes	No	No	No	No	No	No	No
AP 7632/ 7662/ 7612 <sup>1</sup>	Yes	No	No	No	Yes	No	No	No
AP 505/ 510/ 560 <sup>6</sup>	Yes	No	Yes	No	Yes	Yes	No	Yes
AP 410/460	Yes	No	No	No	Yes	Yes	No	Yes

Notes:

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

<sup>2</sup>Support 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 <sup>2</sup>	Advanced Spectrum Analysis <sup>3</sup>	Live RF	Live View	AP Test <sup>5</sup>	Connecti on Troubles hooting	WVA
AP 6522/6562 <sup>1</sup>	No	No	Yes	Yes	Yes	Yes	Yes	No
AP 7161	No	No	No	Yes	Yes	Yes	Yes	No
AP 7532/7522/7562 <sup>4</sup>	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/ 7612 <sup>4</sup>	Yes	No	No	No	Yes	No	No	No
AP 505/ 510/ 560 <sup>6</sup>	Yes	No	No	No	Yes	No	No	No

Notes:

<sup>1</sup>AP 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

<sup>2</sup>Spectrum Analysis is not supported with Radio share enabled.

<sup>3</sup>Advanced Spectrum Analysis in RadioShare mode may impact WLAN performance.

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

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

<sup>6</sup>WIPS, Advanced Forensics and Liveview are only supported in centralized mode with AP5XX

## 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