

Extreme AirDefense v10.6.2-05e4 Release Notes: New Features, Fixes, and Compatibility Details

Extreme AirDefense v10.6.2-05e4 Release Notes	2
Abstract	2
1. New Features in AirDefense 10.6.2-05e4	2
Firmware Version Compatibility	2
ExtremeCloud IQ Controller Version Compatibility	4
Hardware Appliances	4
Virtual Platforms	4
Supported WiNG Wireless Access Points	4
Supported Extreme Wireless Access Points	4
ExtremeCloud IQ Version Compatibility	5
Supported Extreme Wireless Access Points	5
Extreme Switch Compatibility	5
Supported Browsers	5
2. Installation	5
3. SPR/Issues Fixed	6
4. Vulnerabilities Fixed	6
5. Known Issues and Limitations	6
6. Feature Matrix Dedicated Sensing	6
7. Feature Matrix Radio-Share Sensing	9
8. AirDefense Extreme Wireless Feature Matrix	10

Extreme AirDefense v10.6.2-05e4 Release Notes

Note: This document is an addendum to the release notes for the main release 10.6.2-05.

Abstract

Extreme AirDefense v10.6.2-05e4 Release Notes: New Features, Fixes, and Compatibility Details

Extreme AirDefense v10.6.2-05e4, released in May 2026, is a maintenance patch addendum to the 10.6.2-05 base release, delivering targeted defect resolution without introducing new vulnerabilities or known issues. The patch addresses two customer-found defects—CFD-16789 (device sanctioning state corruption on name/description changes) and CFD-16269 (XSS/CSRF vulnerability in ADSP)—and adds support for AP5022, AP5022FX, AP5022S6D, AP5060U, and AP5060D access point models with PMF termination capability. Compatibility is validated against WiNG 7.9.7.0, ExtremeCloud IQ Controller 10.19.01, and ExtremeCloud IQ 25.10, with hardware support for NX-9500/NX-9600 appliances and VMware ESXi 5.5–7.0 virtual platforms. Upgrades are supported exclusively from versions 10.6.2-05 through 10.6.2-05d3. Comprehensive feature matrices detail WIPS, advanced forensics, spectrum analysis, live view, AP testing, and BLE security capabilities across dedicated and radio-share sensing modes for AP models managed via ExtremeCloud IQ, ExtremeCloud IQ Controller, Extreme Campus Controller, ExtremeCloud Appliance, and WiNG controllers.

1. New Features in AirDefense 10.6.2-05e4

The AirDefense 10.6.2-05e4 (patch) release is a maintenance release. This patch contains information on:

- PMF termination
- Fix for Customer Found Defects
 - CFD-16789
 - CFD-16269
- Support for the following AP models:
 - **AP5022, AP5022FX, AP5022S6D**
 - **AP5060U, AP5060D**

Version Compatibility

The 10.6.2-05e4 patch version is upgradable from:

- Version 10.6.2-05 (both ISO and SM)
- Version 10.6.2-05a2 patch
- Version 10.6.2-05b3 patch
- Version 10.6.2-05c3 patch
- Version 10.6.2-05d3 patch

For existing customers who want to upgrade to 10.6.2-05e4, AirDefense is an entitled product and requires an active support contract.

Firmware Version Compatibility

AirDefense 10.6.2-05e4 has been tested for compatibility against:

- WiNG 7.9.7.0

- ExtremeCloud IQ Controller 10.19.01
- ExtremeCloud IQ 25.10

6 GHz validated Sensor Models and Interop Build version

Sensor Model	ExtremeCloud IQ Controller Interop build
AP 5010	10.19.1.0
AP 3000	10.19.1.0
AP 4000	10.19.1.0
AP4020, AP4020X, AP4020FX	10.19.1.0
AP5020, AP5022, AP5022FX, AP5022S6D	10.19.1.0
AP4060, AP4060X	10.19.1.0

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

Sensor Model	WING Interop build
AP 5010, AP5010u	WING 7.9.7.0
AP 410C-1	WING 7.9.7.0
AP 302w	WING 7.9.7.0
AP 305C-1	WING 7.9.7.0
AP 505i	WING 7.9.7.0
AP 310i, AP410i, AP510i	WING 7.9.7.0

Sensor Model	ExtremeCloud IQ Controller Interop build
AP 5010, AP5010u	10.19.1.0
AP 410C-1	10.19.1.0
AP 302w	10.19.1.0
AP 305C-1	10.19.1.0
AP 505i	10.19.1.0
AP 460c	10.19.1.0
AP 310i, AP410i, AP510i	10.19.1.0
AP 5050D, AP5050U	10.19.1.0
AP4020, AP4020X, AP4020FX	10.19.1.0
AP5020, AP5022, AP5022FX, AP5022S6D	10.19.1.0
AP4060, AP4060X	10.19.1.0

Sensor Model	XIQ/HOS
AP410C, AP460C	10.8.7
AP4000	10.8.7

Sensor Model	XIQ/HOS
AP510CX	10.8.7
AP302w	10.8.7
AP305c-1	10.8.7
AP5010, AP5010U	10.8.7
AP3000, AP3000X	10.8.7
AP5050D, AP5050U	10.8.7
AP5020	10.8.7
AP4020, AP4020X, AP4020FX	10.8.7
AP4060, AP4060X	10.8.7

For WiNG feature support information around Dynamic Frequency Selection (DFS), sensor capabilities, and radio share functionality, please refer to the section titled “DFS Tables, Sensor and Radio Share” in the [WiNG release notes](#). For support information on sensor capabilities and radio-share capabilities, see the sections [Feature Matrix Dedicated Sensing](#) and [Feature Matrix Radio-Share Sensing](#) later in this set of AirDefense Release Notes.

ExtremeCloud IQ Controller Version Compatibility

AirDefense 10.6.2-05e4 has been tested for compatibility against:

- ExtremeCloud IQ Controller for version 10.19.01

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

Supported Extreme Wireless Access Points

- AP 3915
- AP 3916
- AP 3917
- AP 3912

- AP 3935
- AP 3965

ExtremeCloud IQ Version Compatibility

AirDefense 10.6.2-05e4 has been tested for compatibility against:

- ExtremeCloud IQ 25.10

Supported Extreme Wireless Access Points

- AP 410C/460C (10.6.1)
- AP305C/305CX
- AP302W
- AP4000
- AP5010/5010U
- AP5050D/5050U
- AP3000X/3000W
- AP510C
- AP4020/X/FX
- AP4060/X
- AP5020

Extreme Switch Compatibility

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

Supported Browsers

Browser	HTML5
Chrome	Version 147.0.7727.138 (Official Build) (64-bit)
Firefox	Version 150.0 (64-bit)
IE Edge	Version 146.0.3856.109 (Official build) (64-bit)

Supported OS

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

2. Installation

Follow these steps to upgrade an AirDefense system that is currently running AirDefense 10.6.2-05 or 10.6.2-05d3 firmware.

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

1. Copy the file AD-upgrade-10.6.2-05e4.tar file to the /usr/local/tmp folder on the AirDefense server using the smxmgr account. You can use tools such as scp, ssh secure file transfer client, or putty 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-10.6.2-05e4.tar* and press <Enter>.

AirDefense installs the 10.6.2-05e4 patch.

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

3. SPR/Issues Fixed

CFD # Fixed	Summary
CFD-16789	Changing Name/Description change Sanctioned devices to Unsanctioned
CFD-16269	ADSP XSS/CSRF vulnerability

4. Vulnerabilities Fixed

- None

5. Known Issues and Limitations

- None

6. 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 /AP460Cyou 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	✓	✗	✓	✓	✗	✗	✗
AP5020 ⁹	10.8r7	✓	✗	✓	✓	✗	✗	✗
AP4020/X/FX ⁷ (4 th radio), / AP4060/ X ⁷ (4 th radio)	10.8r7	✓	✗	✓	✓	✗	✗	✗

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	✓	✗	✓	✓	✓	✓	✗
AP4020/X/FX ⁷ (4 th radio), / AP4060/ X ⁷ (4 th radio)	10.18.01	✓	✗	✓	✓	✗	✗	✗
AP5020 ⁹	10.17.01	✓	✗	✓	✓	✗	✗	✗
AP5022/FX/S6D	10.19.01 ¹⁰	✓	✗	✓	✓	✗	✗	✗

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.

⁷ AP4020/4060 Series—The dedicated fourth sensor radio will provide basic WIPs (Rogue AP detection and PCI/HIPPA reporting). As of XIQ-C release 10.18.01, XIQ release 25.10 AP4020 family and AP4060 now also supports radio share mode on the three client serving radios.

⁹ AP5020—Will use one of the SDR modes (mode 2 and mode 4) where one of the client-serving radio will be converted into a dedicated sensor. The dedicated sensor radio will not serve clients.

¹⁰ PMF Termination—ExtremeCloud IQ Controller v10.19.01 supports PMF termination for the following AP models: AP3000, AP3000X, AP4000, AP4020, 4020X, 4020FX, AP4060, AP5010, AP5020, AP5022FX, AP5022S6D, AP5060D, AP5060U.

7. 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	✓	✗	✗	✓	✗	✗
AO650/510C	10.2r3	✓	✗	✗	✓	✗	✗

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:

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.

8. 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. 2026. All rights reserved.