

AirDefense 10.6.1-07 Release Notes

AirDefense 10.6.1-07 Release Notes	2
1. New Features in AirDefense 10.6.1-07	2
Firmware Version Compatibility	2
Extreme Campus Controller Version Compatibility.....	4
Hardware Appliances.....	4
Virtual Platforms.....	4
Supported WiNG Wireless Access Points	4
Supported Extreme Wireless Access Points	4
Extreme CloudIQ Version Compatibility.....	4
Supported Extreme Wireless Access Points	4
Extreme Switch Compatibility	5
Supported Browsers	5
2. Installation	5
Appliance Installation	5
3. Important Notes	7
4. SPR/Issues Fixed	9
5. Vulnerabilities Fixed	9
6. Known Issues and Recommendations	9
Pre-requisites for multicore configuration	10
Issues specific to EW access points	10
Upgrade related.....	10
Platform	10
Network Assurance.....	12
Bluetooth Monitoring.....	13
HTML5 UI	14
WIPADMIN CLI	14
7. Feature Matrix Dedicated Sensing	15
8. Feature Matrix Radio-Share Sensing	17
9. AirDefense Extreme Wireless Feature Matrix	18

AirDefense 10.6.1-07 Release Notes

1. New Features in AirDefense 10.6.1-07

The AirDefense 10.6.1-07 release introduces the following key features and functionalities:

1. Support for sensing of 6 GHz devices limited to
 - 1.1 Listing of sensed 6 GHz BSS and displaying those BSS's information within the Network Devices page.
 - 1.2 Listing of sensed 6 GHz Client devices and displaying those Client's information within the Network Devices page.
 - 1.3 Detection of Rogue Access points
 - 1.4 Detection of Rogue Clients
2. Sensor manger page: Configuration of the 6 GHz Channels.
3. Angular UI framework upgraded to version 15.

Note: - 6 GHz scanning and listing of sensed devices in this release are only supported by sensors operating on APs managed by IQC.

Version Compatibility

The 10.6.1-07 release is a Service Module 2 (SM2) release. 10.6.0-04 SM1 installation is mandatory before upgrading to this release.

For existing customers who would like to upgrade to 10.6.1-07, AirDefense is an entitled Product and requires an active support contract.

Firmware Version Compatibility

AirDefense 10.6.1-07 ISO was tested for compatibility against

- WiNG 7.9.3.0
- XIQC 10.08.01

6 GHz validated Sensor Models and Interop Build version

Sensor Model	Campus/Identifi Interop build
AP 5010	10.8.1.0-022R
AP 3000	10.8.1.0-022R
AP 4000	10.8.1.0-022R

2.4 GHz/5 GHz Supported Sensor Model and Interop Build version validated

Sensor Model	WING Interop build
AP 5010, AP5010u	WING 7.9.3.0
AP 410C-1	WING 7.9.3.0
AP 302w	WING 7.9.3.0
AP 305C-1	WING 7.9.3.0
AP 505i	WING 7.9.3.0
AP 310i, AP410i, AP510i	WING 7.9.3.0

Sensor Model	Identifi Interop build
AP 5010, AP5010u	10.6.2.0
AP 410C-1	10.6.2.0
AP 302w	10.6.2.0
AP 305C-1	10.6.2.0
AP 505i	10.6.2.0
AP 460c	10.6.2.0
AP 310i, AP410i, AP510i	10.6.2.0
AP 5050D, AP5050U	10.6.2.0

Sensor Model	XIQ/HOS
AP410C, AP460C	10.6.5
AP4000	10.6.5
AP510CX	10.6.5
AP302w	10.6.5
AP305c-1	10.6.5
AP5010, AP5010U	10.6.5
AP3000, AP3000X	10.6.5
AP5050D, AP5050U	10.6.5

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 Campus Controller Version Compatibility

AirDefense 10.6.1-07 ISO was tested for compatibility against

- Extreme Campus Controller 10.08.01

Hardware Appliances

- Model NX-9500
- Model NX-9600

Virtual Platforms

- VMWare EXSi Hypervisor 5.5, 6.0, 6.5,7.0

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
- AP 505, AP 510, AP 560
- AP 410, AP 460
- AP 310, AP 360

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 CloudIQ Version Compatibility

AirDefense 10.6.1-07 ISO was tested for compatibility against

- XIQ (23R7)

Supported Extreme Wireless Access Points

- AP 410C/460C (10.6R1)

- AP305C/305CX
- AP302W
- AP4000
- AP5010/5010U
- AP5050D/5050U
- AP3000X/3000W
- AP510C

Extreme Switch Compatibility

- X440 (31.2.1.1 patch2-1)
- X590 (Firmware 30.5.1.15)

Supported Browsers

Browser	HTML5
Chrome	Version 119.0.6045.200 (Official Build) (64-bit)
Firefox	112.0.2 (64-bit)
IE Edge	Version 119.0.2151.44 (Official build) (64-bit)

Supported OS

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

2. Installation

Appliance Installation

Please follow the below steps to fresh install or upgrade an AirDefense system that is currently running a previous release of AirDefense firmware.

Note :- Installation of 10.6-0-04 is mandatory before installing 10.6.1-07.

Step 1: - Copy AD-service-SM2-10.6.1-07.tar to /usr/local/tmp folder.

Step 2: - Run WIPsadmin command & type servmod . Press ENTER.

```
*** ADSPadmin ***
(M) _Manage      (D) _Dbase      (S) _Software      (C) _Config
[0] to quit    -> servmod
```

Step 3: - Select appropriate tar file by entering its listed line number and Press ENTER

```
  _Enter fully-qualified directory name
  where service module bundle resides
  (<Enter> if in /usr/local/tmp)
  (<C> if on CD/DVD)
  (<F> if on USB flash drive)
  (<Q> to return to previous menu)
  ->
```

Service modules available in /usr/local/tmp:

```
(1)  AD-service-SM2-10.6.1-07.tar

  _Enter line number of service module to use
  (<Q> to return to previous menu)
  -> █
```

Step 4: - type "yes"

```
Service modules available in /usr/local/tmp:
(1)  AD-service-SM2-10.6.1-07.tar

  _Enter line number of service module to use
  (<Q> to return to previous menu)
  -> 1

Note that installing a service module on this system
will restart the services upon exit of ADSPadmin!!!

Continue installing service module /usr/local/tmp/AD-service-SM2-10.6.1-07.tar? (yes/no): yes█
```

3. 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 Installations – VM installs of AirDefense must be allocated with a minimum of 50GB of virtual disk.
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 displays current status of SSLv3 in the system. If it is currently disabled, this option allows the user to enable it.
 - Type [E] to enable/ [D] to disable.
 - Type [Q] to quit.
 - System now warns 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.

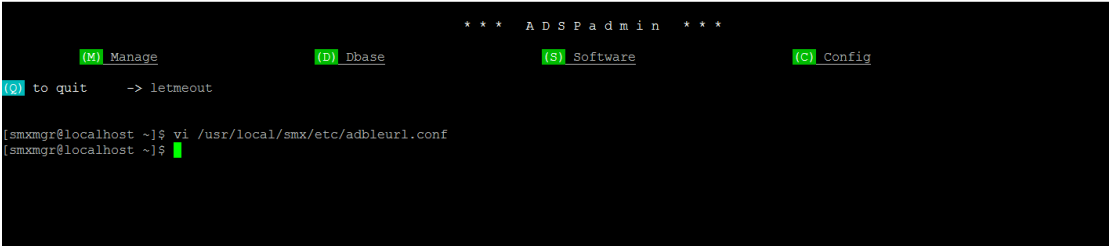
To switch back to 2048 bit certificates:

 - Login to AirDefense as *root* (contact support for assistance)
 - Delete the */usr/local/smx/.k/key1024* file
 - Restart AirDefense services.
7. Upgrade from AirDefense ver. 9.0.3 to ver. 9.1.0 (and higher) is not seamless. AirDefense architecture was significantly revised in ver. 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 ver. 9.0.3 be performed via ver. 9.2.0 release – which has enhancements to ease the upgrade.

8. When upgrading firmware to ver. 9.2.0 (from ver. 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 was 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 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 URLs are not allowed]

Instructions to configure the URLs in a file:

In AirDefense 10.0, this configuration is done via the CLI. Login to the AirDefense CLI using the *smxmgr* credentials



```
*** ADSPadmin ***
(M) Manage      (D) Dbase      (S) Software    (C) Config
(C) to quit    -> letmeout

[smxmgr@localhost ~]$ vi /usr/local/smx/etc/adbleurl.conf
[smxmgr@localhost ~]$
```

On the menu item, type *letmeout* and get the prompt **smxmgr#localhost ~**]

Edit the file using `vi /usr/local/smx/etc/adbleurl.conf`

#Enter allowed URLs (for all macs (or) for specific mac)

#URL=https://www.google.co.in

#Means URL is allowed for all macs and alarm is NOT triggered when this URL is used.

#URL=https://www.google.co.in, MAC=f8:d8:d1:39:63:ae

#Means URL is allowed only for specified mac

Users can add/edit the URL and MAC address as required.

Pre-requisites for multicore configuration

- When adding Areas (which are normally used to represent buildings) to the tree structure, all floors in that Area/building must be created under that same single Area/building.
- Do not create multiple copies of the same Area/building and then place some of the floors under one instance of the Area/building and other floors under a second instance of the Area/building.
 - o This is mandatory as not doing so will result in devices being seen multiple times and may result in undefined WIPS behavior.
- Better to have Auto-placement rules for network devices placement
 - o Messages from sensors in unplaced folder will not be processed.
 - o Polled devices in unplaced folder will not be considered for any WIPS processing.
 - o 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 (IQC)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.
 - o If upgrading from 9.0.3 – this conversion happens automatically when restoring the 9.0.3 config.
 - o If upgrading from 9.1.x - Any rules that were deliberately reversed by the administrator after upgrading from 9.0.3 to work around 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

- Rogue Locationing did not work consistently as devices sometimes placed in the corner of the floor.
- 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 - Honeygot, 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 all 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
 - ADIQ-745 APtest/WVA fails with 802.1x authentication
-
- 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 was 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.
- ADIQ-790: Scheduled AP test results are displayed with non-zero numbers when no tests are scheduled. Select specific device & option from right click to perform AP Test.
- AD-11418 "AirDefense 10.6 import failure of XIQ-C v10.05.02.0019" -- manually drawn floor plan images are not imported to AirDefense, and this is not supported.
- Stations not having associated BSS information in the XIQ, as part of XIQ import will not be listed(shown) in ADSP server.
- ADIQ-842 Rogue AP on Sensor Segment alarm is not generating for Aerohive APs
- ADIQ-832 Sensed Authentication and Encryption in the Properties page of 6G BSS is inaccurate
- ADIQ-833 Information of Non-transmitted SSID carried by mbssid 6E SSID is not displayed in the AirDefense server
- Non transmitted SSID are not listed in the AirDefense server.
- Live view, Wireless Vulnerability Assessment, AP Test & Termination functionalities are not supported for 6E devices.

Network Assurance

- AP Test and WVA fails on legacy platforms (AP650, AP8163, AP7532, AP8533 and AP8432). AP Test works, but WVA is failing on WiFi 6 platforms
- Radio share 310 sensor is keep disconnecting from ADSP server in idle state in distributed mode.

- Liveview with more than 4 sessions hanging the UI
- Liveview is not showing any 5Ghz channel frames if we enable Background SA Scan.
- Campus Mode - 5ghz scanning is not happening when we enable background scan
 - For both the above issues, background SA to be disabled in ADSP to scan 5GHz. This is Fixed in Wing 7.3.1.2.
- In AP505, liveview is not showing any data when it is enabled in radiosshare 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 – 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” – was fixed in WiNG 5.8.1 & higher releases.
- Multiple Vlan IDs cannot be removed – they can only be removed one at a time.
- Liveview: SSID and RSSI value do not appear in devices tab occasionally.
- Live RF with AP 75xx is only supported at 11n rates.

Bluetooth Monitoring

- BT/BLE devices are always placed on the sensor while locating on demand
- The actions are not carried out with filter as device client type for BLE devices
- 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

- Classification of BSS/Wireless Client to Sanctioned(Assign profiles) is not working properly from manual option in network page
- Override and Inherit options across new UI are inconsistent. It requires to save multiple times.
- 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 workflow, 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.
- In Multi-core acknowledge all alarms do not work at AirDefense level. But works in child level.
- All AP Test functionality don’t work in Tool Kit page.

WIPADMIN 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.

7. Feature Matrix Dedicated Sensing

ExtremeCloud IQ (XIQ) Managed								
AP Model Dedicated Sensor	Earliest Supported Firmware Version	WIPS and Advanced Forensics	Spectrum Analysis	Advanced Spectrum Analysis	Live View	AP Test	Wireless Vulnerability Assessment (WVA)	BT/BLE Security
AP410C ² /AP460C ²	10.6r4	✓	✗	✓	✓	✗	✗	✗
AP410C-1 ²	10.4r6	✓	✗	✗	✓	✗	✗	✗
AP4000 ⁵	10.4r1	✓	✗	✓	✓	✗	✗	✗
AP4000-1 ⁵	10.5r1	✓	✗	✓	✓	✗	✗	✗
AP5010 ⁶	10.5r1	✓	✗	✓	✓	✗	✗	✗
AP5050U ² /AP5050D ²	10.5r3	✓	✗	✓	✓	✗	✗	✗
ExtremeCloud IQ Controller v10.x (XIQC) Managed								
AP Model Dedicated Sensor	Earliest Supported Firmware Version	WIPS and Advanced Forensics	Spectrum Analysis	Advanced Spectrum Analysis	Live View	AP Test	Wireless Vulnerability Assessment (WVA)	BT/BLE Security
AP305C ¹ /CX ¹	10.0.0.0	✓	✗	✓	✓	✓	✓	✗
AP305C-1 ¹	10.1.0.0	✓	✗	✓	✓	✓	✓	✗
AP310ie ^{3,4} /360ie ^{3,4}	10.0.0.0	✓	✗	✓	✓	✓	✓	✓
AP410ie ² /460ie ²	10.0.0.0	✓	✗	✓	✓	✓	✓	✓
AP410C ² /AP460C(S) ²	10.0.0.0	✓	✗	✓	✓	✓	✓	✓
AP410C-1 ²	10.1.0.0	✓	✗	✓	✓	✓	✓	✗
AP505i ¹ /510ie ⁴ /560ih ⁴	10.0.0.0	✓	✗	✓	✓	✓	✓	✗
AP4000 ⁵	10.0.0.0	✓	✗	✓	✓	✗	✗	✗
AP4000-1 ⁵	10.1.0.0	✓	✗	✓	✓	✗	✗	✗
AP5010 ⁶ /AP5010U	10.03.01	✓	✗	✓	✓	✓	✓	✓
AP5050U ² /AP5050D ²	10.6.0	✓	✗	✓	✓	✗	✗	✗
AP3000 ¹ /AP3000X ¹	10.6.0	✓	✗	✓	✓	✗	✗	✗
Extreme Campus Controller v5.x (XCC) Managed								
AP Model Dedicated Sensor	Earliest Supported Firmware Version	WIPS and Advanced Forensics	Spectrum Analysis	Advanced Spectrum Analysis	Live View	AP Test	Wireless Vulnerability Assessment (WVA)	BT/BLE Security
AP305C/CX ¹	7.3.5.0	✓	✗	✓	✓	✓	✓	✗
AP310ie ⁴ /360ie ⁴	7.8.5.0	✓	✗	✓	✓	✓	✓	✗
AP310ie-1 ⁴	7.8.5.0	✓	✗	✗	✓	✓	✓	✗
AP410ie ² /460ie ²	7.8.5.0	✓	✗	✓	✓	✓	✓	✗
AP410ie-1 ²	7.8.5.0	✓	✗	✗	✓	✓	✓	✗
AP410C ² /AP460C ²	7.8.5.0	✓	✗	✓	✓	✓	✓	✓
AP505i ¹ /510ie ⁴ /560ih ⁴	7.8.5.0	✓	✗	✗	✓	✓	✓	✗
AP510ie-1 ⁴	7.8.5.0	✓	✗	✗	✓	✓	✓	✗
AP4000 ⁶	7.8.5.0	✓	✗	✗	✓	✓	✗	✓

ExtremeCloud Appliance v4.76.08 (XCA) Managed								
AP Model Dedicated Sensor	Earliest Supported Firmware Version	WIPS and Advanced Forensics	Spectrum Analysis	Advanced Spectrum Analysis	Live View	AP Test	Wireless Vulnerability Assessment (WVA)	BT/BLE Security
AP310ie ⁴ /360ie ⁴	WING 7.3.1.4	✓	✗	✓	✓	✓	✓	✗
AP410ie ² /460ie ²	WING 7.3.1.4	✓	✗	✓	✓	✓	✓	✗
AP505i ¹ /510ie ⁴ /560ih ⁴	WING 7.3.1.4	✓	✗	✗	✓	✓	✓	✗
AP7522 ¹ /7532 ¹ /7562 ¹	WING 7.3.1.4	✓	✗	✗	✓	✓	✓	✗
AP8432 ²	WING 7.3.1.4	✓	✗	✓	✓	✓	✓	✗
AP8533 ²	WING 7.3.1.4	✓	✗	✗	✓	✓	✓	✗

WiNG Controller Managed								
AP Model Dedicated Sensor	Earliest Supported Firmware Version	WIPS and Advanced Forensics	Spectrum Analysis	Advanced Spectrum Analysis	Live View	AP Test	Wireless Vulnerability Assessment (WVA)	BT/BLE Security
AP7532 ¹ /7522 ¹ /7562 ¹	WING 7.3.1.1	✓	✗	✓	✓	✓	✓	✗
AP8533 ²	WING 7.3.1.1	✓	✗	✓	✓	✓	✓	✓
AP8432 ²	WING 7.3.1.1	✓	✗	✓	✓	✓	✓	✓
AP310ie ⁴ /360ie ⁴	WING 7.4.1.2	✓	✗	✓	✓	✓	✓	✓
AP410ie ² /460ie ²	WING 7.4.1.2	✓	✗	✓	✓	✓	✓	✓
AP410C ² /AP460C ²	WiNG 7.6.4.0	✓	✗	✓	✓	✓	✓	✓
AP505i ¹ /510ie ⁴ /560 ⁴	WING 7.9.3	✓	✗	✓	✓	✓	✓	✓
AP310ie-1 ⁴	WING 7.9.3	✓	✗	✓	✓	✓	✓	✗
AP410C-1 ²	WING 7.9.3	✓	✗	✓	✓	✓	✓	✗
AP410i-1 ²	WING 7.9.3	✓	✗	✓	✓	✓	✓	✗
AP510i-1 ⁵	WING 7.9.3	✓	✗	✓	✓	✓	✓	✗
AP5010 ⁶ /AP5010U ⁶	WING 7.9.3	✓	✗	✓	✓	✗	✗	✗

Notes:

¹Both radios must be configured as a sensor. No client service possible when operating as a sensor

²Third radio capable of only 2.4/5GHz sensor functionality. For AP 8432 – First radio can be used either as a dedicated 2.4/5GHz sensor and second radio for data, or both radios can operate as sensors (No client service).

³First radio can operate as 2.4/5GHz sensor. With first radio operating as sensor, only 5GHz client service on second radio

⁴First radio 2.4/5GHz dedicated sensor capable. Second radio also able to operate as dedicated 5GHz single band sensor

⁵Third radio can operate as 2.4/5/6GHz sensor. When enabled, no client service on 6GHz possible

⁶First radio can operate as 2.4/5/6GHz sensor. When enabled, second and third radio provide 5/6GHz client service

8. Feature Matrix Radio-Share Sensing

ExtremeCloud IQ (XIQ) Managed							
AP Model Dedicated Sensor	Earliest Supported Firmware Version	WIPS and Advanced Forensics	Spectrum Analysis	Advanced Spectrum Analysis	Live View	AP Test	BT/BLE Security
AP302W	10.2r3	✓	✗	✗	✓	✗	✗
AP3000/AP3000X	10.6r1	✓	✗	✗	✓	✗	✗

ExtremeCloud IQ Controller v.10.x (XIQC) Managed							
AP Model Radio-Share Sensor	Earliest Supported Firmware Version	WIPS and Advanced Forensics	Spectrum Analysis	Advanced Spectrum Analysis	Live View	AP Test	BT/BLE Security
AP302w	10.0.0.0	✓	✗		✓	✗	
AP305C/CX ³	10.0.0.0	✓	✗	✗	✓	✗	✗
AP305C-1	10.1.0.0	✓	✗	✗	✓	✗	✗
AP310ie ³ /360ie ³	10.0.0.0	✓	✗	✗	✓	✓	✓
AP505i ³ /510ie ³ /560ih ³	10.0.0.0	✓	✗	✗	✓	✓	✗
AP400 ²	10.0.0.0	✓	✗	✓	✓	✗	✗
AP4000-1 ²	10.1.0.0	✓	✗	✓	✓	✗	✗
AP3000/AP3000X	10..06.01	✓	✗	✗	✓	✗	✗

Extreme Campus Controller v5.x (XCC) Managed							
AP Model Radio-Share Sensor	Earliest Supported Firmware Version	WIPS and Advanced Forensics	Spectrum Analysis	Advanced Spectrum Analysis	Live View	AP Test	BT/BLE Security
AP310ie ³ /360ie ³	7.8.5.0	✓	✗	✓	✓	✓	✗
AP310ie-1 ³	7.8.5.0	✓	✗	✗	✓	✓	✗
AP505i ³ /510ie ³ /560 ³	7.8.5.0	✓	✗	✗	✓	✓	✗
AP510ie-1 ³	7.8.5.0	✓	✗	✗	✓	✓	✗

WiNG Controller Managed							
AP Model Radio-Share Sensor	Earliest Supported Firmware Version	WIPS and Advanced Forensics	Spectrum Analysis	Advanced Spectrum Analysis	Live View	AP Test	BT/BLE Security
AP7532/7522/7562 ¹	WiNG 7.3.1.1	✓	✗	✗	✓	✓	✗
AP8432 ²	WiNG 7.3.1.1	✓	✗	✗	✓	✗	✓
AP310ie ³ /360ie ³	WiNG 7.6.1.0	✓	✗	✗	✓	✓	✓
AP505i ³ /510ie ³ /560 ³	WiNG 7.6.1.0	✓	✗	✗	✓	✓	✓
AP310ie-1	WiNG 7.7.1.0	✓	✗	✗	✓	✓	✗
AP510i-1	WiNG 7.7.1.0	✓	✗	✗	✓	✓	✗
AP3000/AP3000X	7.9.2	✓	✗	✗	✓	✗	✗

Notes:

¹Both the first and second radio can operate with radio-share sensing together or independently.

²Spectrum Analysis is not supported with radio-share mode enabled.

³AP 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
- Liveview

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries. All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see:
www.extremenetworks.com/company/legal/trademarks

© Extreme Networks. 2023. All rights reserved.