E Extreme®
networks

ADVANCE WITH US

AirDefense 10.6.0-04a8 Release Notes

AirDefense 10.6.0-04a8 Release Notes

This document is an addendum to the release notes for the main release 10.6.0-04

1. New Features in AirDefense 10.6.0-04a8

The AirDefense 10.6.0-04a8 (patch) release is a maintenance release fixing customer-found issues.

2. Version Compatibility

The 10.6.0-04a8 patch version is upgradable only from version 10.6.0-04.

For existing customers who would like to upgrade to 10.6.0-04a8, AirDefense is an entitled product and requires an active support contract.

Firmware Version Compatibility
AirDefense 10.6.0-04a8 was tested for compatibility with the following:
- WiNG 7.9.3.0
- XIQC 10.06.02

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.

Hardware Appliances
- Model NX-9500
- Model NX-9600

Virtual Platforms
- VMWare EXSi Hypervisor 6.0

3. Installation

Follow these steps to upgrade an AirDefense system that is currently running AirDefense 10.6.0-04 firmware.

Note: Direct upgrade from any other version is not supported.

1. Copy the file `AD-upgrade-10.6.0-04a8.tar` file to the `/usr/local/tmp` folder on the AirDefense server using the **smxmgr** account.
   You can use any tool such as **scp**, **ssh secure file transfer client**, **putty**, etc. to copy the file.

2. Login to AirDefense as **smxmgr**.

3. From the menu select **Software ➔ Servmod,** then accept the default location of the patch file: `/usr/local/tmp/`
   The menu shows available files.

4. Enter the number corresponding to `AD-upgrade-10.6.0-04a8.tar` and press **Enter**
   AirDefense installs the 10.6.0-04a8 patch.

For base system new installations of AirDefense, see the full instructions on how to upload the AirDefense image onto an NX and install it successfully in the *Extreme AirDefense Users Guide*.

4. Important Notes

Refer to the 10.6.0-04 release notes for more details.

5. SPR/Issues Fixed

Sl#	Defect#	Issue Description
1	AD-11412	ADSP | 'Enable Fast Termination' cannot unchecked in New UI
2	AD-11420	ADSP SNMP discovery failed because using deleted communication profile
3	AD-11392	Other Admin account login to ADSP cannot see Tree Structure under License
4	AD-11427	ADSP UI action control cannot see termination list more than 100 entry
5	AD-11428	ADSP Devices online and offline count not accurate
6	AD-11418	AirDefense 10.6 import failure of XIQC v10.05.02.0019
7	AD-11406	ADSP unable to apply more than 50 Security Profiles.
8	AD-11386	AP5010 model number is wrongly updated in the ADSP
9	CFD-6357	Device import from XIQ to AirDefense fails
10	CFD-8723	Device import from XIQ to AirDefense fails
11	CFD-8994	XIQ access points imported to ADSP only as sensors

6. Vulnerabilities Fixed

- None

7. Known Issues and Recommendations

General Note

- AD-11418 "AirDefense 10.6 import failure of XIQ-C v10.05.02.0019" -- manually drawn floor plan images are not imported to ADSP, and this is not supported.
- ADIQ-796

8. 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:
[1]Both radios must be configured as a sensor. No client service possible when operating as a sensor
[2]Third 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).
[3]First radio can operate as 2.4/5GHz sensor. With first radio operating as sensor, only 5GHz client service on second radio
[4]First radio 2.4/5GHz dedicated sensor capable. Second radio also able to operate as dedicated 5GHz single band sensor
[5]Third radio can operate as 2.4/5/6GHz sensor. When enabled, no client service on 6GHz possible
[6]First radio can operate as 2.4/5/6GHz sensor. When enabled, second and third radio provide 5/6GHz client service

9. 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	✓	✗	✗	✓	✓	✗
AP4000[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:
[1]Both the first and second radio can operate with radio-share sensing together or independently.
[2]Spectrum Analysis is not supported with radio-share mode enabled.
[3]AP Testing in radio-share mode - only single-cell/internal BSS AP testing is supported. AP Testing on remote BSS is not supported.

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