

700-00016-000
CabinAXe™
User's Manual



(IMAGE FOR REFERENCE ONLY)

PRELIMINARY

Astronics CSC
Inflight Entertainment and Connectivity Systems

THIS DOCUMENT IS
THE SOLE PROPERTY OF ASTRONICS CONNECTIVITY SYSTEMS & CERTIFICATION ("ASTRONICS CSC") AND SHALL NOT BE
REPRODUCED, COPIED OR ISSUED AS THE BASIS OF MAINTENANCE OR SALE OF APPARATUS WIHTOUT PERMISSION OF ASTRONICS
CSC.

Copyright

© Copyright 2022 Astronics CSC. Astronics CSC trademarks include , Cabin Ace-2™, Cabin Ace™, Cabin Pinnacle™, Cabin Vista™, Edge™, CabinAXe™, All rights reserved. All other trademarks are the property of their respective owners.

Open Source Code

This product includes code licensed under GNU General Public License, and/or certain other open source licenses.

FCC COMPLIANCE STATEMENT

CAUTION: Changes or modifications not expressly approved could void your authority to use this equipment.

This device complies with Part 15 of the FCC Rules. Operation to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet.

Operation in the 5.9725-7.125GHz band is prohibited for control of or communication with unmanned aircraft systems.

INDUSTRY CANADA COMPLIANCE STATEMENT

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

EUROPEAN UNION COMPLIANCE STATEMENT

Hereby, Astronics CSC, declares that this Cabin Wireless Access Point is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU. The full text of the EU Declaration of Conformity (DoC) is available at the following internet address: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0053&from=EN>.

1 TABLE OF CONTENTS

1	User Information.....	5
1.1	Support Documentation	5
1.2	Industry Standards	6
1.3	Warranty.....	6
1.4	Exclusion of Liability Notice.....	6
2	Important Safety Instructions	7
2.1	Safety and Precautions	7
2.2	Regulatory	8
3	Introduction.....	10
3.1	Product Description	10
3.2	Hardware Architecture	10
3.3	Key Hardware Components	11
3.4	Orderable Part Numbers	13
4	Starting Up	14
4.1	Power Up.....	14
4.2	Startup process	14
4.3	IP Strapping Table	19
4.4	Connecting using the Console Port	20
4.5	Connecting using Web-based GUI	21
4.6	Virtual Controller Architecture	24
4.7	WLAN Setup.....	26
5	Physical I/O	34
5.1	Connections and Cabling	34
5.2	Maintenance Connectors	37
5.3	Status Indicators	37
6	Performance Data	38
6.1	Radio Characteristics	38
6.2	RF Performance Table.....	39
7	Technical Data	41
7.1	Electrical and Environmental Specifications	41
7.2	Mechanical Design and Dimensions	44
7.3	Grounding and Bonding	48
7.4	Workmanship	48
7.5	Safety	48
7.6	Protective Devices	48
8	Reliability and Maintainability	49
8.1	Reliability.....	49
8.2	Maintainability.....	49
8.3	Mean Time to Repair (MTTR)	49
8.4	Failure Detection and Fault Isolation	49
8.5	Production Testing	49
9	Support and Service.....	50

9.1	Technical Support	50
9.2	Returning Defective Equipment	50

Table of Tables

Table 1: Astronics CSC Support Documentation	5
Table 2: Aruba Support Documentation	5
Table 3: Industry Standards	6
Table 4: Wi-Fi 6E CWAP (GbE) Orderable Part Numbers	13
Table 5: IP Strapping Table	19
Table 6: CWAP External Connector Interfaces	34
Table 7: AP LED Operation	37
Table 8: Radio Characteristics	38
Table 9: 2.4GHz Maximum Radiated Output Power	39
Table 10: 5GHz Maximum Radiated Output Power	39
Table 11: 6GHz Maximum Radiated Output Power	39
Table 12: Qualification Test Matrix - Environment	41
Table 13: Qualification Test Matrix - EMI	41

Table of Figures

Figure 1: Wi-Fi 6E CWAP (GbE) System Block Diagram	12
Figure 2: CabinAXe™ Equipment	13
Figure 3: Aruba Communications Message	15
Figure 4: SIB Boot Complete	16
Figure 5: Example Console Output of the AP Boot Process	17
Figure 6: Aruba Instant GUI Login Prompt	21
Figure 7: The Sections of the Aruba Instant Main GUI Page	22
Figure 8: System Username and Password Dialog Box	23
Figure 9: The Virtual Controller General Setup screen	24
Figure 10: Select / Edit the Access Point screen	25
Figure 11: The Edit Access Point screen	25
Figure 12: Creating an SSID	26
Figure 13: The Basic Tab of the New Network configuration GUI	27
Figure 14: The VLAN Tab of the New Network GUI screen	28
Figure 15: Open Security level options	29
Figure 16: Personal Security level options	30
Figure 17: Enterprise Security level options	31
Figure 18: Access Rules options	32
Figure 19: Configuring Firewall Rules	32
Figure 20: J1 (Pins) Connector Layout and Pin Definitions	34
Figure 21: J2 (Socket) Connector Layout and Pin Definitions	35
Figure 22: J3 (Socket) Connector Layout and Pin Definitions	36
Figure 26: CWAP Top View	44
Figure 27: CWAP I/O Front View	45
Figure 28: CWAP Side View - Right	45
Figure 29: CWAP Side View – Left	45
Figure 30: CWAP Rear View	46
Figure 31: CWAP Bottom View	46

1 User Information

This User's Manual describes the features supported by Astronics CSC Wi-Fi 6E Cabin Wireless Access Point (CWAP), branded as *CabinAXe™* and provides detailed instructions for setting up and configuring the *CabinAXe™* wireless access point.

This guide is intended for administrators who configure and use CabinAXe™.

1.1 Support Documentation

In addition to this document, the following table describes Astronics CSC support documentation:

Table 1: Astronics CSC Support Documentation

Document Number	Description
700-00016-000-OL	Outline Drawing, Wi-Fi 6E CWAP (GbE)
PS-700-00016-000	Product Specification, Wi-Fi 6E CWAP (GbE)
CMM-44-20-53	Component Maintenance Manual (CMM), Wi-Fi 6E CWAP (GbE)
SRD-700-00016	Software Requirements Document for Wi-Fi 6E CWAP (GbE)
ATP-700-00016-000	Acceptance Test Procedure (ATP), Wi-Fi 6E CWAP (GbE)
FMEA-700-00016-000	Failure Modes and Effects Analysis (FMEA), CWAP, CabinAXe
QTR-700-00016-000ENV	Environmental (ENV) Qualification Test Report
QTR-700-00016-000EMC	Qualification Test Report, Electromagnetic Compatibility (EMC)

CabinAXe™ ships with Aruba Instant firmware. The following table describes the applicable Aruba support documentation for this firmware version. Aruba Instant 8.10 is the minimum version supported.

Table 2: Aruba Support Documentation

Document Name	Description
Aruba Instant User Guide	This User Guide describes the features supported by Aruba Instant and provides detailed instructions for setting up and configuring the Instant network.
Aruba Instant CLI Reference Guide	This document describes the Aruba Instant command syntax and provides information for each Command.
Aruba Instant Rest API Guide	This document describes the configuration procedures and monitoring functions that can be performed using REST APIs
Aruba IoT Websocket Interface Guide	This document describes the Telemetry WebSocket server interface for transporting IoT data.

1.2 Industry Standards

Table 3: Industry Standards

Industry Standard	Description
ARINC 628	Cabin Equipment Interfaces, Part 1, Interfaces, Cabin Management and Entertainment Systems - Peripherals
IEE 802.11	A set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 900 MHz and 2.4, 3.6, 5.6, and 60 GHz frequency bands.
IEE 802.3	A set of media access control (MAC) and physical layer (PHY) specifications for implementing wired local area network (LAN) computer communication.
RTCA/DO-160G	Environmental Conditions and Test Procedures for Airborne Equipment RTCA/DO-178B Software Considerations in Airborne Systems and Equipment
802.11h	Spectrum and Transmit Power Management Extensions (TPC) is supported to ensure that the average power is less than the regulatory maximum to reduce interference to satellites.

1.3 Warranty

The CabinAXe™ is warranted against defects in materials and workmanship for the warranty period from the date of shipment. The warranty does not apply to defects resulting from improper or inadequate maintenance of handling by the buyer, unauthorized modification or misuse, operation outside of the product's environmental specification of improper installation or maintenance. Astronics CSC will not be responsible for any defects or damages to other products not supplied by Astronics CSC that are caused by a faulty Astronics CSC product.

1.4 Exclusion of Liability Notice

Should the user disregard the instructions (specifically the safety instructions) in this manual and possibly on the device, Astronics CSC shall be exempt from legal liability for accidents.

In the event of damage to the device, which is caused by a failure to observe the instructions (specifically the safety instructions) in this manual and possibly on the device, Astronics CSC shall not be required to honor the warranty, including during the warranty period, and shall be exempt from legal liability of accidents.

2 Important Safety Instructions

2.1 Safety and Precautions

The following general instructions should always be followed in order to assure the proper operation of CabinAXe™, the safety of operators and the preservation of warranty coverage.



Warning!

All precautions, procedures, and safeguards to prevent damage due to ESD, and promote the safe handling of electrical components must be followed

1. Avoid removing any identification plates, serial numbers or warning labels unless specifically authorized by the manufacturer.
2. Please observe all specified dimensions required for mounting included in the Outline Drawing, Document 700-00016-000-OL.
3. When installing the CabinAXe™, there must be at least 1.00" free space to the left, right, top and rear of the unit to prevent the system overheating.
4. Leave at least 3.00" of free space to the front of the unit in order to have access to the connector interfaces to properly connect the peripherals.
5. Attach the CabinAXe™ firmly to a clean flat and solid mounting surface. Use proper fastening materials suitable for the mounting surface. Ensure that the mounting surface type and the mounting solution safely support the load of the CabinAXe™ and the attached components.
6. Follow the local/national regulations for grounding. A ground bonding measurement between the CabinAXe™ and the mounting surface should be conducted to ensure proper safety and EMI characteristics are maintained.
7. The voltage feeds must not be overloaded. Adjust the cabling and external overcharge protection to correspond with the electrical data indicated on the type label. For detailed interconnection of power and signal wiring, refer to the Section 4 and Section 5.
8. Electrostatic Discharge (ESD)



Electrostatic boards and their components are sensitive to static electricity. Therefore, care must be taken during all handling operations and inspection of this product, in order to ensure product integrity at all times. Do not handle this product out of its protective enclosure while it is not used for operational purposes unless it is otherwise protected.

A sudden electrostatic discharge can destroy sensitive components. Proper packaging and grounding rules must be observed. Always take the following precautions.

- Keep electrostatically sensitive components in their containers, until they arrive at an electrostatically protected workplace.
- Only touch electrostatically sensitive components when you are properly earthed.



- Store electrostatically sensitive components in protective packaging or on anti-static mats.

2.2 Regulatory

2.2.1. RF Exposure Statement

This equipment complies with RF radiation exposure limits. This equipment should be installed and operated with a minimum distance of 13.78 inches (35cm) between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Déclaration de la concernant l'exposition aux rayonnements à fréquence radioélectrique (FR)

Cet appareil est conforme aux limites d'exposition aux rayonnements FR établies. Il doit être installé et utilisé à une distance minimale de 35 cm (13,78 pouces) entre le radiateur et votre corps. Cet émetteur ne doit pas être installé ou utilisé à proximité immédiate d'une autre antenne ni d'un autre transmetteur.

2.2.2. Canada – ISED Compliance Information

This Class B digital apparatus meets all of the requirements of the Canadian Interference-Causing Equipment Regulations. In accordance with Industry Canada regulations, this radio transmitter and receiver may only be used with an antenna, the maximum type and gain of which must be approved by Industry Canada. To reduce potential radio interference, the type of antenna and its gain shall be chosen so that the equivalent isotropic radiated power (EIRP) does not exceed the values necessary for effective communication.

This device complies with Industry Canada's license-exempt RSS regulations. Operation of this device is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation.

When operated in the 5.15 to 5.25 GHz frequency range, this device is restricted to indoor use to reduce the potential for harmful interference with co-channel Mobile Satellite Systems.

Déclaration d'Industrie Canada

Conformément aux réglementations d'Industrie Canada, cet émetteur-récepteur radio doit être utilisé uniquement avec une antenne dont le type et le gain maximal doivent être approuvés par Industrie Canada. Pour réduire les interférences radio potentielles, le type d'antenne et son gain doivent être choisis de façon à ce que la puissance isotrope rayonnée équivalente (PIRE) ne dépasse pas les valeurs nécessaires à une communication efficace.

Ce périphérique est conforme aux règlements RSS exempts de licence d'Industrie Canada. L'utilisation de ce périphérique est soumise aux deux conditions suivantes : (1) ce périphérique ne doit pas provoquer d'interférences, et (2) ce périphérique doit accepter toute interférence, y compris les interférences susceptibles de provoquer un dysfonctionnement.

En cas d'utilisation dans la plage de fréquences de 5,15 à 5,25 GHz, cet appareil doit uniquement être utilisé en intérieur afin de réduire les risques d'interférence avec les systèmes satellites mobiles partageant le même canal.

2.2.3. European Union

Wireless Channel Restrictions:

The CabinAXe™ operates in the 5150-5350MHz band and is designed for indoor use only in the countries; Austria (AT), Belgium (BE), Bulgaria (BG), Croatia (HR), Cyprus (CY), Czech Republic (CZ), Denmark (DK), Estonia (EE), Finland (FI), France (FR), Germany (DE), Greece (GR), Hungary (HU), Iceland (IS), Ireland (IE), Italy (IT), Latvia (LV), Liechtenstein (LI), Lithuania (LT), Luxembourg (LU), Malta (MT), Netherlands (NL), Norway (NO), Poland (PL), Portugal (PT), Romania (RO), Slovakia (SK), Slovenia (SL), Spain (ES), Sweden (SE), Switzerland (CH), Turkey (TR).

Radio	Frequency Range (MHz)	Max EIRP (dBm)
BLE/Zigbee	2402-2480	10
Wi-Fi	2412-2472	20
	5150-5250	20
	5250-5350	20
	5470-5725	20
	5725-5850	14
	5945-6425	20

Operations in the 6GHz band are blocked by firmware for some countries depending on the adoption of the spectrum. Refer to Aruba DRT release notes for details.

For EU Compliance, the following label is applied to the Cabin AXe™ shipping container:

							
AT	BE	BG	CZ	DK	EE	FR	DE
IS	IE	IT	EL	ES	CY	LV	LI
LT	LU	HU	MT	NL	NO	PL	PT
RO	SI	SK	TR	FI	SE	CH	HR
UK(NI)							

3 Introduction

3.1 Product Description

The Cabin Wireless Access Point (CWAP) is a network distribution system specifically designed for commercial aircraft applications. The CWAP supports Wi-Fi 6E functionality and is backwards compatible with 802.11ac/a/b/g/n. The CWAP leverages the use of a COTS wireless access point to facilitate wireless communications to wireless client radios in the aircraft cabin, as well as other devices on the network. The CWAP provides a bridge between IEEE 802.3 wired Ethernet LANs and IEEE 802.11 compliant wireless networks.

The unit is provided with aircraft level discrete inputs and outputs to facilitate event notification to and from other aircraft systems, including remote management of the ON/OFF function. The unit is equipped with an airborne-type AC power supply capable of operating from 115VAC, 360 Hz – 800 Hz power, with a 200 msec hold-up capability for power interruptions. The CWAP does not require an active cooling system. The unit communicates to a host server by physical connection over a Gigabit Ethernet wired interface either in a “Daisy chain” or “Star” network topology environment.

The CWAP has integrated antennas supporting 2.4GHz, 5GHz, and 6GHz bands. Additionally, the CWAP includes a Bluetooth Low Energy (BLE 5.0) and 802.15.4 (Zigbee) radio for low-power connected devices, and onboard sensors and beacons.

This User Manual pertains to a CWAP with integrated antennas supporting 2.4GHz, 5GHz, and 6GHz bands.

This unit is identified as Astronics CSC part number 700-00016-000 and is branded as *CabinAXe™*.

3.2 Hardware Architecture

The CWAP leverages a state-of-the-art, commercial enterprise-class Wireless Access Point (AP). The AP selected for this application is manufactured by Aruba Networks, a Hewlett Packard Enterprise company. The Aruba model AP-635 has been ruggedized and repackaged to meet the operational requirements of commercial aircraft environment. The CWAP meets the electrical and mechanical requirements of ARINC 628.

The CabinAXe™ feature set includes:

- Architecture based on Wi-Fi 6E wireless standards (includes 1GHz of spectrum at 6GHz).
- Tri-band coverage across 2.4GHz, 5GHz, and 6GHz using three dedicated radios.
- IEEE 802.11ax, 2 x 2 MIMO, 2SS operation up to seven 160MHz channels.
- Peak data rates: 2.4Gbps (6GHz, HE160/2SS) + 1.2Gbps (5GHz, HE80/2SS) + 574Mbps (2.4GHz, HE40/2SS).
- 2x Integrated antennas omni-directional antennas with adaptive beam forming for enhanced throughput capabilities.
- OFDMA and Bi-Directional MU-MIMO for more active concurrent users.
- WPA-3 and Enhanced Open Security. WPA2-MPSK
- TPM 2.0 for secure key storage and credentials.
- Improved Client Roaming to optimize AP utilization.
- Hotspot 2.0.
- Dynamic Frequency Selection.
- Support for up to 512 associated client devices per radio.
- Fully Autonomous without Requiring a Separate Wireless Controller.

- Support for Worldwide (-WW) operation via the CLI which can automatically configure the CWAP in accordance with location information (provided by the aircraft) to pre-set regulatory domains (country codes) stored within the CWAP.
- Bluetooth Low Energy (BLE 5.0) and 802.15.4 (Zigbee) radio for low-power connected devices, and onboard sensors and beacons.
- Dual Gigabit Ethernet interfaces.
- Discrete inputs to control Remote ON/OFF and RF Enable.
 - The RF Enable/Disable discrete input state is read by the SIB and can be queried via the Manufacturing Data Server. The SIB firmware does not take any direct action when a state change is detected.
- Discrete output for PSU and AP status.
- IP address strapping bits.
- Support for input power pass thru to downstream CWAPs.
- Aircraft-grade AC power supply unit with 200 msec of hold-up capacity.
- Support for pass-thru Ethernet to downstream CWAPs (per ARINC 763).
- Redundant power supply to support Ethernet bypass in the event of a CWAP primary power supply failure.
- Connectors:
 - EN4165 style connectors for all I/O (per ARINC 628).
 - Micro USB for serial console connection.

3.3 Key Hardware Components

The CWAP key hardware components include:

- Commercial AP with integrated antennas for Wi-Fi, BLE, and Zigbee radios.
- PSU: Includes primary AC/DC, and secondary AC/DC power supplies.
- Signal Interface Board (SIB).
- External connectors Interface for Power, Ethernet, Discrete I/O (per ARINC 628).
- Mechanical housing; meets mounting requirements of ARINC 628.

Figure 1 shows the CWAP System Block Diagram.

(Intentionally Left Blank)

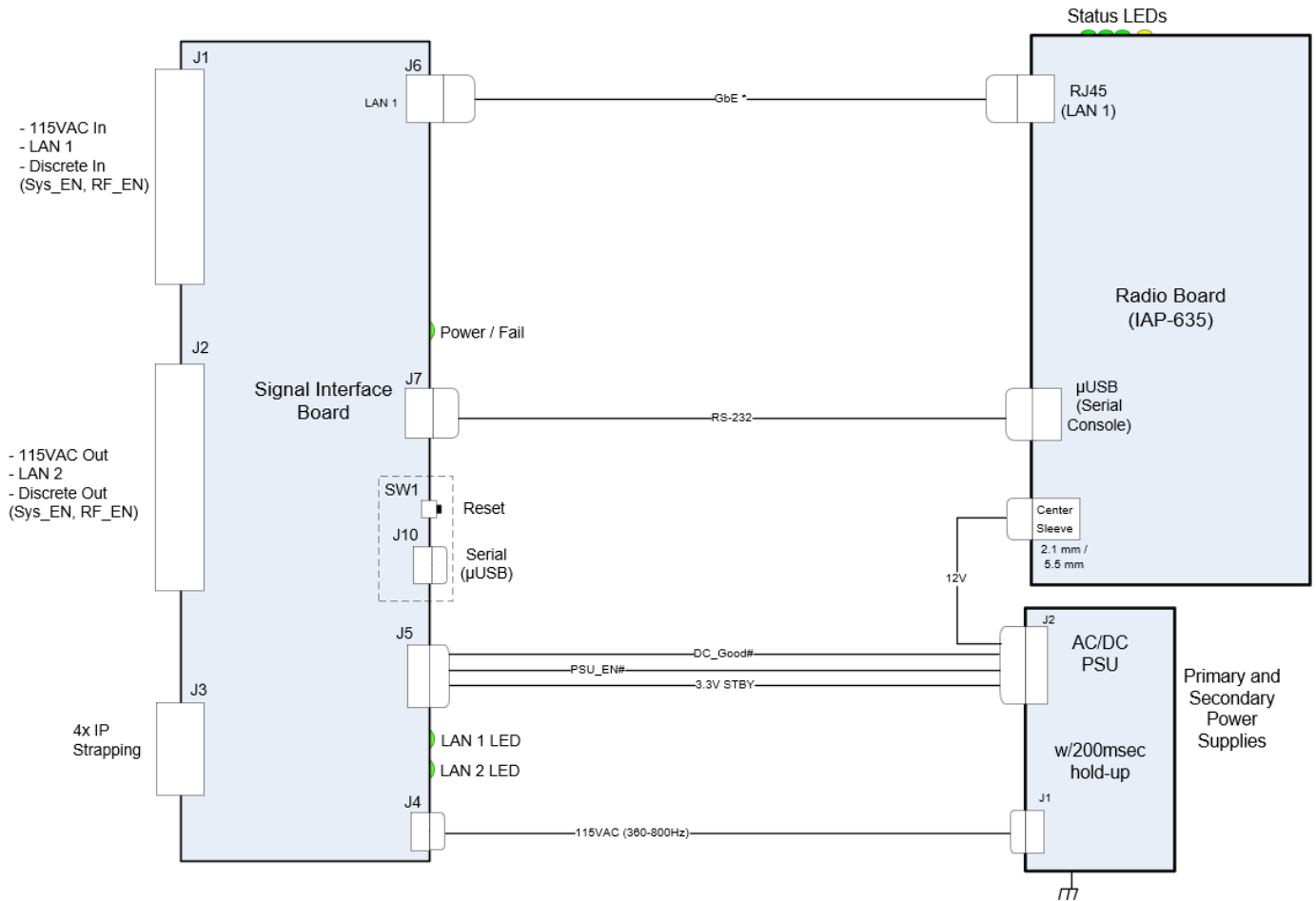


Figure 1: Wi-Fi 6E CWAP (GbE) System Block Diagram

3.4 Orderable Part Numbers

Table 4: Wi-Fi 6E CWAP (GbE) Orderable Part Numbers

ID	Astronics CSC P/N	Description
1	700-00016-000	LRU, Wi-Fi 6E CWAP (GbE)
2	E54-331	Cable Assy, Power/Signal/GbE, CWAP (J1)
3	E54-332	Cable Assy, Power/Signal/GbE, CWAP (J2)
4	E54-333	Cable Assy, Discretes, CWAP (J3)
5	E54-319-03	Cable Assy, AC Power Disconnect
6	E54-345	DB-9 Loop-back Test Connector (J1)
7	COTS part	USB Type A Male to Micro-USB Type B Male Cable
8	E54-352	Cable Assy, Daisy chain



Note: Items 2 – 8 are available for test purposes and are not intended to be used in flight.

Figure 2: CabinAXe™ Equipment

4 Starting Up

4.1 Power Up

The J1 power cable assembly, Astronics CSC P/N E54-331, and DB-9 loop-back connector, Astronics CSC P/N E54-345, are required to be connected to the CabinAXe™ to activate the unit when power is applied.

	WARNING! The specified voltage input range is 97 to 134 VAC, 60 – 800 Hz, single-phase power. DO NOT connect to 220 VAC. The power source must supply a minimum of 20W. The power source must be switched off via AC power disconnect, P/N E54-319, and must be easily accessible. Ambient temperature must be above -20 °C for the CWAP to turn on. Power is not switched internally and the unit will boot up as soon as power is applied.
---	--

Properly connect Astronics CSC P/N E54-331 to the CWAP J1 connector. The power source must be switched off via AC Power disconnect, Astronics CSC P/N E54-319, to make sure that no voltage is present at the terminal during the connecting procedure. Plug the DB-9 loopback connector, Astronics CSC P/N E54-345, to the mating connector of J1, E54-331 cable assembly.

Connect the other end of the power cord to the power source (not provided). Switch on the power source via the AC power disconnect.

4.2 Startup process

The CWAP needs two IP addresses for network connectivity, one for the access point and one for the Signal Interface Board (SIB). The four discrete IP strapping pins in the J3 connector are set to HIGH (+5v DC) by pull up resistors, and can be grounded to set static IP addresses. By default the CWAP is configured as a DHCP client, and will request two IP addresses from the network DHCP server. If no DHCP server responds to the request then auto configuration will assign an address to the AP on the 169.254.0.0 255.255.0.0 network (the SIB will continue to send DHCP requests).

Note: The IP strapping bits are read by the CWAP at power up and will over-write any static IP assignment made in the Aruba GUI. This behavior persists even when interface J3 is not connected.

4.2.1 Boot Up

4.2.2 SIB Boot Up

The SIB runs the bootloader application which provides the functionality to perform firmware updates on power up. The bootloader waits for up to two (2) seconds for a firmware update to start over the console port. If no firmware update occurs, then after that two second delay the application firmware is loaded, and begins execution.

Upon starting the application firmware, a Power on Self-Test (POST) is performed. The power on self test reads SIB configuration and manufacturing data from EEPROM and confirms the EEPROM integrity by checking the stored CRC. It also queries the discrete pins, verifies the Ethernet Switch, Temperature Sensor, Wiznet interface and the Aruba console to SIB communication path. If POST completes successfully the configuration of the Aruba is verified. At this point the console communication with the Aruba is password protected. To access the console you must enter the default password of #0211 followed by a return key, after you see the Aruba Communications message that is shown at the bottom of Figure 3. Additional information on SIB firmware features can be found in the Software Requirements Document SRD-700-00016.

```
SIB: Booting firmware [part number]: 900-00071-001 [version]: 1.0.0BL1

SIB: SW Build date: May 18 2022 11:43:00

SIB: EEPROM Version: 1
SIB: Initializing EEPROM Cache
SIB: EEPROM Manufacturing Data: VALID
SIB: SIB Serial Number    DEF_SIB_SN
SIB: MFG Date             05/2022
SIB: CWAP Serial Number   000002
SIB: CWAP Part Number     700-00016-000
SIB: FW Part num          900-00071-001
SIB: FW Revision          1.0.0BL1
SIB: Cust Part Number     N/A
SIB: HW Rev               2
SIB: CWAP Rev             A
SIB: CWAP Mod             0
SIB: ATP Test Pattern     csc
SIB: Aruba Serial Number  PHMBKYJ04V
SIB: Last ATP Date        2022-06-29

SIB: Aruba communications are secured. Please enter password to unlock communication to the Aruba
```

Figure 3: Aruba Communications Message

After the boot process completes there is a five (5) second window in which you may be asked to enter SIB command mode by your technical service representative. The console output of the SIB boot process is shown in Figure 4, the **[Boot Complete]** prompt indicates the beginning of the five (5) second delay. (Note if the operator unlocks the console communications and send a 'return' to the Aruba the boot delay counter is extended to 60 seconds. This delay will be reset for each new character sent, so the 60 seconds is from the last character received.)

```
SIB: PSU_EN#           : 0
SIB: RF_EN#            : 0
SIB: RESET#            : 1
SIB: TEMP_GOOD#        : 0
SIB: DC_GOOD#          : 0
SIB: ARUBA_POWER_EN#   : 0
SIB: ADDR_0            : 1
SIB: ADDR_1            : 1
SIB: ADDR_2            : 1
SIB: ADDR_3            : 1
SIB: BOARDREV_0        : 0
SIB: BOARDREV_1        : 1
SIB: BOARDREV_2        : 0

SIB: [Boot Complete]
```

Figure 4: SIB Boot Complete

4.2.3 Access Point (AP) Boot

Following SIB boot, the firmware boots the Aruba AP. During startup, the AP provides an auto-boot countdown prompt that allows you to interrupt the normal startup process and access **apboot** mode. The SIB firmware uses this mode to set the IP address configuration as defined by the IP strapping pins, then starts a ten (10) second inactivity counter to allow user access to apboot. If the user has 'unlocked' communications with the Aruba console as detailed above and the operator sends a 'return' to the console the ten second initial delay before fully booting is extended to sixty (60) seconds to permit the operator to enter commands in the Aruba apboot utility without needing to rush. If no characters are received within those 60 seconds, the AP will automatically boot.

The console output of the AP boot process is shown in Figure 5; the **apboot>** prompt indicates the beginning of the ten (10) second counter (Note if the operator unlocks the console communications and send a 'return' to the Aruba the boot delay counter is extended to 60 seconds).

```
SIB: [Boot Complete]
SIB: Aruba communications enabled
SIB: PSU EN# - Power ON
SIB: Aruba monitor initialized
SIB: IP Config Mode is: [Set Addr mode - Reverse Pin Map]
SIB: Address pins: 0xf offset: 0xf
SIB: Using DHCP for IP port configuration
SIB: Checking Aruba User Config ...
SIB: User config check complete.

APBoot 2.6.2.3 (build 80087)
Built: 2021-04-29 at 10:04:03

Model: AP-635
DRAM: 2 GiB
Flash: Detected MX25U6435F: total 8 MiB
MMC: 0 (eMMC)
PCIE: link up
Power: DC
Radio: qcn9072#0, ipq6010#1, ipq6010#2
Reset: cold
FIPS: passed

Hit <Enter> to stop autoboot: 0
SIB: Set Aruba Provisional SSID Broadcast to Disabled
printenv disable_prov_ssid
disable_prov_ssid=1
apboot> SIB: Provisional SSID Broadcast already Disabled
SIB: Current pins: 0x0f
SIB: Setting Aruba for DHCP mode

printenv ipaddr
## Error: "ipaddr" not defined
apboot>
SIB: Aruba ipaddr previously cleared

printenv netmask
## Error: "netmask" not defined
apboot>
SIB: Aruba netmask previously cleared

printenv gatewayip
## Error: "gatewayip" not defined
apboot>
SIB: Aruba gatewayip previously cleared

SIB: Aruba previous configuration correct. Update not required

SIB: APBOOT Configuration Complete
SIB: PT is enabled
SIB: DHCP: IP Assigned:
SIB: IP : 192.168.1.101
SIB: Net Mask : 255.255.255.0
SIB: Gateway : 192.168.1.1
SIB: SIB IP Valid - Starting MDS Server
SIB: Socket open OK: mode: 0x02 status: 0x22

apboot> :
```

Figure 5: Example Console Output of the AP Boot Process

While in **apboot** mode you have access to the following commands:

?	- alias for 'help'
boot	- boot the OS image
clear	- clear the OS image or other information
dhcp	- invoke DHCP client to obtain IP/boot params
factory_reset	- reset to factory defaults
help	- print command description/usage
mfginfo	- show manufacturing info
osinfo	- show the OS image version(s)
ping	- send ICMP ECHO_REQUEST to network host
printenv	- print environment variables
purgeenv	- restore default environment variables
reset	- Perform RESET of the CPU
saveenv	- save environment variables to persistent storage
setenv	- set environment variables
tftpboot	- boot image via network using TFTP protocol
upgrade	- upgrade the APBoot or OS image
version	- display version

The **setenv** command can be used to set the environment variables listed below. Enter commands one per line, replacing the equal sign with a space. To clear an environment variable, enter the variable name followed by <CR>.

```
os_partition=0
ipaddr=192.168.1.101
gatewayip=192.168.1.1
netmask=255.255.255.0
dnsip=8.8.8.8
name=IAP308
domainname=arubanetworks.com
```

4.3 IP Strapping Table

In IP Strapping mode the Cabin AXe™ will get two IP addresses assigned on the 192.168.10.0/24 network with the default gateway address 192.168.10.1.

The IP addresses that will be assigned are shown in Table 5.

Table 5: IP Strapping Table

ADDR3	ADDR2	ADDR1	ADDR0	Hostname Strapping		IP Strapping	
				Hostname	IP Offset	Standard Map	Reverse Map
Open	Open	Open	Open	WAP01	DHCP	DHCP	DHCP
Open	Open	Open	GND	WAP02	DHCP	192.168.10.24	192.168.10.10
Open	Open	GND	Open	WAP03	DHCP	192.168.10.23	192.168.10.11
Open	Open	GND	GND	WAP04	DHCP	192.168.10.22	192.168.10.12
Open	GND	Open	Open	WAP05	DHCP	192.168.10.21	192.168.10.13
Open	GND	Open	GND	WAP06	DHCP	192.168.10.20	192.168.10.14
Open	GND	GND	Open	WAP07	DHCP	192.168.10.19	192.168.10.15
Open	GND	GND	GND	WAP08	DHCP	192.168.10.18	192.168.10.16
GND	Open	Open	Open	WAP09	DHCP	192.168.10.17	192.168.10.17
GND	Open	Open	GND	WAP10	DHCP	192.168.10.16	192.168.10.18
GND	Open	GND	Open	WAP11	DHCP	192.168.10.15	192.168.10.19
GND	Open	GND	GND	WAP12	DHCP	192.168.10.14	192.168.10.20
GND	GND	Open	Open	WAP13	DHCP	192.168.10.13	192.168.10.21
GND	GND	Open	GND	WAP14	DHCP	192.168.10.12	192.168.10.22
GND	GND	GND	Open	WAP15	DHCP	192.168.10.11	192.168.10.23
GND	GND	GND	GND	WAP16	DHCP	192.168.10.10	192.168.10.24

Default mode is: IP Strapping, Reverse Map

4.4 Connecting using the Console Port

The integrated USB to UART provides console access via the micro USB port that is located behind the maintenance door. Use these settings to connect to the console:

Port	COM*
Baud rate	9600
Data	8 bit
Parity	None
Stop	1 bit
Flow Control	None

* Select the newly added USB Serial Port

Connecting to the console port gives you access to SIB boot, AP boot, SIB command mode, and the Aruba Instant Access Point (IAP) Command Line Interface (CLI).

The IAP CLI becomes available after completion of the startup process, and requires administrator credentials to start a session. Refer to section 4.5.1 for the default credentials.

After login, the privileged command mode is enabled which provides access to **show**, **clear**, **ping**, **traceroute**, and **commit** commands. The configuration commands are available in the configuration (config) mode. To move from privileged mode to the configuration mode, enter the following command at the command prompt:

```
(Cabin AXe) # configure terminal
```

The configure terminal command allows you to enter the basic configuration mode and the command prompt is displayed as follows:

```
(Cabin AXe) (config) #
```

Some commands in configuration mode allow you to enter into a sub-mode to configure the commands specific to that mode. When you are in a configuration sub-mode, the command prompt changes to indicate the current sub-mode.

You can exit a sub-command mode and return to the basic configuration mode or the privileged Exec (enable) mode at any time by executing the **exit** or **end** command.

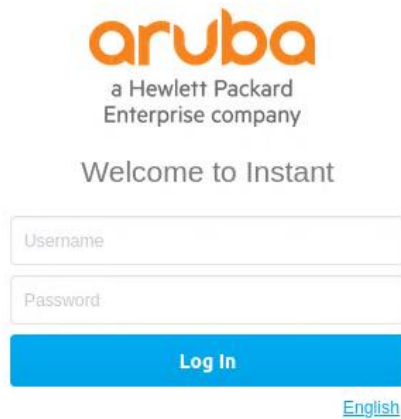
You can use the question mark (?) to view the commands available for your current mode.

Refer to the *Aruba Instant CLI Reference Guide*, for additional information on the IAP CLI.

4.5 Connecting using Web-based GUI

You can connect to the web-based GUI by entering the Aruba AP's IP address in a web browser, and entering the Username and Password when prompted as shown below in Figure 6. If the IP strapping pins have not been set, you can use the **show ip interface** CLI command to display the IP address that was assigned by your DHCP server

Note: The following subsections refer to the [Aruba] IAP, or AP which shall be used interchangeably with the CWAP. The sections are summarized from Aruba Instant documentation and training materials. For additional information refer to the Aruba Instant User Guide.



The image shows the Aruba Instant GUI login page. At the top is the Aruba logo with the text 'a Hewlett Packard Enterprise company'. Below this is the text 'Welcome to Instant'. There are two input fields: 'Username' and 'Password'. Below the password field is a blue 'Log In' button. To the right of the button is a link that says 'English'.

Figure 6: Aruba Instant GUI Login Prompt

You may see a Certificate Error message. This is because the certificates issued to the AP do not match the IP address used to connect to the GUI. It is recommended that you add a certificate issued by your network, to ensure secure administrative communication.

The main GUI page is broken up into the following sections. These sections are identified below Figure 7.
Note: The left-most panel on the GUI provides access to Dashboard, Configuration, Maintenance, and Support areas.

1. **Overview**—This section displays the number of configured networks, access points, and clients.
2. **Info**—This section displays information about the access point name, country code, virtual controller IP address, management, conductor Instant AP IP address, IPv6 address, uplink type, and uplink status.
3. **Clients**—The Clients graph displays the number of clients that were associated with the virtual controller in the last 15 minutes.
4. **Throughput**—The Throughput Graph shows the throughput of the selected client for the last 15 minutes.
 - a. **Out** – Throughput for the outgoing traffic is displayed in blue.
 - b. **In** - Throughput for the incoming traffic is displayed in orange. To see an enlarged view, click the graph. To see the exact throughput at a particular time, move the cursor over the graph line.
5. **RF Dashboard**—This section displays the Instant APs that exceed the utilization, noise, or error threshold. It also shows the clients with low speed or signal strength in the network and the RF information for the Instant AP to which the client is connected.

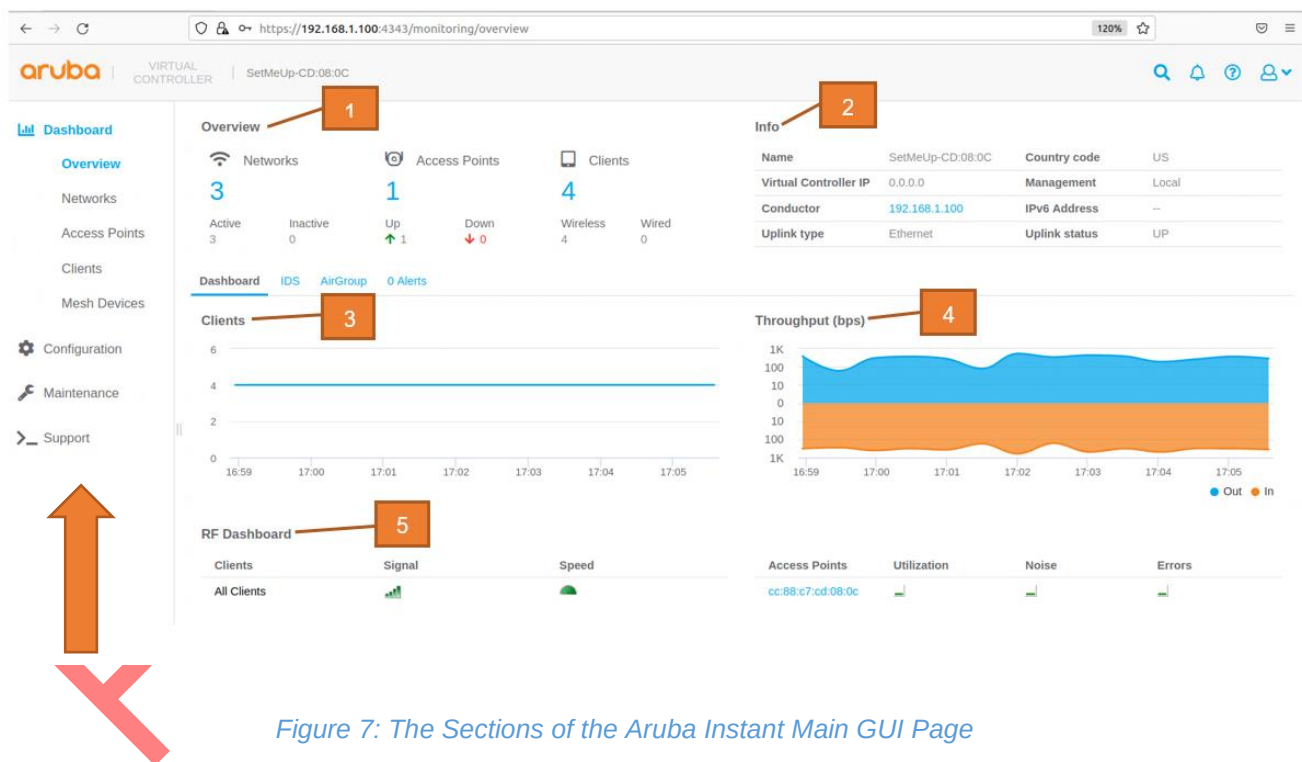


Figure 7: The Sections of the Aruba Instant Main GUI Page

4.5.1 System Username and Password

The default username for the Aruba is *admin*. The default password will be one of the following, *admin*, *cabinaxe*, or the Aruba serial number. It is recommended that these be changed. The system username and password can be changed from the Admin selection in the GUI. Using the options on the GUI left-most panel, the path to set this is: *Configuration > System*, then select *Admin* from the GUI as shown in Figure 8.

The screenshot shows the Aruba Virtual Controller GUI. The browser address bar indicates the URL is `https://192.168.1.100:4343/configuration/system`. The left sidebar contains a 'Configuration' menu item, which is highlighted with a red arrow. The main content area shows the 'System' configuration page. Under the 'General' tab, the 'Admin' section is expanded. The 'Local' section has a dropdown for 'Authentication' set to 'Internal', a 'Username' field with 'admin', and 'Password' and 'Retype' fields with masked characters. An orange arrow points to the 'Password' field. Below 'Local' are sections for 'View Only', 'Guest Registration Only', 'AirWave', and 'SSH'. At the bottom, there is a 'Show advanced options' button.

Figure 8: System Username and Password Dialog Box.

4.6 Virtual Controller Architecture

The Aruba IAP uses a Virtual Controller architecture for ease of deployment and centralized wireless network management.

An Instant AP cluster consists of member Instant APs and a conductor Instant AP in the same VLAN, as they communicate with broadcast messages. A virtual controller is a combination of the whole cluster, as the member Instant APs and conductor Instant AP coordinate to provide a controllerless Instant solution. In an Instant deployment scenario, the first Instant AP that comes up becomes the conductor Instant AP. All other Instant APs joining the cluster after that Instant AP, become the member Instant APs.

In an Instant deployment scenario, only the first Instant AP or the conductor Instant AP needs to be configured. The other Instant APs download configurations from the first Instant AP that is configured. The Instant solution constantly monitors the network to determine the Instant AP that must function as a conductor Instant AP at a given time. The conductor Instant AP may change as necessary from one Instant AP to another without impacting network performance. Each Instant AP model has a minimum required software version.

You can set the name of the virtual controller along with other configuration parameters, from the General tab of the System dialog box, as show in Figure 9 below.

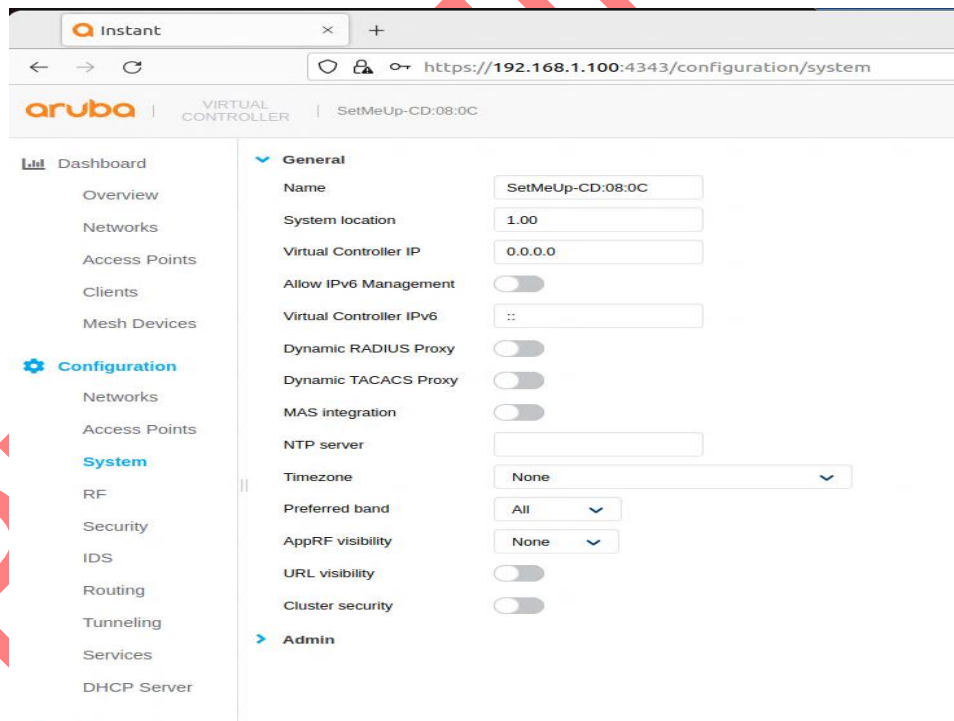


Figure 9: The Virtual Controller General Setup screen.

4.6.1 IAP Configuration

On the Configuration GUI page you can select one of the IAPs and edit the configuration. You should give each of your IAPs a relevant name for easy identification. You can also select which IAP will be the preferred master. Whichever IAP is configured as the preferred master will also become the virtual controller. Access is via the left-panel: **Configuration > Access Points** (Select the Access Point, and use the edit “pencil”). See Figures 10 & 11.

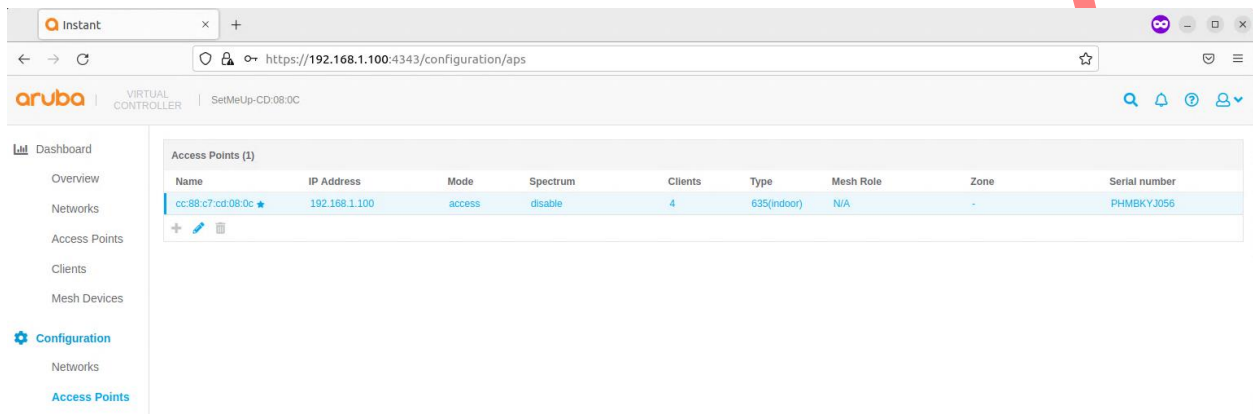


Figure 10: Select / Edit the Access Point screen.

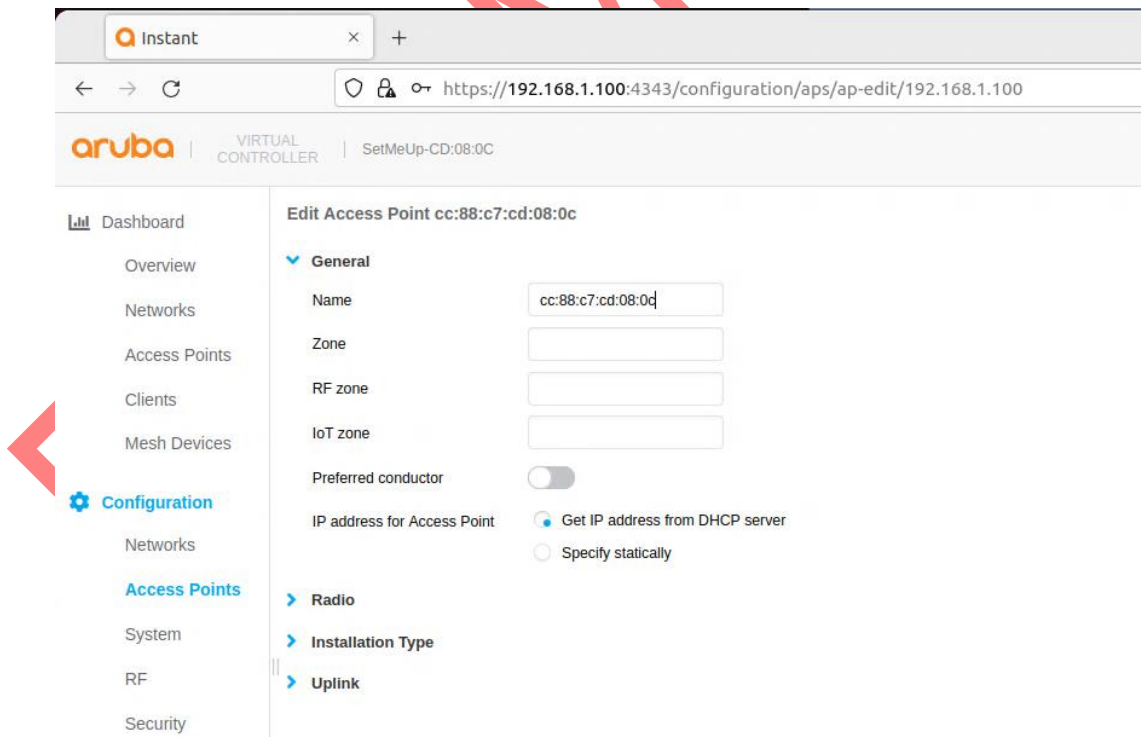


Figure 11: The Edit Access Point screen.

4.7 WLAN Setup

There are four steps to creating an SSID:

1. Configure WLAN Settings. Select the type of SSID you want to create.
 - a. Employee Network: This network type is used by the employees in an organization and it supports passphrase-based or 802.1X-based authentication methods.
 - b. Voice Network: This network type provides voice traffic prioritization, and allows you to configure a network profile for devices that only provide voice services.
 - c. Guest Network: Provides captive portal or passphrase-based authentication methods for non-employee users.
2. Configure VLAN Settings for a WLAN SSID Profile.
3. Configure Security Settings for a WLAN SSID Profile.
 - a. Enterprise and Personal support a variety of encryption methods.
 - b. The Open security level, no encryption settings are required, but optional methods are available.
4. Configure Access Rules for a Network.

The GUI used to configure SSIDs is shown below in Figure 12. Click on the “+” button to add a new SSID.

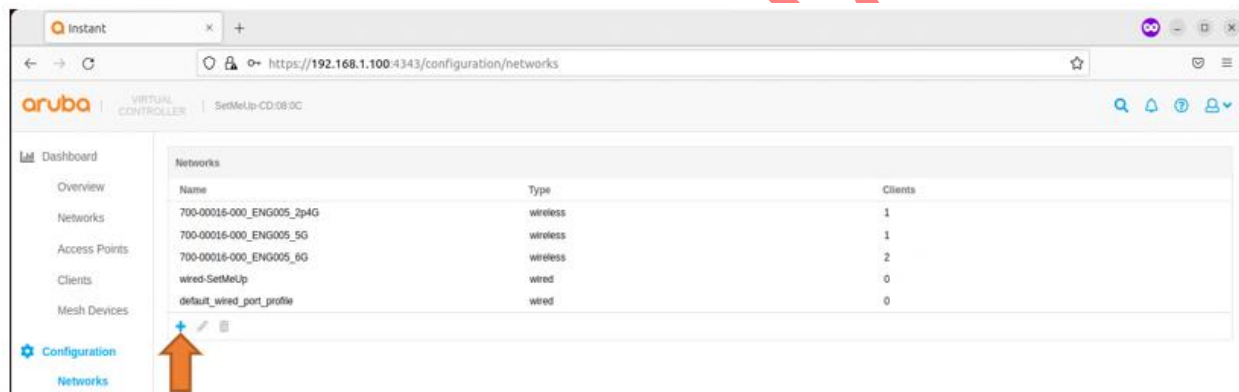


Figure 12: Creating an SSID

Step 1

Clicking the “ + ” button brings up the **New Network - Basic** tab. Provide a name for the new network, and select the type of SSID you want to create as shown in Figure 13

The screenshot displays the Aruba Virtual Controller web interface. At the top, there's a browser tab labeled 'Instant' and a URL bar showing 'https://192.168.1.100:4343/configuration/networks/network-add'. Below the browser bar, the Aruba logo and 'VIRTUAL CONTROLLER' text are visible, along with a session timer 'SetMeUp-CD:08:0C'. The main navigation menu on the left includes 'Dashboard' (with sub-items: Overview, Networks, Access Points, Clients, Mesh Devices) and 'Configuration' (with sub-item: Networks). The 'New Network' button is highlighted in blue. The configuration tabs at the top are '1 Basic', '2 VLAN', '3 Security', and '4 Access'. The 'Basic' tab is active, showing the 'Name & Usage' section. It contains three fields: 'Name' with the value 'Test_Network1', 'Type' with a dropdown menu set to 'Wireless', and 'Primary usage' with a dropdown menu set to 'Employee'. The 'Primary usage' dropdown is open, showing options: 'Employee', 'Voice', and 'Guest'. A large red 'PRELIM' watermark is diagonally across the image.

Figure 13: The Basic Tab of the New Network configuration GUI

Step 2

The VLAN screen is where you configure the VLAN assignment and client IP assignment. The available VLAN and client IP assignment options are shown below in Figure 14.

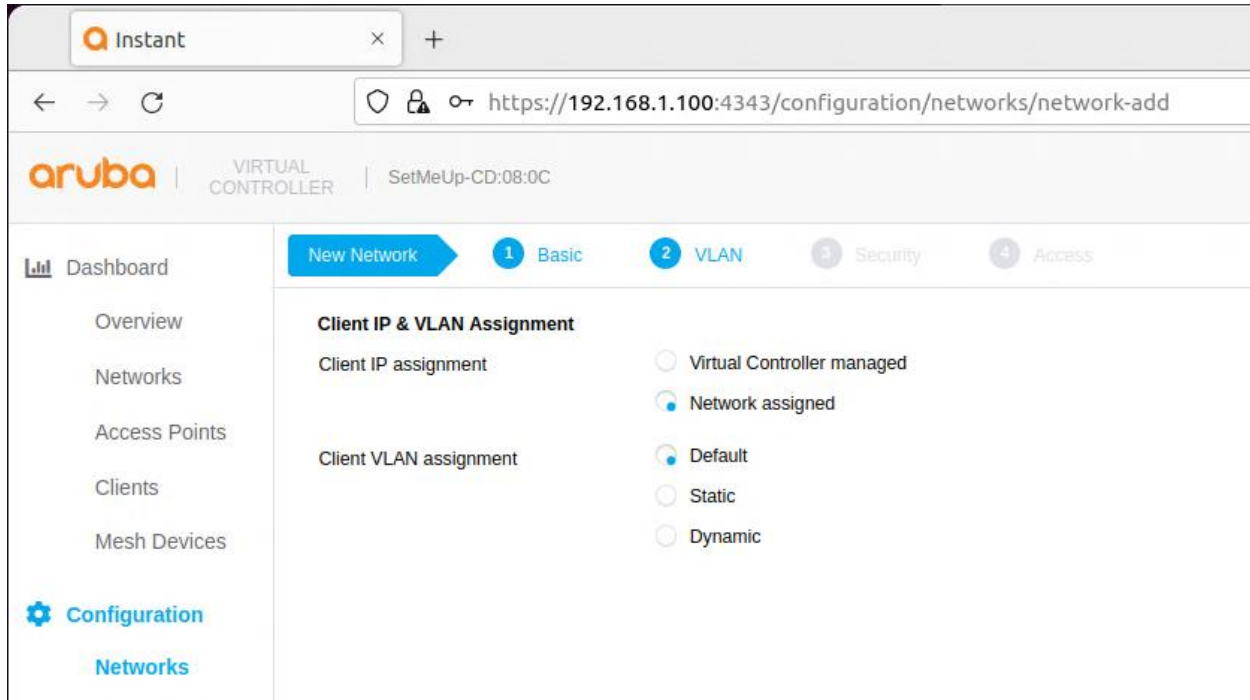


Figure 14: The VLAN Tab of the New Network GUI screen

The two client IP assignment options are Virtual Controller Managed and Network assigned.

Virtual Controller Managed

On selecting this option, the wired client obtains the IP address from the virtual controller. When this option is used, the source IP address is translated to the physical IP address of the conductor Instant AP for all client traffic that goes through this interface. The virtual controller can also assign a guest VLAN to the client.

Network Assigned

On selecting this option, the IP address is obtained from the network.

Step 3

The Security tab is where you set the security level. There are three levels; Open, Personal, and Enterprise. Selecting the Open level provide options shown in Figure 15.

The screenshot shows the Aruba Virtual Controller SetMeUp interface. The top header includes the Aruba logo, 'VIRTUAL CONTROLLER', and 'SetMeUp-CD:08:0C'. The left sidebar contains navigation links: Dashboard, Configuration (with sub-links for Networks, Access Points, System, RF, Security, IDS, Routing, Tunneling, and Services), and a 'New Network' button. The main content area is titled 'New Network' and has three steps: 1 Basic, 2 VLAN, and 3 Security. The 'Security' step is active, showing the 'Security Level' dropdown set to 'Open'. Below this, there are settings for Encryption (None), Enhanced Open (checked), MAC authentication (unchecked), Denylisting (unchecked), and Enforce DHCP (unchecked). Under the 'Fast Roaming' section, 802.11k and 802.11v are both unchecked.

aruba | VIRTUAL CONTROLLER | SetMeUp-CD:08:0C

Dashboard

Configuration

- Networks
- Access Points
- System
- RF
- Security
- IDS
- Routing
- Tunneling
- Services

New Network

1 Basic 2 VLAN 3 Security

Security Level

Security Level Open

Encryption None

Enhanced Open ☒

MAC authentication ☐

Denylisting ☐

Enforce DHCP ☐

Fast Roaming

802.11k ☐

802.11v ☐

Figure 15: Open Security level options

Selecting the Personal level provides the options shown in Figure 16.

VIRTUAL CONTROLLER

SetMeUp-CD:08:0C

Dashboard

Configuration

Networks

Access Points

System

RF

Security

IDS

Routing

Tunneling

Services

DHCP Server

Maintenance

New Network

1 Basic

2 VLAN

3 Security

Security Level

Security Level

Personal

Key management

WPA2-Personal

Passphrase format

8-63 chars

Passphrase

Retype

MAC authentication

Denylisting

Enforce DHCP

Fast Roaming

802.11r

802.11k

802.11v

Figure 16: Personal Security level options

Finally, selecting the Enterprise level allows you to configure an external RADIUS authentication server, as shown below in Figure 17.

The screenshot displays the Aruba Virtual Controller web interface for configuring a new network. The browser address bar shows the URL: `https://192.168.1.100:4343/configuration/networks/network-add`. The page header includes the Aruba logo and the text "VIRTUAL CONTROLLER" and "SetMeUp-CD:08:0C".

The left sidebar contains a navigation menu with the following items: Dashboard, Overview, Networks, Access Points, Clients, Mesh Devices, Configuration (highlighted), Networks (highlighted), Access Points, System, RF, Security, IDS, Routing, Tunneling, Services, and DHCP Server.

The main content area is titled "New Network" and features four tabs: 1 Basic, 2 VLAN, 3 Security (active), and 4 Access. The "Security" tab is selected, showing the following configuration options:

- Security Level:** Enterprise (dropdown)
- Key management:** WPA2-Enterprise (dropdown)
- Authentication server 1:** InternalServer (dropdown) with a "+" button
- Reauth interval:** 0 (input field) and min. (dropdown)
- MAC authentication:**
 - ☐ Perform MAC authentication before 802.1X
 - ☐ MAC authentication fail-thru
- Internal server:** No users (text) and Users (link)
- Denylisting:** ☐
- Enforce DHCP:** ☐
- Fast Roaming:**
 - Opportunistic Key Caching(OKC):** ☐
 - 802.11r:** ☐
 - 802.11k:** ☐
 - 802.11v:** ☐

A red "PROV" watermark is visible across the bottom half of the image.

Figure 17: Enterprise Security level options

Step 4

The Access tab is where you configure the firewall rules and user rights. As shown in Figure 18, the Access tab allows you to create Network-Based rules and Role-Based rules. You also have the option to leave the SSID Unrestricted.

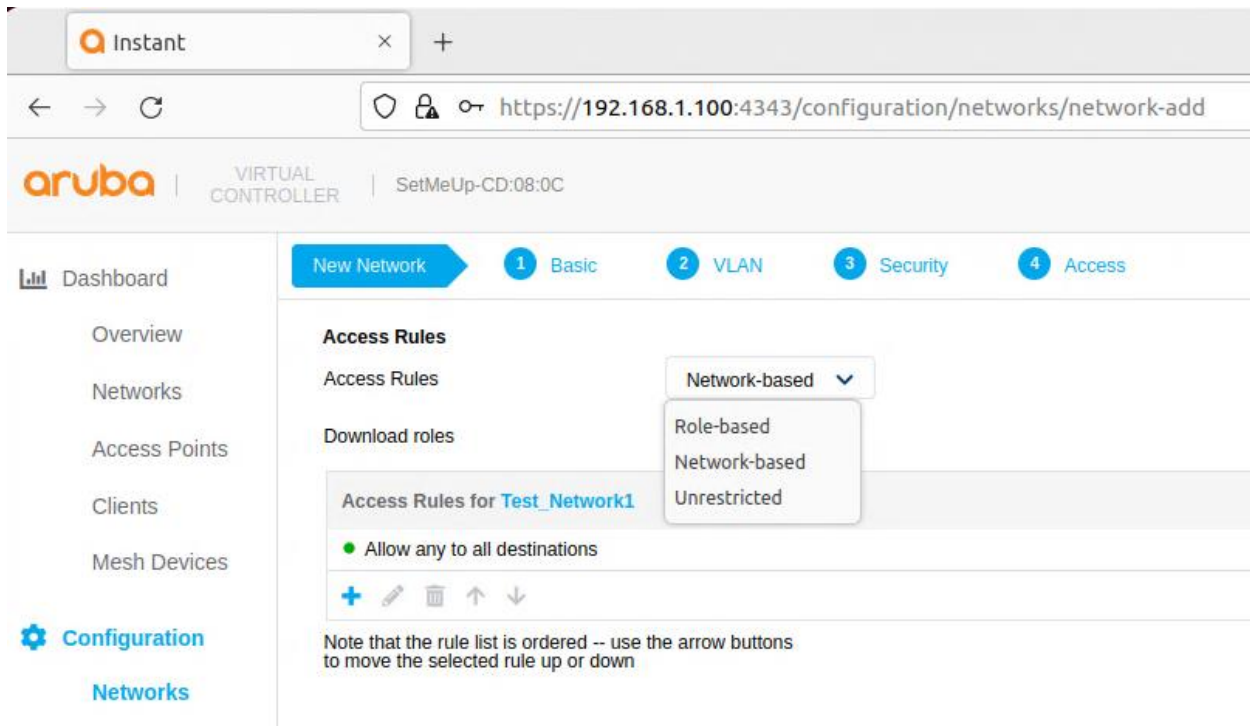


Figure 18: Access Rules options

Figure 19 shows an example of creating a rule that denies all DNS traffic except to the DNS server with the IP address of 192.168.10.1.

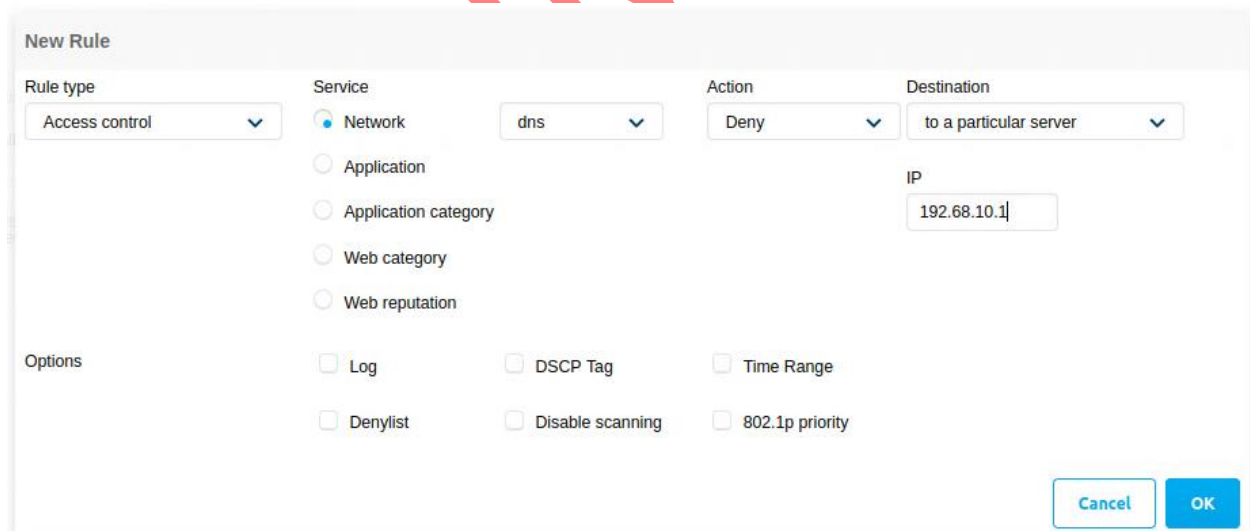


Figure 19: Configuring Firewall Rules

Refer to the *Aruba Instant Users Guide* for additional information on the Virtual Controller GUI.

4.7.1 6 GHz Radio Considerations

To maintain regulatory compliance while operating on aircraft, additional frequency restrictions may be required. The rf dot11-6ghz-radio-profile can be used to select the allowed channels. The following radio profile can be used to restrict 6 GHz operation to only allow the U-NII-5 band.

- rf dot11-6ghz-radio-profile
- allowed-channels 1,5,9,13,17,21,25,29,33,37,41,45,49,53,57,61,65,69,73,77,81,85,89,93

PRELIMINARY

5 Physical I/O

5.1 Connections and Cabling

Table 6 lists the CWAP's external connector interfaces (per ARINC 628).

Table 6: CWAP External Connector Interfaces

Ref Des.	Shell	Insert	Mating Shell	Mating Insert
J1	EN4165M01AA	EN4165A20-22-1NA	EN4165M61AA	EN4165A20-22-1NB
J2	EN4165M01AB	EN4165A20-22-1NB	EN4165M61AB	EN4165A20-22-1NA
J3	EN4165M01AC	EN4165A20-22-1NA	EN4165M61AC	EN4165A20-22-1NB

5.1.1 Connector Definition J1

The J1 connector carries the input power, connects the CWAP to the upstream server/network, and carries both the Power Enable and RF Enable discrete signals to the unit.

Figure 20 shows connector layout and pin definitions for the CWAP's J1 external aircraft connection.

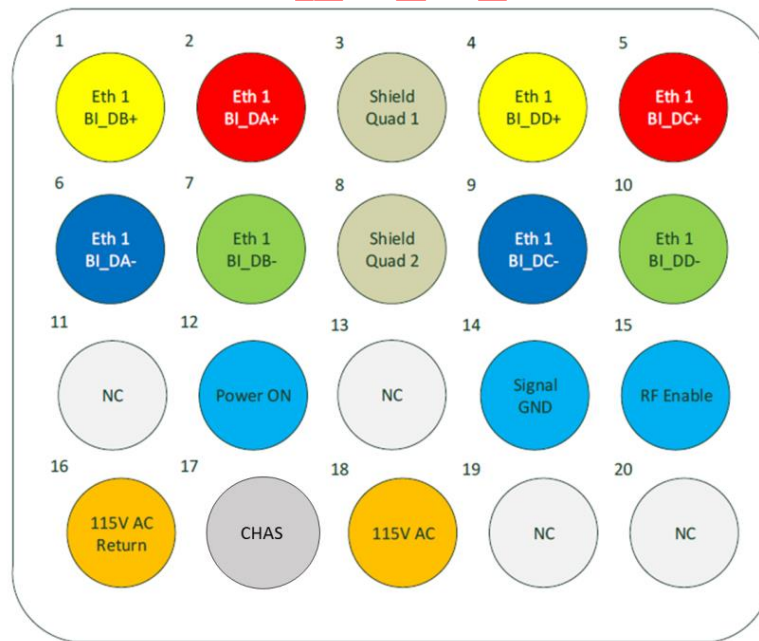


Figure 20: J1 (Pins) Connector Layout and Pin Definitions

5.1.2 Connector Definition J2

The J2 connector passes power, Ethernet and both the Power Enable, and RF Enable discrete signals to the next downstream CWAP when the units are in a Daisy Chain configuration.

Figure 21 shows connector layout and pin definitions for the CWAP's J2 external aircraft connection.

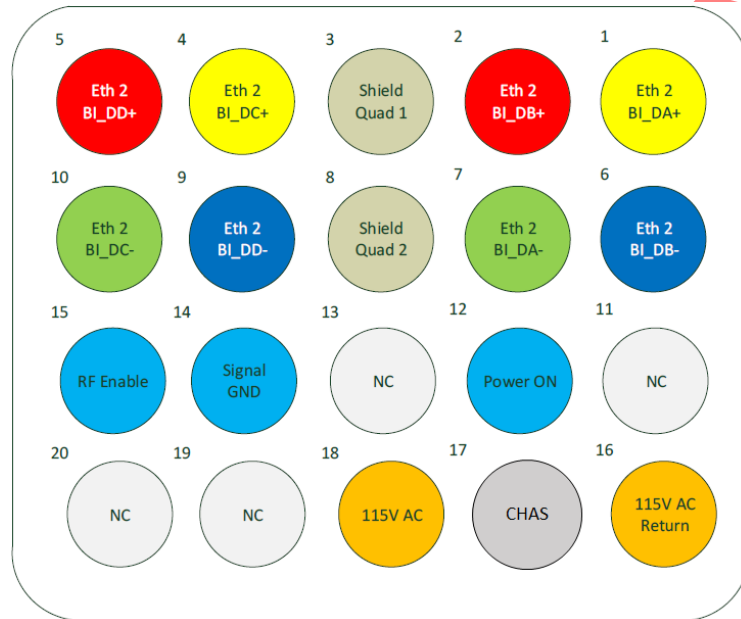


Figure 21: J2 (Socket) Connector Layout and Pin Definitions

5.1.3 Connector Definition J3

The J3 carries the discrete IP strapping signals from the aircraft to the CWAP. Figure 22 shows connector layout and pin definitions for the CWAP's J3 external aircraft connection. Please see Table 5 for IP Address information.

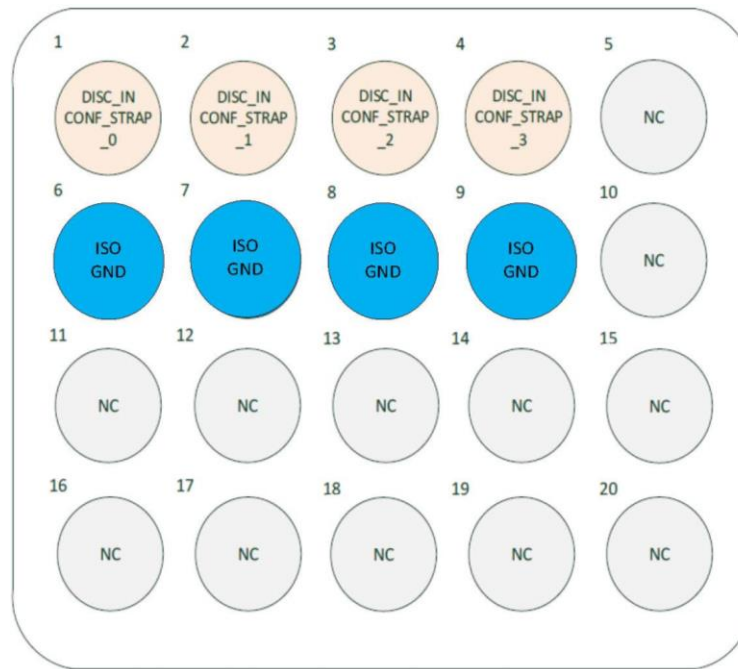


Figure 22: J3 (Socket) Connector Layout and Pin Definitions

5.2 Maintenance Connectors

Two maintenance connectors are located on the front of the unit behind the maintenance door.

- The J10 connector is a female micro USB that provides a serial interface to both the SIB and the AP.
- A four pin SIB programming header is located below the J10 connector. This programming header provides an interface for programming the SIB bootloader.

Reset button

The reset button is located behind the maintenance door. Holding the reset button for 5 seconds, until the power LED rapidly blinks, will factory reset the Aruba AP.

5.3 Status Indicators

The CWAP has four (4) AP status LEDs, and three (3) CWAP indicators that are visible on the top (radome) of the CWAP and are to be used to indicate the AP status and activity. The meanings of these indicators are defined in Table 7 below.

Table 7: AP LED Operation

Indicator	Color/State	Meaning
AP Status LED	OFF	AP Powered OFF.
	Green - Solid	AP ready, fully functional, no network restrictions.
	Green - Blinking ^{note 1}	AP booting, not ready.
	Green - Flashing Off ^{note 2}	Device ready, fully functional, either uplink negotiated in sub-optimal speed (<1Gbps).
	Amber - Solid	Device ready, restricted power mode, no network restrictions.
	Amber - Flashing Off	Device ready, restricted power mode, uplink negotiated in sub-optimal speed.
	Red - Solid	System error condition.
AP Radio Status (One each for 2.4GHz, 5GHz, 6GHz radios)	OFF	Device is powered OFF, or radios disabled.
	Green - Solid	Radios enabled in access mode.
	Green - Flashing Off	One radio enabled in uplink or mesh mode.
	Amber - Solid	Radios enabled in monitor mode or spectrum analysis mode.
CWAP Power	Green - Solid	AC is present – No fault detected.
	Red - Solid	AC power present – Fault detected.
Ethernet Link (LAN 1, LAN 2)	Green - Blinking	Indicates link activity for LAN 1 (J1 connector) and LAN 2 (J2 connector).

Notes:

1. Blinking: one second on, one second off, 2-seconds cycle
2. Flashing off: mostly on, fraction of a second off, 2-second cycle

6 Performance Data

6.1 Radio Characteristics

Table 8: Radio Characteristics

Feature	Description
Supported Frequency Bands (country-specific restrictions apply)	-2.400 to 2.4835 GHz ISM -5.150 to 5.250 GHz U-NII-1 -5.250 to 5.350 GHz U-NII-2 -5.470 to 5.725 GHz U-NII-2E -5.725 to 5.850 GHz U-NII-3/ISM * -5.850 to 5.895 GHz U-NII-4 * -5.925 to 6.425 GHz U-NII-5 ** -6.425 to 6.525 GHz U-NII-6 * -6.525 to 6.875 GHz U-NII-7 * -6.875 to 7.125 GHz U-NII-8 *
Operating Channels	Dependent on configured regulatory domain.
Supported radio technologies	-802.11b: Direct-sequence spread-spectrum (DSSS) -802.11a/g/n/ac: Orthogonal frequency-division multiplexing (OFDM) -802.11ax: Orthogonal frequency-division multiple access (OFDMA)
Supported Modulation Types	-802.11b: BPSK, QPSK, CCK -802.11a/g/n/ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM -802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM, 4096-QAM -802.11n high-throughput (HT) support: HT20/40 -802.11ac very high throughput (VHT) support VHT20/40/80 -802.11ax high efficiency (HE) support HE20/40/80/160
Transmit Power Adjustment	Software configurable in increments of 0.5 dBm.
Maximum Available Transmit Power***	Maximum (aggregate, conducted total) transmit power (limited by local regulatory requirements): -2.4GHz band: +21 dBm (18 dBm per chain) -5 GHz band: +21 dBm (18 dBm per chain) -6 GHz band: +21 dBm (18 dBm per chain) -Note: conducted transmit power levels exclude antenna gain. For total (EIRP) transmit power, add antenna gain + correlation gain.
Supported data rates (Mbps)	-802.11b: 1, 2, 5.5, 11 -802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54 -802.11n: 6.5 to 400 -802.11ac: 6.5 to 1,083 -802.11ax (2.4GHz) 3.6 to 574 -802.11ax (5GHz) 3.6 to 1,201 -802.11ax (6GHz) 3.6 to 2,882
Wi-Fi Antennas	Integrated downtilt omni-directional antennas for 2x2 MIMO with peak antenna gain of 4.6 dBi in 2.4GHz, 7.0 dBi in 5GHz and 6.3 dBi in 6GHz. Built-in antennas are optimized for horizontal overhead orientation of the AP. The downtilt angle for maximum gain is roughly 30 to 40 degrees.
Bluetooth Low Energy (BLE5.0) and Zigbee (802.15.4) radio	-BLE: up to 5 dBm transmit power (class 1) and -100 dBm receive sensitivity (125 kbps) -Zigbee: up to 5 dBm transmit power and -97 dBm receive sensitivity (250 kbps)

* Country specific restrictions apply.

** This band range is 5945-6425 for EU based on country specific restrictions.

***The aggregate EIRP is limited to 20dBm (100mW)

6.2 RF Performance Table

The 2.4GHz transmitter has a maximum Radiated output power as follows:

Table 9: 2.4GHz Maximum Radiated Output Power

Frequency Range (MHz)	Mode	Output Power (dBm)	Output Power (mW)
2412 - 2484	802.11b	20*	100
2412 - 2484	802.11g	20*	100
2412 - 2484	802.11n-HT20	20*	100
2412 - 2484	802.11n-HT40	20*	100
2412 - 2484	802.11ax-HE20	20*	100
2412 - 2484	802.11ax-HE40	20*	100

*The aggregate EIRP is limited to 20dBm (100mW)

The 5GHz transmitter has a maximum Radiated output power as follows:

Table 10: 5GHz Maximum Radiated Output Power

Frequency Range (MHz)	Mode	Output Power (dBm)	Output Power (mW)
5150 - 5895	802.11a	20.0*	100
5150 - 5895	802.11ac-VHT20	20.0*	100
5150 - 5895	802.11ac-VHT40	20.0*	100
5150 - 5895	802.11ac-VHT80	20.0*	100
5150 - 5895	802.11ax-HE20	20.0*	100
5150 - 5895	802.11ax-HE40	20.0*	100
5150 - 5895	802.11ax-HE80	20.0*	100

*The aggregate EIRP is limited to 20dBm (100mW)

The 6GHz transmitter has a maximum Radiated output power as follows:

Table 11: 6GHz Maximum Radiated Output Power

Frequency Range (MHz)	Mode	Output Power (dBm)	Output Power (mW)
5925 - 7125	802.11ax-HE20	20.0*	100
5925 - 7125	802.11ax-HE40	20.0*	100
5925 - 7125	802.11ax-HE80	20.0*	100
5925 - 7125	802.11ax-HE160	20.0*	100

*The aggregate EIRP is limited to 20dBm (100mW)

PRELIMINARY

7 Technical Data

7.1 Electrical and Environmental Specifications

The CWAP meets the electrical and environmental test categories per Table 12 and Table 13.

Table 12: Qualification Test Matrix - Environment

Test Description	Test Spec	Test Section / Category
Temperature		
Ground Survival Low Temp and Short Time Operating Low Temp	DO-160G	§4.5.1, CAT A1
Operating Low Temperature	DO-160G	§4.5.2, CAT A1
Ground Survival High Temp. and Short Time Operating High Temp.	DO-160G	§4.5.3, CAT A1
Operating High Temperature	DO-160G	§4.5.4, CAT A1
Temperature Variation (2°/min)	DO-160G	§5.0 CAT C
Altitude (15,000 FT)	DO-160G	4.6.1 CAT A1
Decompression (50,000 FT)	DO-160G	4.6.2 CAT A1
Overpressure (170 kPa)	DO-160G	4.6.3 CAT A1
Humidity	DO-160G	6.3.1, CAT A
Waterproofness (140 l/m ² /Hr)	DO-160G	10.3.2, CAT W
Vibration – Random	DO-160G	8.5.2, CAT S, Curve C
Operational Shock	DO-160G	7.2.1, CAT B
Crash Safety – Impulse (20g/11ms)	DO-160G	7.3.1, CAT B
Crash Safety –Sustained (12g/3s min) ⁽¹⁾	DO-160G	7.3.3,CAT B
Fungus Resistance ⁽²⁾	DO-160G	13.0, CAT F

Notes:

(1) Crash Safety – Sustained satisfied by structural substantiation analysis and test, STP-700-00016-000 (Astronics)

(2) Fungus Resistance verified by analysis, FAS-700-00016-000 (Astronics)

Table 13: Qualification Test Matrix - EMI

Test Description	Test Spec	Test Section / Category
Magnetic Effect	DO-160G	§15CAT C
Power Input: Voltage and Frequency (ac)	DO-160G	§16.5.1.1.b CAT A(WF)X
Power Input: Voltage Modulation (ac)	DO-160G	§16.5.1.2 CAT A(WF)X
Power Input: Frequency Modulation (ac)	DO-160G	§16.5.1.3 CAT A(WF)X
Power Input: Momentary Power Interruptions (ac)	DO-160G	§16.5.1.4.b, c CAT A(WF)X
Power Input: Normal Transients, Normal Surge Voltage (ac)	DO-160G	§16.5.1.5.1.b CAT A(WF)X
Power Input: Normal Transients, Normal Frequency Transients (ac)	DO-160G	§16.5.1.5.2.b CAT A(WF)X
Power Input: Normal Frequency Variations (ac)	DO-160G	§16.5.1.6 b CAT A(WF)X
Power Input: Voltage DC Content (ac)	DO-160G	§16.5.1.7 b CAT A(WF)X
Power Input: Voltage Distortion (ac)	DO-160G	§16.5.1.8 CAT A(WF)X
Power Input: Abnormal Voltage and Frequency Limits in Steady State (ac)	DO-160G	§16.5.2.1 b CAT A(WF)X
Power Input: Momentary Undervoltage Operation (ac)	DO-160G	§16.5.2.2 b CAT A(WF)X
Power Input: Abnormal Surge Voltage (ac)	DO-160G	§16.5.2.3.1 b CAT A(WF)X
Power Input: Abnormal Frequency Transients (ac)	DO-160G	§16.5.2.3.2 b CAT A(WF)X
Power Input: Abnormal Frequency Variations (ac)	DO-160G	§16.5.2.3.3 b CAT A(WF)X
DC Current Content in Steady-State Operation (All ac Equipment)	DO-160G	§16.7.3
Inrush Current Requirements (ac and dc), Designation I	DO-160G	§16.7.5.2, CAT A(WF)I
Current Modulation in Steady-State Operation (ac), Designation L	DO-160G	§16.7.6 CAT A(WF)L
Power Factor (All ac Equipment)	DO-160G	§16.7.8 CAT A(WF)P
Voltage Spike	DO-160G	§17.4 CAT A
Audio Frequency Conducted Susceptibility – Power Inputs	DO-160G	§18 CAT R(WF)
Induced Signal Susceptibility: Magnetic Fields Induced into the Equipment	DO-160G	§19.3.1 CAT CW
Induced Signal Susceptibility: Electric Fields Induced into the Equipment	DO-160G	§19.3.2 CAT CW

Test Description	Test Spec	Test Section / Category
Induced Signal Susceptibility: Magnetic Fields Induced into Interconnecting Cables	DO-160G	§19.3.3 CAT CW
Induced Signal Susceptibility: Electric Fields Induced into Interconnecting Cables	DO-160G	§19.3.4 CAT CW
Induced Signal Susceptibility: Spikes Induced into Interconnecting Cables	DO-160G	§19.3.5 CAT CW
Radio Frequency Susceptibility: Conducted	DO-160G	§20.4 CAT T
Radio Frequency Susceptibility: Radiated	DO-160G	§20.5 CAT S
Emission of Radio Frequency Energy: Conducted RF Emissions	DO-160G	§21.4 CAT M
Emission of Radio Frequency Energy: Radiated RF Emissions	DO-160G	§21.5 CAT M
Lightning Induced Transient Susceptibility: Pin Injection Tests	DO-160G	§22.5.1 (Pin Injection - Damage Test) CAT A2
Lightning Induced Transient Susceptibility: Cable Bundle Tests	DO-160G	§22.5.2 (Cable Bundle - Multi stroke/Multi Burst - Functional Upset) Ethernet Cables (shielded): CAT J2L2 AC Power, Discrete Inputs (connector J1 and J2, unshielded): CAT G2L2 Address strapping connections (on J3): CAT G2L2
Electrostatic Discharge	DO-160G	§25 CAT A

7.2 Mechanical Design and Dimensions

The CWAPs metal components include a proper finish to offer maintenance-free service over the life of the CWAP. The CWAP's internal chassis, circuit cards, wiring and cabling, and other major components are mounted and secured to provide maximum protection against imposed shock and vibration.

7.2.1 Top View

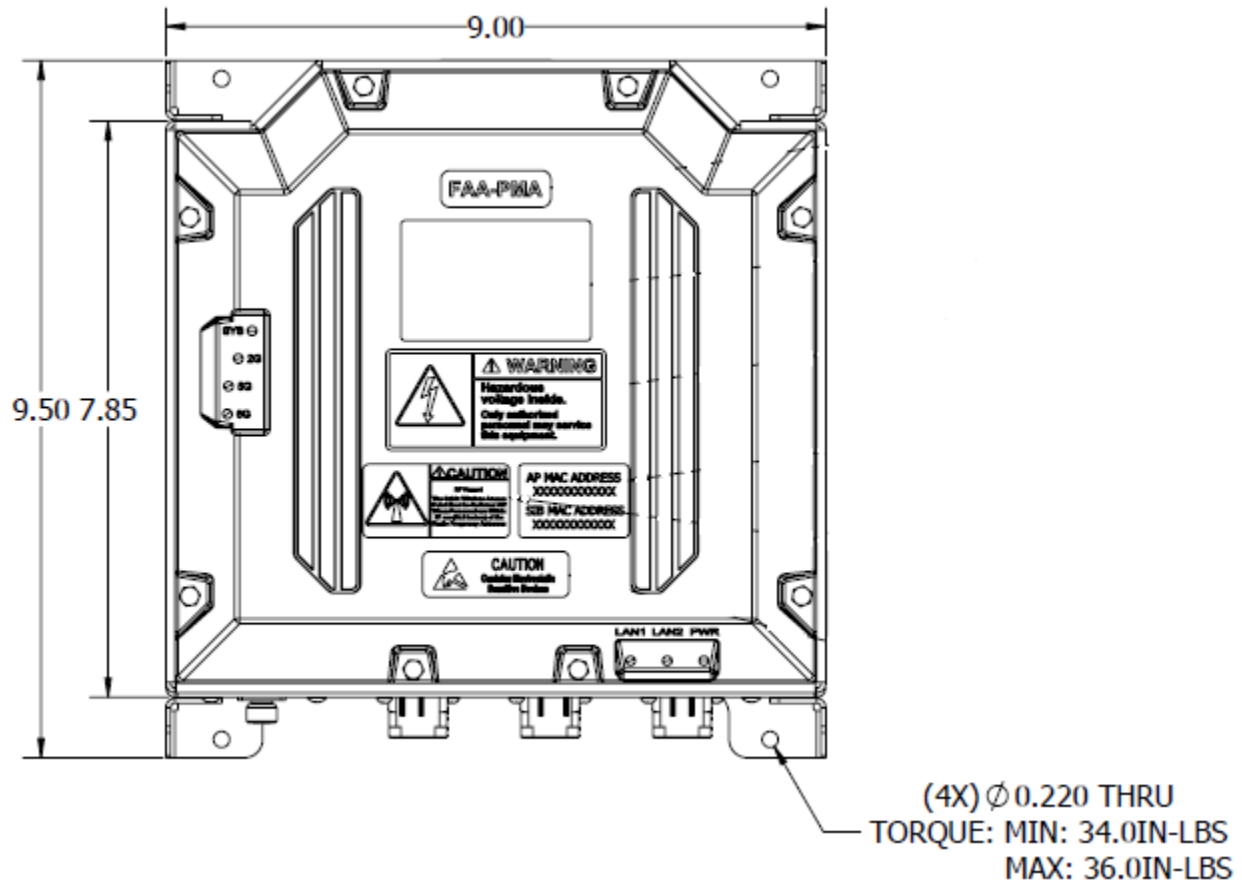


Figure 23: CWAP Top View

7.2.2 I/O Front View

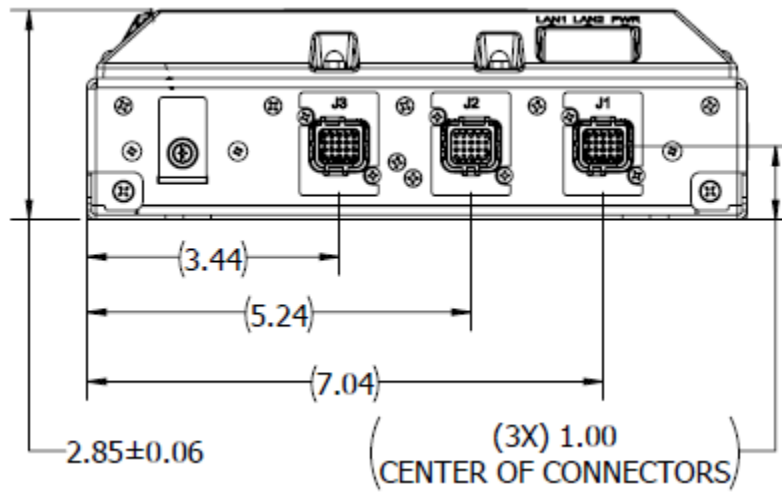


Figure 24: CWAP I/O Front View

7.2.3 Side View – Right

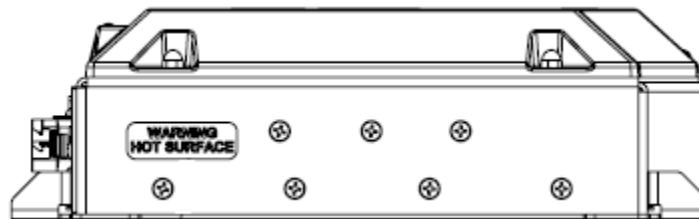


Figure 25: CWAP Side View - Right

7.2.4 Side View – Left

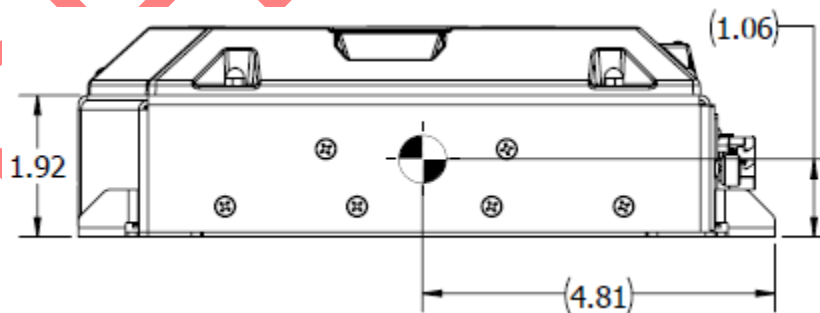


Figure 26: CWAP Side View – Left

7.2.5 Rear View

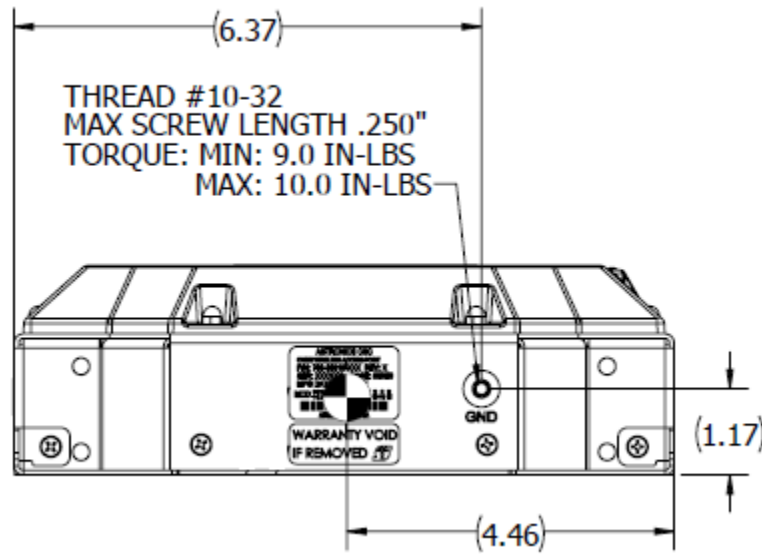


Figure 27: CWAP Rear View

7.2.6 Bottom View

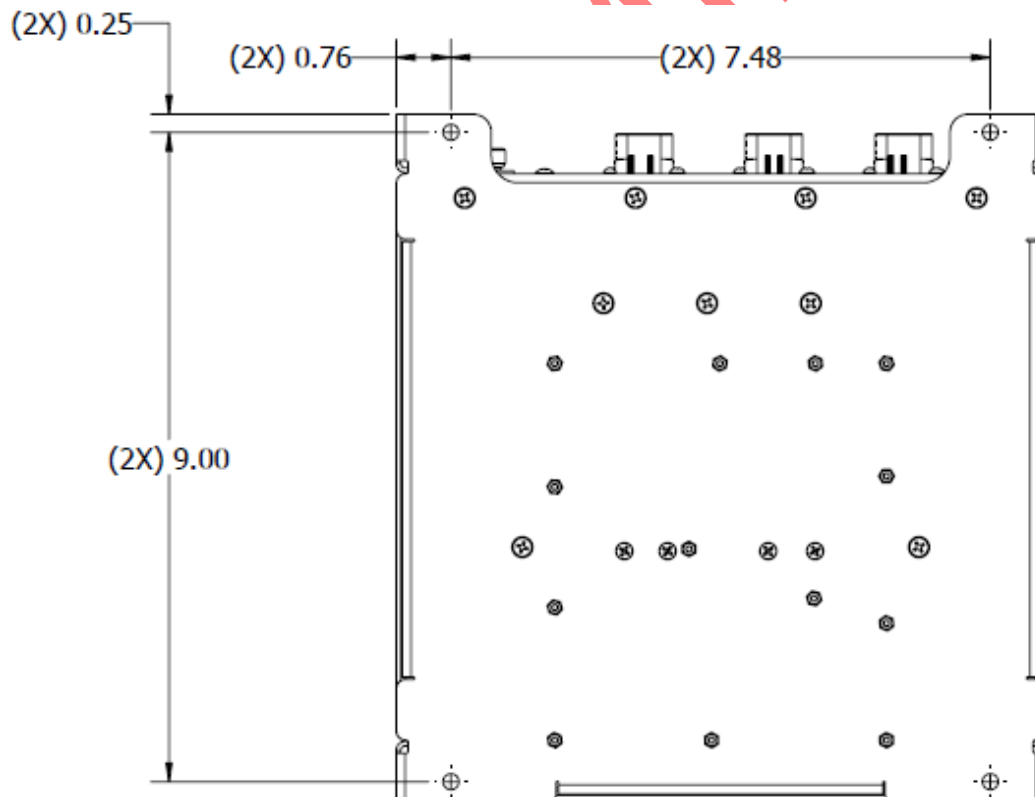


Figure 28: CWAP Bottom View

7.2.7 Product Identification

The Part Number Identification Label for each CWAP LRU is located on the rear panel and contains information as shown in Figure 27.

7.2.8 Finish and Color

The paint color of the CWAP is medium texture black. The bottom surface of the mounting plate is unpainted and contains a clear, RoHS compliant coating per MIL-DTL-5541, Type II, Class 3. The unpainted surface is provided for bonding of the CWAP enclosure to the aircraft airframe.

7.2.9 Materials

All materials used in the construction of the CWAP are inherently non-nutrient to fungus and do not support combustion. The materials are of the best commercial quality and will not blister, corrode, crack, soften, or show other immediate latent defects that affect the storage, operation, or environmental capabilities of the unit after any or all of the tests specified.

Materials used in the CWAP have been selected in accordance with the appropriate flammability requirements of Code of Federal Regulations FAR-25.853a.

7.2.10 Weight

The CWAP weighs 4.67 lbs. Nominal

7.2.11 Cooling Characteristics

The CWAP is designed with passive cooling.

- Operational Power Dissipation: 23.5 W Max
- Operational Power Dissipation: 20.2 W Nominal

7.2.12 Installation Limitations

The CWAP is intended to be installed in the crown of the cabin to provide adequate RF coverage of the Wi-Fi signal. An installation where there is a potential for falling water requires a drip shield. Installations per ARINC 628 part 7 (Stand Alone) shall always have the minimum air gap spacing as follows:

- Bottom (G1) = 0.00"
- Left (G2) = 1.00"
- Right (G3) = 1.00"
- Top (G4) = 1.00"
- Front (G5) = 3.00"
- Rear (G6) = 1.00"

Installations violating the above air gap spacing must be approved by Astronics CSC engineering.

There are no minimum installation distances between CWAPs. The maximum distance shall be determined by aircraft type and configuration and content (e.g. throughput considerations).

Radiation Hazard: Maintain a safe distance when in operation. The device should be installed to provide a minimum distance of 27cm to nearby persons while in operation. Remove power if working within these distances.

7.3 Grounding and Bonding

Electrical grounding and bonding of the CWAP unit follow standard avionics industry design practices, ensuring proper grounding for electrical safety and for Electromagnetic Interference (EMI) control and compliance.

7.4 Workmanship

Workmanship, including ANSI/IPC-A-620 soldering, is designed to meet ANSI/J-STD-002 and RTCA/DO-254.

7.5 Safety

The CWAP is designed to meet the safety requirements of RTCA/DO-254.

7.6 Protective Devices

The CWAP contains a power line fuse that provides electrical separation between the airplane AC power and the CWAP system in the event of a circuit upset per the recommendations of RTCA/DO-254. All input/output signals within the CWAP contains ESD (TVS) protective Diodes and/or isolation transformers that will provide protection from external noise/ESD/lightning. The protection devices have fail-safe features, ensuring that any failure does not create a hazardous condition to the CWAP.

The CWAP has a dual output temperature sensor to protect the internal electronics from an over-temperature or under-temperature condition. Additionally, a separate temperature sensor is in place to enable/disable the unit based on low ambient temperatures (below -20°C).

8 Reliability and Maintainability

8.1 Reliability

The Mean Time Between Failure (MTBF) for the CWAP is a minimum of 270,000 operating hours calculated using the RIAC 217+ (AIC, +30°C, 65% duty cycle, 1428 cycles per year).

8.2 Maintainability

The CWAP is considered an LRU and is repairable only by Astronics CSC or an authorized repair facility. Periodic maintenance of the CWAP is not required.

8.3 Mean Time to Repair (MTTR)

Repair time will not exceed 30 minutes, which entails replacement of the LRU on the aircraft.

8.4 Failure Detection and Fault Isolation

LED indicators located on the system enclosure provide functional status of the CWAP.

8.5 Production Testing

Production units are subjected to Environmental Stress Screening (ESS) and a production Acceptance Test Procedure (ATP) prior to shipment. These tests are intended to ensure that all elements of the product are functional and capable of performing at both high and low temperature extremes and that they are free of manufacturing defects. The Acceptance Test Procedure is run pre- and post-ESS to test the functional characteristics of the product.

9 Support and Service

9.1 Technical Support

For technical support, please contact support@astronics.com.

Contact Address for EU

PGA.sales@astronics.com

Astronics PGA
ZI La Malterie, Avenue Jean Monnet
Montierchaume, 36130 France

9.2 Returning Defective Equipment

All equipment returned to Astronics CSC must have a Return Material Authorization (RMA) number assigned exclusively by Astronics CSC. Astronics CSC cannot be held responsible for any loss or damage caused to the equipment received without an RMA number. The Buyer accepts responsibility for all freight charges for the return of goods to the Astronics CSC designated facility. Astronics CSC will pay return freight charges back to the Buyer's location in the event that the equipment is repaired or replaced within the warranty period stipulated herewith.

Contact and Delivery Address

Astronics CSC
804 S. Northpoint Blvd.
Waukegan, IL 60085
Attn: RMA number

Revision History				
Date	Revision Level	Description of Change	Written By	Approved By
07-26-2022	A	Initial Release per ECO-1471	Mike O'Connor	David Fay
09-08-2022	B	Release per ECO-XXXX Page 2, Add EU compliance statement Add section 2.2 Regulatory Table-8, add BLE and Zigbee details	Chris Hinojosa	David Fay

PRELIMINARY