ADSP 9.4.0-11 Release Notes

ADSP 9.4.0-11 Release Notes

1. New Features in ADSP 9.4.0-11

The ADSP 9.4.0-11 release introduces the following key features and functionalities:

- Anomalous behavior detection with dynamic per site thresholding
- Fast Termination Support (for country South Korea).
- WPS Detection
- Support for Huawei Controllers (model: AC-6005).
- WIPS Support for AP 7602 and AP 7622.

Anomalous Behavior Detection

ADSP collects several stats per device (BSS/ Client) using polled sensor data. This data is used to establish a per-site threshold during a “learning phase”. Learning is done by reading forensics data for the last 15 days. Learning establishes a separate threshold for each hour of the day per site. Once learning is complete, live data is compared against the previously established site threshold. When actual data exceeds the previously established threshold for that hour, the corresponding anomalous behavior alarm is generated. The learning phase repeats over time using a sliding window scheme, adjusting to changing traffic behavior with time.

The following new alarms are added in the ADSP 9.4.09 release:

- MU Management Frame Anomalous Behavior frames
- MU Data Frame Anomalous Behavior frames
- MU Control Frame Anomalous Behavior frames
- AP Management Frame Anomalous Behavior frames
- AP Data Frame Anomalous Behavior frames
- AP Control Frame Anomalous Behavior frames
- MU Management Frame Anomalous Behavior bytes
- MU Data Frame Anomalous Behavior bytes
- MU Control Frame Anomalous Behavior bytes
- AP Management Frame Anomalous Behavior bytes
- AP Data Frame Anomalous Behavior bytes
- AP Control Frame Anomalous Behavior bytes
- AP Anomalous number of Associated MUs

The feature is configured by creating a Performance Profile and enabling that profile at a Site/Building/Floor level. See the ADSP User Guide for additional details.

Fast Termination

The ADSP 9.4.0-11 release adds support for Fast Termination for AP 8432, AP 7532 and AP 7522. Support is limited to these access points to be used together with WiNG 5.8.6.10 firmware. In addition, AP 650 is also supported with the same firmware but is limited to normal termination (no fast termination). This release is limited to South Korea and is not available for use in other countries.

This release provides Fast termination for following alarms:

- Unsanctioned BSS alarm
- Wireless Client Accidental Association
- Rogue AP on Wired Network
- Rogue Client
- Rogue AP on Sensor Segment
- Rogue Client on Sensor Segment
- Ad-Hoc Connection between Sanctioned Stations
- Ad-Hoc Networking Extrusion Detected
- Ad-hoc Network Violation Unsanctioned Client
- Wi-Fi Direct Group Owner Alarm. Termination action for the 3 alarms below is triggered using the “group owner” alarm. This alarm is only generated in Fast Termination mode (FTMODE below is enabled)
    a. Wi-Fi Direct Network Violation Unsanctioned Client
    b. Wi-Fi Direct Network Violation Sanctioned Client
    c. Wi-Fi Direct Extrusion Detected
- Unauthorized roaming

The following functionalities are also included:

- Increased termination scalability by performing termination through a primary sensor - eliminating duplicate entries on other sensors that also see the rogue device.
- Increased termination scalability identifying BSSs which do not have any clients associated with them and reducing the time such BSS stay in the termination table.

Enable Fast termination from CLI as follows.

- Login using smxmgr from ADSP machine
- Go to Config
- In Config menu, type FTMODE
- The screen will display the current status of the Fast Termination mode
- Select Enable/Disable the FTMODE

Once you change the FTMODE status, the user is warned as ADSP services will restart to take effect. The system will restart automatically once you save the state and come out of WIPSadmin console.

Note: Fast Termination configuration is not retained on upgrade from 9.1.3-10d3 service release to 9.4.0-11 (via 9.2→9.3→9.4). FTMode needs to be enabled via CLI as above, restart ADSP services and enable it in the GUI.

WPS Detection

Wi-Fi Protected Setup (WPS) is typically implemented on consumer Wi-Fi devices to simplify setup of such home networks. Presence of WPS makes the network vulnerable to breaches. ADSP 9.4 adds the capability to detect the presence of WPS enabled access points in the network and generates a new alarm (WPS enabled for AP). As before, Alarm action manager rules can also be configured to automatically disallow client associations to such BSS.

Support for Huawei Controllers

This feature adds the capability to poll Huawei controller (model: AC-6005) via SNMPv2 to auto-sanction adopted access points and adopted clients adopted to that controller. This is similar to previously supported import of polled data from WiNG NX controllers. SNMPv3 based import has not been tested and is not supported in this release.

WIPS Support for AP 7602 and AP 7622
ADSP 9.4 also supports WIPS and Advanced Forensics features for AP 7602 and AP 7622 access points together with WiNG 5.8.4.21.

2. Version Compatibility

The 9.4.0-11 SM version is upgradable from 9.3.0-09. Direct upgrade from any other version is not supported.

For existing customers who would like to upgrade to 9.4.0-11, ADSP is an entitled Product and requires a support contract to be in place.

WiNG Version Compatibility

ADSP 9.4.0-11 SM has been tested for compatibility against

- WiNG 5.8.6
- WiNG 5.8.6.10 (limited to South Korea).
- WiNG 5.8.4.21 (for AP 7602 and AP 7622)

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.

Unified Mode Migration Backup Restore

Unified Mode is EOL and no longer supported - 9.1.3-10 was the last ADSP release supporting Unified mode. We recommend that existing unified mode customers looking for fixes/ support migrate to standalone mode.

To upgrade a Unified mode installation from 9.1.2/ 9.1.2a6, use the following procedure

- Upload the 9.1.3-10.tar unified mode firmware file to “/usr/local/tmp” – you can use a tool like WINSCP for this.
- Use “virtual-machine console adsp” on the NX-9500
- use WIPSadmin -> Software -> Servmod command to install the upgrade

Standalone Direct Backup Restore 8.x and above

Direct Backup Restore is supported from 8.x and above.

Standalone Direct Backup Restore 7.x

A 7.3.4 backup can only be restored to an 8.x system. If this is done with the intention of going to a 9.x system, the 8.x system should be checked to assure the restore is correct prior to moving on.

When restoring from a 7.x version, Group Folders from 7.x will become Building Folders in ADSP, and Location Folders from 7.x will become Floor Folders in ADSP. Also, not all 7.x floor plan formats are supported in ADSP, and unsupported floor plans will not be restored.

Any 7.x system prior to 7.3.4 should be upgraded to 7.3.4 prior to taking a backup to be restored into ADSP.

Hardware Appliances

- Model NX-95x0
- Model SV-3652
- Model SV-1252

Note: ADSP 9.0.x and later do not support legacy appliances without 64-bit OS support. Customers that have a 32-bit server cannot upgrade beyond 8.1.3

Note: ADSP 9.1.x and later do not support legacy appliances without 2GB of RAM or greater. Customers that have a 1GB server cannot upgrade beyond 9.0.3.

Virtual Platforms

- Xen - Hypervisor 4.1.2
- VMWare - vSphere 5.5 & 6.0 (ESXi)

Supported Access Points

- AP 6511
- AP 621, AP 6521
- AP 7131, AP 7161, AP 7181
- AP 650, AP 6532
- AP 622, AP 6522, AP 6562
- AP 7522, AP 7532, AP 7562
- AP 8122, AP 8132, AP 8163
- AP 8232 (with 3rd radio sensor module only)
- AP 8533
- AP 8432
- AP 7602
- AP 7622
- TW 511

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

For details on the supported APs/switches, refer to “ADSP Infrastructure Management Supported Devices” on the Support Central.

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

3. Installation

Please follow the steps below to upgrade an ADSP system that is currently running ADSP 9.3.0-09 firmware. Direct upgrade from any other version is not supported.

- Copy the file AD-service-SM3-9.4.0-11 .tar to the /usr/local/tmp folder on the ADSP server using the smxmgr account. You can use any tool like scp, ssh secure file transfer client, putty etc. for this.
- Login to ADSP 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-9.4.0-11 and press enter. ADSP will now install 9.4.0-11.

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

4. Important Notes

Upgrade from ADSP 9.0.3 to 9.1 (and higher) is not seamless. ADSP 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.

1. With ADSP 9.4.0 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 ADSP 9.4 to permit communication with legacy sensors. To disable the SSLv3 communication 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 those releases support TLS v1.2
   - Login to ADSP 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 ADSP services will need to restart.
   - Type Yes to continue.
   - Once you exit of the WIPSadmin login, the ADSP service will be restarted
2. ADSP 9.4 toolkit will need to be re-installed. Toolkits installed in prior versions should not be reused with 9.4.
3. With ADSP 9.2.0 the sensor to ADSP server communication has been switched to use TLS 1.2 and 2048 bit key length. By default ADSP will use 2048 key length certificate. In order to fall back to 1024 bit key length, please follow the following steps.
   - Login to ADSP as root (contact support for assistance)
   - Touch file /usr/local/smx/.k/key1024
   - Restart ADSP services.

   Upon restarting ADSP will now fall back to 1024 bit certificate for sensor-server communication.

   To switch back to 2048 bit certificates:
   - Login to ADSP as root (contact support for assistance)
   - Delete /usr/local/smx/.k/key1024 file
   - Restart ADSP services.
4. 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”.
5. If NIC Bonding is being used, please follow the procedures described in the 9.1.2 release notes in the “Hotfix for Ethernet NIC Bonding Issue” section prior to upgrading.
6. Backup the 9.0.3 config and forensics files prior to upgrade

7. After the firmware has been upgraded to 9.2.0, 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.
8. Branding related changes -
    - Branding has been changed from Motorola to ADSP.
    - The new default values for 9.1.3, where changed from prior releases, are defined in the "ISO / VM New 9.1.3 install" – the second column in the table below
    - When the administrator replaced a default parameter value with a new value prior to the upgrade to 9.1.3, that value is preserved on the upgrade to 9.1.3. When the parameter was left at its default value, it is replaced with the new 9.1.3 default. This is defined in more detail in the remaining columns (under Upgrade)
    - When a config backup from a prior release is restored on 9.1.3, the certificates and passwords that are in that config backup will be restored. If this backup file contains motorola, this will NOT be automatically replaced with ADSP during the backup restore.
    - MAC OUI changes – Client devices that were previously identified as Motorola devices based on their vendor prefix will now be identified as Zebra devices
    - Uploaded WiNG firmware images will be matched against Zebra device types
    - Planned devices under LiveRF will be placed under Zebra.
    - Device Action Manager rules with filter 'DeviceManufacturer' value "Zebra Technologies Inc." will need to be manually updated to "Extreme Networks" for these rules to work correctly. Due to the multitude of combinations of expressions in which these may appear, it is not possible to automatically update these correctly in the internal database.

Parameter	**ISO / VM New 9.1.3 install**	**Upgrade**	
		From 9.1.2/ 9.1.2a6	**To 9.1.3**
Server (self signed) certificate	CN=ADSP (default)	CN=Motorola (default)	CN=ADSP (default)
		Own - non-default	Own (unchanged)
admin password	admin123 (default)	motorola (default)	admin123 (default)
		Own - non-default	Own (unchanged)
CLI Configuration Name	Zebra (default)	Motorola (default)	Zebra (default)
		Own - non-default	Own (unchanged)
Device Firmware - Device Type	Zebra (default)	Motorola (default)	Zebra (default)
		Own - non-default	Own (unchanged)
Communication Settings - Template Name	Zebra (default)	Motorola (default)	Zebra (default)
		Own - non-default	Own (unchanged)
Default communication profile – snmpv3 password	admin123 (default)	motorola (default)	admin123 (default)
		Own - non-default	Own (unchanged)

9. Radio 2 cannot be used as a sensor on EU SKUs for AP 622/ 6522/ 6562, use Radio 1 instead.
10. Auto classification, Location Tracking and Device Management scheduled events in 9.0.3 appear to be missing in 9.1 and higher releases – they are really not missing -
    - Auto classification events are merged in Device Action Manager rules
    - The 4 Device Management Poll events have been renamed to 2 Status Poll events and 2 Data Poll events. These 4 events are scheduled by ADSP.
    - Location Tracking Engine Poll has been removed. This is ADSP scheduled event.
11. Upgrades and config pushes for WiNG controllers should be done using WiNG mechanisms. This functionality is not supported by ADSP.

12. Alarm action manager profiles – exception option has been removed from GUI in 9.1.2 and added to the advanced filter.
13. ADSP VM – Note that the minimum virtual disk size must be 50GB for the VM solution.
14. 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 ADSP after the file is modified for the changes to take effect.

5. SPR/Issues Fixed

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

SPR/ CQ	Description
3270	Radio Share WIPS license does not enable manual termination menu
3291	TLS 1.0 / 1.1 also disabled for sensor to server communication.
3292	Fixed CVE-2017-6074 - a use-after-free vulnerability
3295	Online help references an incorrect version of the user guide.
3304	Disabled unused port 80 (http)
3317	Removed SSH Arcfour weak algorithms
3320	Not deleting the security profile from postgres database after deleting the device.

6. Vulnerabilities Fixed

Vulnerabilities Fixed in ADSP 9.4

ADSP 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-2015-8325
- CVE-2016-7545

Vulnerabilities Fixed in ADSP 9.3

ADSP 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 ADSP 9.2

ADSP 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 ADSP 9.1.3-10b6

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

Vulnerabilities Fixed in ADSP 9.1.3-10a8

- OpenSSL vulnerability – LOGJAM - CVE-2015-4000

Vulnerabilities Fixed in ADSP 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 ADSP 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

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 now 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 ADSP 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

- “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 ADSP, 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 ADSP Alarm Action Manager.
- CQ 208842 – AP Test Fails when using with 3rd radio sensor module and AP 8232 with WiNG 5.7.1. Works fine with AP 8132 with sensor module, problem is specific to AP 8232. Workaround: Works fine with WING 5.7 – use that instead.
- CQ 208843 –Live view and Termination do not work on channel 153 with 8232 3rd radio sensor module with WiNG 5.7.1. Works fine with AP 8132 with sensor module, problem is specific to AP 8232. Workaround: Works fine with WING 5.7 – use that instead.
- ADSP 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) crashes 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, ADSP 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 ADSP 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 ADSP (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 ADSP 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 retry 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.
- WSP-8562 : ADM6.3.2.5 does not connect to ADSP 9.2 - ADM is old platform and still uses older version of TLS protocol to connect to ADSP server. Starting with release 9.2.0, ADSP has switched to TLSv1.2. To get the older ADM working with the new ADSP, please reach out to support. They will need to perform the following workaround on your server. The Tomcat server in ADSP will need to be re-configured to open up communication with other legacy protocols (SSLv2, TLSv1 and TLSv1.1) using the steps below. Note however, that this will make ADSP vulnerable to attacks.
  - Login as root
  - Change /usr/local/tomcat/conf/server.xml
    Add values to sslProtocols attribute in the connector parameter:
    Change sslProtocols="TLSv1.2" to sslProtocols="SSLv2Hello,TLSv1,TLSv1.1,TLSv1.2"
  - Save and restart Tomcat.
- ADSP Toolkit is only supported on Windows. It is not supported on Linux.
- T5 switch and TW 511 APs – Rogue AP detection does not work with one method:
  - ADSP is not able to learn wired devices in the segment of T5 sensors. So, with out-of-the-box setup, ADSP is not able to detect rouge AP in its network. APs report the wired device MACs they see on its wired interfaces. In ADSP, these devices are listed under ‘unknown devices’ and the ‘On Network’ field of these devices will be listed as ‘Sensor Segment’. With T5 sensors, such devices are not seen in ADSP.
  - If we sanction one of the BSS in same segment, ADSP is able to detect rogue AP.
    ADSP learns wired devices MAC from wireless packets coming out of sanctioned BSS . In ADSP, these devices are listed under ‘unknown devices’ and the ‘On Network’ field of these devices will be mentioned as ‘Authorized AP’. With T5 sensors, once one of the wired devices is detected as from ‘Authorized AP’, rogue AP alarm is generated against unsanctioned APs in the segment.
  - CQ 209106 - T5 v5.3.1 sensor intermittently goes offline when LiveView is running –This issue does not happen with earlier versions of T5 e.g. version 5.2. If you need to use v 5.3.1, the workaround is to configure “sensor.message.timeout.pulse” in

/usr/local/smx/etc/airids.conf. Please reach out to support to implement this workaround as it will require root access.

- When Performance Profiles are enabled, there will be a delay in Fast Termination timings.

Infrastructure Management

- CQ 201328 – AP 7532 device icons displayed incorrectly when device goes offline
- When AP 6521 and AP 6511 devices are upgraded from ADSP, they will be displayed as offline because of the extended time required by the upgrade process. They will complete the upgrade even when time out occurs
- AP 6532 running WiNG 5.4.x with radio-1 configured as a sensor and radio-2 as a RadioShare AP, no frames are sent by RadioShare sensor to ADSP.
- APs cannot be upgraded to any versions between WiNG 5.2.13 and WiNG 5.5 via ADSP using SFTP. FTP is recommended.
- The format of the folder for CLI variables must be:
  /<serverName>/<country>/<region>/<city>/<campus>/<building>/<floor>
  For example, /ADSP/USA/South/Atlanta/Alpharetta/Atlanta_main/Floor_2
  All other profiles accept the following folder format:
  <country>/<region>/<city>/<campus>/<building>/<floor>
- The In-Band sensor configuration of *password* and *sensor-server* parameters will be applied only to default policies/RF domains, but not for new management profile and/or RF domains.
- The firmware upgrade/downgrade process from ADSP fails for WS2000 device on 2.0.0-36R and 2.1.0-35R firmware versions.
- When configuring a device using expansion variable and the Address Field is left blank in RF-Domain, the configuration is not applied on a WiNG device. This occurs only when the internal relay server in the ADSP is set to SFTP.
- Upgrade of Cisco devices which implement SSH version 1.5 are not supported.
- In some cases radio indexes can get out of sync on RFS clusters when using expansion variables to configured the radios and WLANs.
- Upgrade of device firmware to releases ending in “MR” such as 3.2.2.0-015MR will show upgrade failure even when upgrade was successful.
- After changing appliance configuration to allow reception of SNMP traps from infrastructure a warm boot is required before traps will be received.
- The appliance relay server may not always work for WLC based upgrades.
- Help desk account set to read-only access still permits saving/ pushing CLI templates.

Network Assurance

- Clearing configuration in Appliance Manager may prevent edits to Live-RF application configuration. If the system gets into this state please contact support team or re-install ADSP.
- Changes to duty cycle field in the Advanced Spectrum Analysis (ASA) 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 621, AP 6521 and AP 622 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

Proximity & Analytics

- The locationing performance degrades when a floor map exceeds 10,000 sq meters.
- AD Mobile 6.3.1 or later must be used with ADSP 9.1.0 when performing Sensor Survey as ADSP 9.1 requires a live connection between AD Mobile and the ADSP appliance during the Sensor Survey.
- A warm boot is required when 3rd party system communication settings are changed in existing LBS Subscriber profiles.
- API - The API LBSClient no longer caches the streaming data by default. It assumes that it will receive data from ADSP and immediately forward the data to a registered LBSStreamListener object. To help 9.0.0-23 clients migrate to 9.0.1/9.0.2, the 9.0.0-23 APIs were left in place but they do not accumulate data unless instructed to by a call to LBSClient.enableStreamingEventsCache. This affects: 'LBSClient.getNewLocations', 'LBSClient.getPresenceEvents', 'LBSClient.getRegionEvents', and 'LBSClient.getRssiData'.
- API - returns location information in meters only
- RTLS Engine - If there are a large number of buildings with location tracking enabled it can take several minutes for the location tracking engine to load its cache. This occurs at startup or warm boot of the system. Live RF/Floor Plan will not display station locations and the LBS data will not be seen from the API until the load is complete.
- RTLS Engine - BSS locations are not tracked in real-time.

- Live RF/Floor Plan - Within a Virtual Region or Exclusion Region type bounding areas cannot be deleted or edited individually. If one bounding area needs to be deleted or edited then the entire Region definition must be deleted. A Virtual Region or Exclusion Region type can be created for each bounding area if desired.
- CQ 108132 – GUI error in Sensor Operation when saving configuration if nothing has been selected. Atleast one of the check boxes needs to be checked.
- Performance slows down after 2 days of running with 2500 sensors of which 1500 are LBS sensors. Other performance issues are seen with LBS approaching peak specified platform capacity. This will be addressed in a future release.
- Proximity reports can be run for a maximum of 150,000 devices. If its necessary to scale beyond this, please split into multiple reports.
- Proximity: Wireless clients are not seen on the floor plan for AP 650 and AP 622 with WING 5.8.4.

Bluetooth Monitoring

- Bluetooth device types are reported to ADSP via the IOGear Bluetooth dongle, ADSP can display but cannot control what device types are reported.
- Bluetooth Alarm: The Device column is shows incorrect information in alarm notification
- 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

8. ADSP Feature Matrix

This section defines features supported by access point/ sensor module. TW 511 is not supported in WiNG.

Network Assurance Toolset when Radio is dedicated as a sensor	WIPS	Spectrum Analysis	Advanced Spectrum Analysis	Live RF	Live View	AP Test	Connection Troubleshooting	Proximity
AP 6511/6521[1]	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
AP 650/6532	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
AP 6522/6562	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
AP 7131/7161	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
AP 7532/7522/7562[3]	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
AP 8132/8122/8163	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
AP 8232/8222	No	No	No	No	No	No	No	No
AP 7502	No	No	No	No	No	No	No	No
AP 8533[2]	Yes	No	Yes	No	Yes	Yes	Yes	Yes
AP 8432[2]	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
AP 7602/7622	Yes	No	No	No	No	No	No	Yes

Notes:

[1] GUI is disabled and the number of SSH sessions is limited to 1

[2] Support is limited to the dedicated sensor (Radio 3) for AP 8533. Support is limited to the dedicated sensor (Radio 1) for AP 8432.

[3] AP 7522, AP 7532, AP 7562 radios are band-locked, entire AP needs to be dedicated as sensor

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

Network Assurance Toolset with Radio Share	WIPS	Spectrum Analysis[2]	Advanced Spectrum Analysis[3]	Live RF	Live View	AP Test	Connection Troubleshooting	Proximity
AP 6511/ 6521[1]	No	No	Yes	Yes	Yes	Yes	Yes	Zone only
AP 650/6532	No	No	No	Yes	Yes	Yes	Yes	Yes
AP 6522/6562	No	No	Yes	Yes	Yes	Yes	Yes	Yes
AP 7131/7161	No	No	No	Yes	Yes	Yes	Yes	Yes
AP 7532/7522/7562	Yes[4]	No	No	Yes	Yes	Yes	Yes	Yes
AP 8132/8122/8163	No	No	Yes	Yes	Yes	Yes	Yes	Yes
AP 8232/8222	No	No	No	No	No	No	No	No
AP 7502	No	No	No	No	No	No	No	No
AP 8533	No	No	No	No	No	No	No	Yes
AP 8432	No	No	No	No	No	No	No	Yes
AP 7602/7622	No	No	No	No	No	No	No	Yes

Notes:

[1] GUI is disabled when Radio Share is enabled.

[2] Spectrum Analysis is not supported with Radio share enabled.

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

[4] Does not work in WiNG 5.8.3.

[5] AP 622, 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

[6] AP 7522, AP 7532, AP 7562 radios are band-locked, both radios are required for sensing

[7] AP 6511 does NOT support OCS or over-the-air termination

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

© Extreme Networks. 2017. All rights reserved.