COMMON CRITERIA CONFIGURATION GUIDANCE

ARUBA OS 8.10 SUPPLEMENTAL GUIDANCE

Target of Evaluation: Aruba Remote Access Points with Mobility Controllers running ArubaOS 8.10-FIPS

Version 2.3

November 2023

6280 AMERICA CENTER DR | SANTA JOSE, CA 95002
info @arubanetworks.com

CONTENTS

1 Introduction

This document serves as a supplement to the official Aruba user guidance (documentation), consolidating configuration information specific to the following Protection Profiles (PPs) or PP Modules:

- collaborative Protection Profile for Network Devices v2.2e
- PP-Module for Virtual Private Network (VPN) Gateways v1.2

This document contains configuration "snippets" from an ArubaOS configuration file. For the sake of simplicity, only command-line interface (CLI) commands are included. When configuring an Aruba controller, a graphical user interface (WebUI) is also available; this document does not include screenshots from the WebUI. Refer to the official ArubaOS User Guide for WebUI instructions, if needed.

https://www.arubanetworks.com/techdocs/ArubaOS-8.x-Books/810/ArubaOS-8.10.0.0-User-Guide.pdf

The ordering of items in this document is based on the ordering of items in the Protection Profiles and Security Target. Configuration guidance in this document is provided so that specific test activities within the PP may be completed.

1.1 Initial Configuration

Evaluation of the TOE deployment in its evaluated configuration is met through conformance to the guidance instructions below. To perform initial configuration of the Mobility Controller and Remote Access Point, the Security Administrator should follow the procedures contained within the Hardware Installation and Set-up Guides referenced in Section 3 of this document. To ensure compliance to the FIPS cryptographic requirements, the Security Administrator should then enable FIPS mode through the console using the command ‘fips enable’ through the CLI.

Only the security functionality and interfaces claimed within the Security Target and highlighted in this document have been evaluated as part of the TOE deployment.

Before use on a network, a Security Administrator should perform the following checks to ensure the TOE is in a secure operational state:

(1) VERIFY FIPS mode has been enabled by outputting the running config (‘show running-config’)

(2) VERIFY the controller is running on the evaluated version (‘show version’)

(3) Verify the FIPS tamper evident labels are applied and have not been tampered with to ensure physical security is maintained. The TOE components are validated under FIPS 140-2 CMVP Level 2.

The evaluated configuration was tested with more than one RAP device. The number of RAP devices in a deployment has no impact on the overall enforcement of the SFR’s since each RAP is configured in the same way as described in this document.

Please note: Version verification of the RAP devices is performed during each connection to the controller automatically. If the firmware of the RAP does not match the firmware of the controller, the controller will push the update to the RAP before re-attempting the connection.

1.2 Evaluated Platforms

The following platforms are covered under the evaluated configuration:

Aruba Mobility Controller Appliances

- 7210
- 7220
- 9004

Aruba Remote Access Points (RAP)

- AP-303H
- AP-503H
- AP-505H

1.3 Version Information

This document covers Aruba Mobility Controllers running ArubaOS 8.10. Customers are advised to use the newest available 8.10 release to take advantage of defect fixes, which may include fixes for security vulnerabilities.

1.4 Aruba Firewall high-level concepts

In an Aruba mobility controller, firewall rules may be applied in multiple ways:

1. To traffic entering a physical port (Ethernet interface) or logical port (VLAN or tunnel) which has been labeled in the configuration as “trusted”. The notion of “trusted” does not mean that the interface necessarily connects to a trusted network. The “trusted” marking in the configuration means that no user-focused processing takes place on traffic entering this interface. That is, the concept of users and user-roles is not applied, and IP addresses learned through this interface will not appear in the user table. This configuration of the mobility controller corresponds to the traditional view of a firewall as a physical device sitting between two networks. The examples used in this configuration guidance will focus on this mode of operation.
2. To traffic entering from an untrusted user. The concept of a “user” can be described as “an IP address learned through an untrusted interface”. Wi-Fi users connecting through Access Points (APs) are automatically untrusted. VPN users connecting to the mobility controller with a VPN client are automatically untrusted. Physical ports and logical ports (VLAN or tunnel) may be configured as “untrusted”, in which case every source IP address learned through that interface will appear in the user table and will have a role/firewall policy assigned to it.
3. To traffic directed to the mobility controller itself (i.e. management traffic). Management traffic may be filtered using the two methods previously described, or it may be filtered through a special “service ACL” configuration which applies universally to all interfaces.

See the ArubaOS User Guide for full details on roles, firewall policies, authentication, and user management.

https://www.arubanetworks.com/techdocs/ArubaOS-8.x-Books/810/ArubaOS-8.10.0.0-User-Guide.pdf

1.5 Acceptance Procedures

Upon delivery of each TOE component, the security administrator should perform the following to ensure all steps necessary have been taken to ensure secure acceptance of the TOE:

1) Ensure that Mobility Controller and RAP has been received in the packaging provided from HPE Aruba Networking.
2) Review the packaging slip/label and ensure that each component delivered is listed within the Security Target.
3) After verification, remove the products from their packaging and place them within a secure storage location to prevent access from unauthorized individuals.
4) Connect power and serial console to the devices and press the power button.
5) Completion the initial set up instructions, configuring the IP address and default admin credentials.
6) Login to the device and enter 'show version'. Verify that the version displayed matches the version claimed within the Security Target (or PCL listing).
    a. Alternatively, the security administrator can review the power on console logs to see the version of the product.
7) Enter 'show inventory' and review the model number listed within the output. Verify the model number provided matches that which is printed on the chassis, packaging, and Security Target.
8) If Steps 1 through 7 have been completed and the hardware and software model are in alignment with the claims made within the Security Target, the acceptance procedures have been successfully completed.
9) After successful acceptance, perform the following steps to place the product in to FIPS mode:
    a. #conf t
    b. #fips enable
10) The device will reboot using the FIPS 140-3 compliant cryptographic settings.

Following completion of the above acceptance procedures, follow the guidance within this document for proper configuration of the various Security Functional Requirements.

If any concerns are identified or additional assistance is required, navigate to https://asp.arubanetworks.com and contact support.

1.6 Preparatory Guidance

Before installing the Aruba Mobility Controller, the operational environment must be set up to ensure that the Aruba MC can be operated consistent with its evaluated configuration.

This includes ensuring that the operational environment can support:

- Remote authentication to the TOE using TACACS+ or RADIUS, and that the AAA servers are properly secured and support the necessary encryption schemes.
- An NTP server is available and that the NTP server can supply the Mobility Controller with time information that is secured via an IPsec-encrypted trusted channel, or by using pre-shared keys.
- A syslog server that provides remote audit storage via IPsec.

- You review the ArubaOS 8.10 User Guide and relevant Installation Guide and understand what default passwords are present and are prepared to change them immediately.
- Administrator workstations are evaluated to ensure that they support the appropriate TLS and SSH cipher suites to administer the ArubaOS Mobility Controller properly and securely.
- An OCSP responder that provides certificate revocation status information to the TOE.

1.7 Writing Memory on CLI

Following configuration of product functionality through the CLI, the security administrator should enter the following command to ensure the configuration takes effect:

(config) #write memory

While this is not mandatory for every configuration step, it will ensure the configuration is stored in the event of a power cycle and for major configuration changes.

2 Configuration

The purpose of this section is to provide the commands and information necessary to configure the device to be compliant with the government approved protection profile. The following Requirement classes are covered within this document:

- Security Audit (FAU)
- Communication (FCO)
- Cryptographic Support (FCS)
- Identification and Authentication (FIA)
- Security Management (FMT)
- Packet Filtering (FPF)
- Protection of the TSF (FPT)
- TOE Access (FTA)
- Trusted Path/Channels (FTP)

2.1 Security Audit (FAU)

2.1.1 FAU_GEN.1

All required audit logs are generated by default. Note that for compliance with FPF_RUL_EXT.1, the "log" keyword must be used on any firewall rules that should be logged. In the event that a TOE network interface is overwhelmed by traffic, the TOE will drop packets and generate an audit event for every packet that is denied and dropped. These statistics are also available through the "show interface" command.

Logging should be configured without the bsd-standard format to ensure that the logs include all required information in the timestamp including year, month, day, hour, minute, and seconds.

```
(config) #logging 192.168.215.253 source-interface 215
(config) #write mem

Saving Configuration...

Configuration Saved.
(config) #
```

Note that the sample audit records in the table below do not contain the year, however, when configured as described above, the audit records will contain the full timestamp. For example:

```
Jan 14 16:17:38 2021 Aruba7220 localdb[3763]: <133112> <3763> <DBUG>
<Aruba7220 192.168.144.200> |db| DELETE FROM cpsec_whitelist WHERE
enable=2 and sequence_num <= 0;
```

Requirement	Auditable Events	Additional Content
NDcPP22e:FAU_GEN.1	None	None
VPNGW12: FAU_GEN.1/VPN	None	None
NDcPP22e:FAU_GEN.2	None	None
NDcPP22e:FAU_GEN_EXT.1	None	None
NDcPP22e:FAU_STG_EXT.1	None	None
NDcPP22e:FAU_STG_EXT.4	None	None
NDcPP22e:FAU_STG_EXT.5	None	None
NDcPP22e:FCO_CPC_EXT.1	Enabling communications between a pair of components. Disabling communications between a pair of components.	Identities of the endpoint pairs enabled or disabled
May 30 16:19:40 2019 Aruba <Aruba 192.168.144.249> profmgr [3638]: USER:admin@192.168.144.4 NODE:"/mm/mynode" COMMAND:<whitelist-db rap add mac-address 20:3c:03:0a:17:e0 ap-group default ap-name AP-303H> -- command executed successfully		

Aug 22 11:26:42 2019 Aruba <Aruba 192.168.144.249> cli[7634] USER:admin@192.168.144.4 NODE:"/mm/mynode" COMMAND:<whitelist-db rap revoke mac-address 20:3c:03:0a:17:e0 revoke-comment "Revocation CC"> - - command executed successfully Aug 22 11:32:10 2019 Aruba <Aruba 192.168.144.249> profmgr[3717]: USER:admin@192.168.144.4 NODE:"/mm/mynode" COMMAND:<whitelist-db rap del mac-address 20:3c:03:0a:17:e0 > -- command executed successfully Aug 14 13:10:00 172.20.57.10 sapd[2076]: <326088> <INFO> |AP AP-203R@172.20.51.10 sapd| |ap| AM: Marking Switch 172.16.11.20 as Down Aug 14 13:10:49 172.20.57.10 sapd[2076]: <326278> <NOTI> |AP AP-203R@172.20.51.10 sapd| |ap| AM: STA 90:e1:7b:0e:e3:32 Authenticated with AP 84:3d:c6:37:4e:71 Aug 14 16:00:42 172.20.57.10 sapd[2076]: <311030> < NOTI > |AP AP-203R@172.20.51.10 sapd| |ap| zone0 Recv ERROR from 172.16.11.20 TunDev non Error RC_ERROR_PEER_DELETE_SA Aug 14 16:00:42 172.20.57.10 sapd[2076]: <311030> < NOTI > |AP AP-203R@172.20.51.10 sapd| |ap| zone0 Dispatch Event TUNNEL_DOWN state UP -> UP		
NDcPP22e:FCS_CKM.1	None	None
VPNGW12:FCS_CKM.1/IKE	None	None
NDcPP22e:FCS_CKM.2	None	None
NDcPP22e:FCS_CKM.4	None	None
NDcPP22e:FCS_COP.1/DataEncryption	None	None
VPNGW12:FCS_COP.1/DataEncryption	None	None
NDcPP22e:FCS_COP.1/Hash	None	None
NDcPP22e:FCS_COP.1/KeyedHash	None	None
NDcPP22e:FCS_COP.1/SigGen	None	None
NDcPP22e:FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Reason for failure.
Jul 28 19:28:24 httpd[5853]: [ssl:error] [pid 5853:tid 870642864] [client 192.168.144.249:53892] AH02039: Certificate Verification: Error (19): self signed certificate in certificate chain, referer: Aug 19 12:56:01 Aruba7030 httpd[6598]: <350008> <6603> <ERRS> <Aruba7030 192.168.144.201> |webserver| SSL Library Error: error:1408C095:SSL routines:SSL3_GET_FINISHED:digest check failed Aug 19 14:10:24 Aruba7220 httpd[7470]: <350008> <7490> <ERRS> <Aruba7220 192.168.144.200> |webserver| SSL Library Error: error:1408A0C1:SSL routines:SSL3_GET_CLIENT_HELLO:no shared cipher Too restrictive SSLCipherSuite or using DSA server certificate? Aug 19 12:55:25 Aruba9004LTE httpd[12094]: <350008> <12104> <ERRS> <Aruba9004LTE 192.168.144.202> |webserver| SSL Library Error: error:1408B010:SSL routines:SSL3_GET_CLIENT_KEY_EXCHANGE:EC lib Aug 19 13:50:03 ArubaVMC-DTech httpd[20783]: <350008> <20797> <ERRS> <ArubaVMC-DTech 192.168.144.204> |webserver| SSL Library Error: error:1408A10B:SSL routines:SSL3_GET_CLIENT_HELLO:wrong version number		
NDcPP22e/VPNGW12:FCS_IPSEC_EXT.1	Failure to establish an IPsec SA.	Reason for failure.

Oct 6 11:30:23 Aruba7030 isakmpd[3520]: <103063> <3520> <DBUG> <Aruba7030 192.168.144.201> 192.168.144.154:4500-> I <-- Notify: NO_PROPOSAL_CHOSEN spi={f2caa917e13078bd 0000000000000000} np=SA Dec 17 08:24:30 Aruba7220 isakmpd[3616]: <103054> <3616> <INFO> <Aruba7220 192.168.144.200> Dropping IKE message drop from 192.168.144.154 500 due to notification type:NO_PROPOSAL_CHOSEN		
NDcPP22e:FCS_NTP_EXT.1	Configuration of a new time server Removal of configured time server	Identity of new/removed time server
Oct 26 12:27:22 Aruba7220 <Aruba7220 192.168.144.200> cli[29443]: USER:admin@172.16.16.100 NODE:"/mm/mynode" COMMAND:<ntp server 192.168.144.100 > -- command executed successfully Oct 26 12:38:02 Aruba7220 <Aruba7220 192.168.144.200> cli[29443]: USER:admin@172.16.16.100 NODE:"/mm/mynode" COMMAND:<no ntp server 192.168.144.100 > -- command executed successfully		
NDcPP22e:FCS_RBG_EXT.1	None	None
NDcPP22e:FCS_SSHS_EXT.1	Failure to establish an SSH session.	Reason for failure.
Oct 11 01:59:46 sshd[7305]: <199801> <7305> <INFO> |sshd| Failed password for admin from 192.168.144.249 port 36920 ssh2		
NDcPP22e:FCS_TLSS_EXT.1	Failure to establish a TLS Session.	Reason for failure.
Feb 25 08:02:01 httpd[5131]: [ssl:warn] [pid 5131:tid 715980496] AH01909: ECC certificate configured for webui.securelogin.arubanetworks.com:443 does NOT include an ID which matches the server name, referer:		
NDcPP22e:FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).
Feb 25 08:08:17 Aruba7220 aaa[3814]: <125061> <3614> <WARN> <Aruba7220 192.168.144.200> User readonly locked out, exceeded authentication threshold, Logged in from 192.168.10.100 port 35460, Connecting to 192.168.144.200 port 4343 connection type HTTPS		
NDcPP22e:FIA_PMG_EXT.1	None	None
VPNGW12:FIA_PSK_EXT.1	None	None
NDcPP22e:FIA_UAU.7	None	None
NDcPP22e:FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
Tested as part of FIA_UIA_EXT.1		
NDcPP22e:FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
Oct 11 00:09:18 sshd[24685]: <199801> <24685> <DBUG> |sshd| debug1: userauth-request for user admin service ssh-connection method password		

Oct 11 00:09:18 sshd[24685]: <199801> <24685> <INFO> |sshd| Accepted password for admin from 192.168.144.249 port 36904 ssh2 Feb 28 02:11:41 authmgr[3950]: <522038> <3950> <NOTI> |authmgr| username=user1 MAC=b8:d7:af:8d:1a:05 IP=0.0.0.0 Authentication result=Authentication Successful method=802.1x server=rad1 Feb 28 02:13:30 authmgr[3950]: <522274> <3950> <ERRS> |authmgr| Mgmt User Authentication failed. username=admin userip=0.0.0.0 servername=rad1 serverip=192.168.144.249 Feb 28 01:37:53 webui[3800]: USER: admin has logged in from 192.168.144.253. Feb 28 01:34:15 cli[29241]: USER: admin has logged in using serial. Feb 28 01:48:27 cli[30967]: USER: admin connected using serial has logged out. Feb 28 01:50:15 cli[32640]: USER: admin has logged in using serial.		
NDcPP22e:FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate. Any addition, replacement or removal of trust anchors in the TOE's trust store	Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store
Oct 26 08:55:55 Aruba7030 isakmpd[3524]: <103063> <3524> <DBUG> <Aruba7030 192.168.144.201> 192.168.144.154:4500-> Notify: 16417ike2_state.c (7683): errorCode = ERR_CERT_EXPIRED Oct 27 09:49:37 Aruba7030 <Aruba7030 192.168.144.201> webui[3408]: USER:admin@192.168.144.153 NODE:"/mm/mynode" COMMAND:<crypto pki-import pem TrustedCA rootca-unacceptable-rsa rootca-unacceptable-rsa.pem ****** > -- command executed successfully Oct 27 09:49:37 Aruba7030 <Aruba7030 192.168.144.201> profmgr[3559]: USER:admin@192.168.144.153 NODE:"/mm/mynode" COMMAND:<crypto-local pki TrustedCA rootca-unacceptable-rsa rootca-unacceptable-rsa.pem > -- command executed successfully		
NDcPP22e/VPNGW10:FIA_X509_EXT.2	None	None
NDcPP22e/VPNGW10:FIA_X509_EXT.3	None	None
NDcPP22e:FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update.	None
Dec 14 16:17:04 Aruba7030 <Aruba7030 192.168.144.201> cli[6558]: USER:admin@serial NODE:"/mm/mynode" COMMAND:<copy tftp: 172.16.16.153 ArubaOS_70xx_8.6.0.7-FIPS_78216 system: partition 0 > -- command executed successfully		
NDcPP22e:FMT_MOF.1/Services	None	None
NDcPP22e:FMT_MTD.1/CoreData	None	None
NDcPP22e:FMT_MTD.1/CryptoKeys	None	None

VPNGW10:FMT_MTD.1/CryptoKeys	None	None
NDcPP22e:FMT_SMF.1	All management activities of TSF data.	None

Ability to administer the TOE locally and remotely
See audit records for NDcPP22e:FIA_UIA_EXT.1 where successful login audits are recorded for each method of administration (both local and remote)

Ability to configure the access banner
Jan 7 13:46:10 cli[8523]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<banner motd | THIS IS THE BANNER |> -- command executed successfully

Ability to configure the session inactivity time before session termination
Jan 7 14:16:20 Aruba7030 <Aruba7030 192.168.144.201> cli[21465]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<loginsession timeout 0> -- command executed successfully

Ability to update the TOE, and to verify the updates using digital signature and [no other] capability prior to installing those updates
Dec 14 16:17:04 Aruba7030 <Aruba7030 192.168.144.201> cli[6558]: USER:admin@serial NODE:"/mm/mynode" COMMAND:<copy tftp: 172.16.16.153 ArubaOS_70xx_8.6.0.7-FIPS_78216 system: partition 0 > -- command executed successfully

Ability to configure the authentication failure parameters for FIA_AFL.1
Jan 7 16:17:05 Aruba7030 <Aruba7030 192.168.144.201> cli[14808]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<aaa password-policy mgmt> -- command executed successfully

Jan 7 16:17:05 Aruba7030 <Aruba7030 192.168.144.201> cli[14808]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<enable> -- command executed successfully

Jan 7 16:17:05 Aruba7030 <Aruba7030 192.168.144.201> cli[14808]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<password-lock-out 3> -- command executed successfully

Jan 7 16:17:05 Aruba7030 <Aruba7030 192.168.144.201> cli[14808]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<password-lock-out-time 1> -- command executed successfully

Ability to start and stop services
Dec 15 15:13:49 Aruba7030 <Aruba7030 192.168.144.201> profmgr[3582]: USER:admin@172.16.16.153 NODE:"/mm/mynode" COMMAND:<no logging 1.1.1.1> -- command executed successfully

Nov 13 09:22:56 Aruba7030 <Aruba7030 192.168.144.201> cli[24718]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<logging 172.16.16.154 format bsd-standard severity debugging > -- command executed successfully

Ability to manage the cryptographic keys
Jan 8 09:57:06 Aruba7030 profmgr[3568]: <334000> <3568> <DBUG> <Aruba7030 192.168.144.201> profmgr_np_config_commit_working_entry: new objtype_buffer added , CMD: crypto-local pki TrustedCA ROOT_TEST rootca-rsa.pem

Ability to configure the cryptographic functionality
Jan 8 09:14:15 Aruba7030 <Aruba7030 192.168.144.201> cli[20633]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<crypto isakmp policy 111> -- command executed successfully

Jan 8 09:14:27 Aruba7030 <Aruba7030 192.168.144.201> cli[20633]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<authentication pre-share> -- command executed successfully

Jan 8 09:15:14 Aruba7030 <Aruba7030 192.168.144.201> cli[20633]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<encryption aes128> -- command executed successfully

Jan 8 09:15:27 Aruba7030 <Aruba7030 192.168.144.201> cli[20633]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<hash sha> -- command executed successfully

Jan 8 09:15:42 Aruba7030 <Aruba7030 192.168.144.201> cli[20633]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<group 20> -- command executed successfully

Ability to configure the lifetime for IPsec SAs
Jan 7 15:37:33 Aruba7030 <Aruba7030 192.168.144.201> cli[6821]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<crypto-local ipsec-map gss 111> -- command executed successfully

Jan 7 15:37:33 Aruba7030 <Aruba7030 192.168.144.201> cli[6821]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<set security-association lifetime seconds 86400> -- command executed successfully

Jan 7 15:37:33 Aruba7030 <Aruba7030 192.168.144.201> cli[6821]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<crypto isakmp policy 111 > -- command executed successfully

Jan 7 15:37:33 Aruba7030 <Aruba7030 192.168.144.201> cli[6821]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<lifetime 86400> -- command executed successfully

Ability to import X.509v3 certificates to the TOE's trust store
Oct 27 09:49:37 Aruba7030 <Aruba7030 192.168.144.201> webui[3408]: USER:admin@192.168.144.153 NODE:"/mm/mynode" COMMAND:<crypto pki-import pem TrustedCA rootca-unacceptable-rsa rootca-unacceptable-rsa.pem ****** > -- command executed successfully

Oct 27 09:49:37 Aruba7030 <Aruba7030 192.168.144.201> profmgr[3559]: USER:admin@192.168.144.153 NODE:"/mm/mynode" COMMAND:<crypto-local pki TrustedCA rootca-unacceptable-rsa rootca-unacceptable-rsa.pem > -- command executed successfully

Ability to manage the TOE's trust store and designate X509 v3 certificates as trust anchors
See audit records for 'Ability to import X.509v3 certificates to the TOE's trust store'.

Note: The designation of a trust anchor will occur when the certificate type of "*TrustedCA*" is selected at the time of import. All other certificate type selections do not result in the certificate being designated as a trust anchor.

Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1

Jan 9 14:34:30 Aruba7030 <Aruba7030 192.168.144.201> profmgr[3568]: USER:admin@172.16.16.153 NODE:"/mm/mynode" COMMAND:<banner motd ~ THIS IS THE BANNER! ~> -- command executed successfully

Ability to set the time which is used for time-stamps
Aug 26 10:28:58 Aruba7030 <Aruba7030 192.168.144.201> cli[18263]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<clock set 2020 august 26 10 28 58 > -- command executed successfully
Ability to configure NTP
Jan 20 20:00:46 Aruba7030 <Aruba7030 192.168.144.201> cli[6558]: USER:admin@serial NODE:"/mm/mynode" COMMAND:<ntp server 1.1.1.1 > -- command executed successfully

Ability to configure the reference identifier for the peer
Jan 8 09:13:02 Aruba7030 <Aruba7030 192.168.144.201> cli[20147]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<peer-cert-dn testing> -- command executed successfully

Ability to configure the interaction between TOE components
See FCO_CPC_EXT.1

Ability to manage the trusted public keys database
Jan 8 09:17:12 Aruba7030<Aruba7030 192.168.144.201> profmgr[3695]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<mgmt-user ssh-pubkey client-cert ssh-super super-cli root node / > -- command executed successfully

VPNGW12:FMT_SMF.1/VPN	All administrative actions	No additional information.

Definition of packet filtering rules
Mar 10 14:02:31 2023 Aruba7210_01 <Aruba7210_01 10.128.8.10> cli[11102]: USER:admin@10.50.10.13 NODE:"/mm/mynode" COMMAND:<ip access-list session DEMO > -- command executed successfully

Mar 10 14:02:31 2023 Aruba7210_01 <Aruba7210_01 10.128.8.10> cli[11102]: USER:admin@10.50.10.13 NODE:"/mm/mynode" COMMAND:<host 192.168.4.2 host 192.168.3.2 1 permit log > -- command executed successfully

Association of packet filtering rules to network interfaces

Mar 10 14:07:37 2023 Aruba7210_01 <Aruba7210_01 10.128.8.10> cli[26230]: USER:admin@10.50.10.13 NODE:"/mm/mynode" COMMAND:<interface gigabitethernet 0/0/2 > -- command executed successfully

Mar 10 14:08:03 2023 Aruba7210_01 <Aruba7210_01 10.128.8.10> cli[26230]: USER:admin@10.50.10.13 NODE:"/mm/mynode" COMMAND:<ip access-group session DEMO > -- command executed successfully

Ordering of packet filtering rules by priority

There is no way to administratively reorder rules except by deleting them and readding them. Therefore, audit messages associated with this management function are equivalent to those in 'Definition of packet filtering rules'.		
NDcPP22e:FMT_SMR.2	None	None
VPNGW12:FPF_RUL_EXT.1	Application of rules configured with the 'log' operation	Source and destination addresses Source and destination ports Transport Layer Protocol
ACL logs: Feb 20 17:42:53 authmgr[3957]: <124006> <3957> <WARN> |authmgr| {944} UDP srcip=2001:192:168:144::254 srcport=32000 dstip=2001:172:16:8::15 dstport=21, action=permit, policy=ffw_1_5 Feb 20 17:43:03 authmgr[3957]: <124006> <3957> <WARN> |authmgr| {4562} UDP srcip=192.168.144.6 srcport=32000 dstip=172.16.8.15 dstport=21, action=deny, policy=ffw_1_5 Feb 20 21:08:08 authmgr[3957]: <124006> <3957> <WARN> |authmgr| {5693} ICMP srcip=192.168.144.2 dstip=192.168.144.251, type=8, code=0, sequence=256, id=40206, action=deny, policy=ffw_1_5 Feb 20 17:34:43 authmgr[3957]: <124006> <3957> <WARN> |authmgr| {914} ICMPv6 srcip=2001:192:168:144::254 dstip=fe80::b:8600:1b4:b347, type=136, code=0, action=permit, policy=ffw_1_5		
NDcPP22e:FPT_APW_EXT.1	None	None
NDcPP22e:FPT_ITT.1 **NDcPP22e:FPT_ITT.1/Join**	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel.	Identification of the initiator and target of failed trusted channels establishment attempt.
See FTP_ITC.1 for examples		
VPNGW12:FPT_FLS.1/SelfTest	None	None
NDcPP22e:FPT_SKP_EXT.1	None	None
NDcPP22e:FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged.	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).

	See also application note on FPT_STM_EXT.1)	
Aug 26 10:28:58 Aruba7030 <Aruba7030 192.168.144.201> ctrlmgmt: USER:admin: clock changed from Wed Aug 26 10:29:02 EDT 2020 to Wed Aug 26 10:28:58 EDT 2020 Aug 26 10:28:58 Aruba7030 <Aruba7030 192.168.144.201> cli[18263]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<clock set 2020 august 26 10 28 58 > -- command executed successfully		
NDcPP22e:FPT_TST_EXT.1	None	None
VPNGW12:FPT_TST_EXT.3	None	None
NDcPP22e:FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure).	None
Dec 11 16:39:02 Aruba7030 <Aruba7030 192.168.144.201> cli[31503]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<copy tftp: 172.16.16.153 ArubaOS_70xx_8.6.1.0-FIPS.fcs86x_fips_no_sig system: partition 1 > -- command executed successfully		
VPNGW12:FPT_TUD_EXT.1	None	None
NDcPP22e:FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None
Feb 27 10:52:23 webui[3800]: USER: admin connected from 192.168.144.3 has timed out. Sep 8 10:52:44 Aruba7030 <Aruba7030 192.168.144.201> cli[14459]: USER: admin connected from 172.16.16.154 has logged out. Reason: Idle timeout		
NDcPP22e:FTA_SSL.4	The termination of an interactive session.	None
Feb 28 02:26:52 webui[3800]: USER: admin connected from 192.168.144.253 has logged out. Feb 28 02:57:47 sshd[15323]: <199801> <15323> <INFO> |sshd| Close session: user admin from 192.168.144.253 port 51968 id 0 Sep 8 11:30:05 Aruba7030 sshd[10027]: <199801> <10027> <INFO> <Aruba7030 192.168.144.201> Received disconnect from 172.16.16.154 port 40676:11: disconnected by user		
NDcPP22e:FTA_SSL_EXT.1	(if 'lock the session' is selected) Any attempts at unlocking of an interactive session. (if 'terminate the session' is selected)	None

	The termination of a local session by the session locking mechanism.	
Sep 8 11:33:34 Aruba7030 <Aruba7030 192.168.144.201> cli[10822]: USER: admin connected using serial has logged out. Reason: Idle timeout		
NDcPP22e:FTA_TAB.1	None	None
NDcPP22e:FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions. Failed attempts to establish a trusted channel (including IEEE 802.11). Detection of modification of channel data	Identification of the initiator and target of failed trusted channels establishment attempt. Identification of the initiator and target of channel.
Initiation: Oct 11 01:52:12 isakmpd[3922]: <103076> <3922> <DBUG> |ike| IKEv2 IPSEC Tunnel created for peer 192.168.144.243:50750 Oct 14 14:20:17 Aruba7030 isakmpd[3519]: <103077> <3519> <INFO> <Aruba7030 192.168.144.201> IKEv2 IKE_SA succeeded for peer 192.168.144.154:4500 Termination: Feb 27 14:46:53 isakmpd[3949]: <103102> <3949> <INFO> |ike| IKE SA deleted for peer 192.168.145.249 Failure: Oct 11 01:36:37 isakmpd[3922]: <103060> <3922> <DBUG> |ike| 192.168.144.243:50750-> ike_phase_1.c:attribute_unacceptable:2850 Proposal match failed in auth algo, configured=RSA_SIG, peer using=unknown Nov 16 12:00:39 Aruba7030 dot1x-proc: 2[4207]: <138086> <4207> <INFO> <Aruba7030 192.168.144.201> WPA 2 Key exchange failed to complete, de-authenticating the station 74:9e:f5:ff:a5:e9 associated with AP b4:5d:50:6f:7b:90 ap225		
VPNGW12:FTP_ITC.1/VPN	Termination of the trusted channel Failure of the trusted channel functions	Identification of the initiator and target of failed trusted channel establishment attempt

See NDcPP22e:FTP_ITC.1 above.		
NDcPP22e:FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	None

Initiation:

Oct 15 09:17:20 Aruba7030 sshd[4976]: <199801> <4976> <INFO> <Aruba7030 192.168.144.201> Connection from 192.168.144.154 port 44596 on 192.168.144.201 port 22

Jul 28 11 01:59:46 sshd[7305]: <125032> <7305> <info> |sshd| Authentication Succeeded for User admin, Logged in from 192.167.144.253 port 22, Connecting to 192.168.144.5 port 22 connection type SSH

Oct 26 12:16:28 Aruba7030 <Aruba7030 192.168.144.201> webui[3408]: TLS connection with client 192.168.144.153 is established.

Feb 28 01:37:53 webui[3800]: USER: admin has logged in from 192.168.144.253.

Termination:

2022-08-31T10:20:42-04:00 2022 Aruba7030 <Aruba7030 172.17.17.201> webui[3451]: TLS session with client 172.16.16.248 is terminated due to idle session time out.

Oct 14 13:41:04 Aruba7030 <Aruba7030 192.168.144.201> webui[3403]: TLS connection with client 192.168.144.153 is terminated.

Feb 27 10:52:23 webui[3800]: USER: admin connected from 192.168.144.3 has timed out.

Oct 15 12:11:08 Aruba7030 sshd[6100]: <199801> <6100> <INFO> <Aruba7030 192.168.144.201> Received disconnect from 192.168.144.154 port 44802:11: disconnected by user

Oct 15 12:11:08 Aruba7030 sshd[6100]: <199801> <6100> <INFO> <Aruba7030 192.168.144.201> Disconnected from user admin 192.168.144.154 port 44802

Feb 28 02:57:47 sshd[15323]: <199801> <15323> <INFO> |sshd| Close session: user admin from 192.168.144.253 port 51968 id 0

Failure:

Jul 28 19:28:24 httpd[5853]: [ssl:error] [pid 5853:tid 870642864] [client 192.168.144.249:53892] AH02039: Certificate Verification: Error (19): self signed certificate in certificate chain, referer:

Oct 8 10:07:05 Aruba7030 sshd[22714]: <199801> <22714> <INFO> <Aruba7030 192.168.144.201> Failed password for admin from 192.168.144.154 port 33902 ssh2

All Administrative actions are audited by the TOE. As noted within the Syslog Guide for 8.X (https://www.arubanetworks.com/techdocs/ArubaOS-8.x-Books/810/ArubaOS-8.10.0.0-Syslog-Reference-Guide.xlsx), the controller creates syslog entries for all commands and configuration changes that alter system behavior, the user name of the user making the change, and the location of the user. This information appears in the output of the syslog, with the keyword COMMAND. This same information also appears in the output of the CLI command **show audit-trail**.

The syslog information in the example below shows that a user with the username **admin** logged in to the controller through the serial port, changed logging levels, loaded new software onto partition 1, then updated the system clock.

Oct 2 18:50:00 cli[19855]: USER:admin@serial NODE:"/mm/mynode" COMMAND:<clock set 2018 october 2 18 50 00> -- command executed successfully

Sep 1 01:26:34 nanny[5174]: <399814> <5174> <DBUG> |nanny| PROCESS_RUNNING Process ntpwrap marked as PROCESS_RUNNING Timeout value : 240 Time updated: 56 sec

Oct 2 20:55:43 nanny[5174]: <399814> <5174> <DBUG> |nanny| PROCESS_RUNNING Process ntpwrap marked PROCESS_NOT_RESPONDING Timeout value : 240 Time since not updated : 2748544 sec

By default, the controller does not generate a log entry for **show** commands issued using the CLI, as these commands display existing settings but do not change system behavior. To create a log entry for all commands issued, (including show commands) access the CLI in config mode and issue the command **audit-trail all**.

2.1.2 FAU_GEN_EXT.1

The Remote AP maintains locally stored audit records which are sent to the Controller during regular operation. This traffic is sent through the secure channel established between the Controller and AP and is established during the provisioning process without Security Administrator interaction.

2.1.3 FAU_GEN.2

No configuration required.

2.1.4 FAU_STG_EXT.1

Local storage space for audit logs is limited on a mobility controller. The local protected log storage operates using the first in, first out (FIFO) method, therefore audit logs are overwritten when the available space is exhausted. To operate in the evaluated configuration, an external syslog server must be used. All audit logs are simultaneously written to both the local audit log and the syslog server. The local audit logs and logs sent to a remote server are identical. No configuration is required for the RAP to implement the secure connection for automatic

transmission of audit records to the Mobility Controller. This is configured without user interaction during initial enrollment/provisioning of the RAP.

To configure an external syslog server:

```
(config)# logging <ip address>
```

The connection between the mobility controller and the syslog server must be protected using IPsec. Configure a site-to-site VPN tunnel to carry this traffic. The syslog server must use a different IP address for the syslog receiver process than it uses for IPsec termination. Alternatively, a VPN gateway (such as an Aruba mobility controller) may front-end the syslog server to provide the IPsec tunnel. The following is an example of an IPsec tunnel which assumes that the syslog receiver process listens on 192.168.1.1, and the IPsec tunnel terminates on 192.168.2.1 – these IP addresses may be on the same server, or on different systems.

```
crypto-local ipsec-map <name> 10
  version v2
  set ikev2-policy <policy>
  peer-ip <ip address>
  src-net <ip address> <subnet>
  dst-net <ip address> <subnet>
  set transform-set "<transform-set>"
  set security-association lifetime seconds <seconds>
  set security-association lifetime kilobytes <kilobytes>
  pre-connect enable
  trusted enable
  uplink-failover disable
  force-natt disable
  set ca-certificate root-ca
  set server-certificate server-cert
```

Adjust the above ipsec-map as appropriate, following instructions in the ArubaOS User Guide. The peer-ip and dst-net addresses cannot be the same. Note that bi-directional communication is not necessary – syslog is sent using UDP, so the only requirement is that packets are able to flow from the mobility controller to the syslog server.

2.2 Cryptographic Support (FCS)

2.2.1 FCS_CKM.1 & FCS_CKM.2

No configuration required. Ensure the controller has FIPS mode enabled so that cryptographic requirements are met.

(config)# fips enable

During regular operation of the TOE, key generation is invoked during session establishment between the TOE and external IT entities for user sessions. An administrator can invoke the use of RSA and ECDSA during generation of certificates used for X.509.

No configuration is required to permit only the allowed algorithms as defined within the Security Target once FIPS mode has been enabled. For IPsec, TLS, and SSH the TOE supports cryptographic key generation for RSA schemes using key sizes of 2048 bits, ECC schemes using NIST curves P-256, P-384. These Key generation schemes are supported by both the RAP and MC for IPsec connections. The RAP and MC act as sender and receiver for these connections. The key generation schemes are also supported by the MC as a TLS Receiver and FFC Schemes using Diffie-Hellman group 14 key sizes of 2048-bit is supported for IPsec as sender and receiver by both the RAP and MC.

All key generation is performed using the TOE's DRBG as input.

2.2.2 FCS_CKM.4

No configuration required. During runtime, all CSPs will be zeroized automatically when no longer needed. To erase all CSPs stored in flash memory (as well as software images and configuration files), issue the command 'zeroize-tpm-keys' (for hardware) and 'wipe out flash' (for virtual). This command will overwrite the entire flash with an alternating pattern. The controller must be restored through TFTP after this process. In addition, files in the flash can be zeroized using the 'write erase all' command. There are no configurations or circumstances that do not strictly conform to the key destruction requirement.

For further details on sanitizing systems, request the document "Identification of Non-Volatile Storage and Sanitization of System Components" from HPE Aruba Networking.

2.2.3 FCS_COP.1

Ensure that the Advanced Cryptography License is installed in order for all required cryptographic algorithms to be enabled. Ensure the controller has FIPS mode enabled so that cryptographic requirements are met.

(config)# fips enable

2.2.4 FCS_HTTPS_EXT.1

No configuration is required. The TOE will function over HTTPS, compliant to RFC 2818, when operating in FIPS mode.

2.2.5 FCS_NTP_EXT.1

Configuration of the NTP is performed on the Mobility Controller. Time synchronization with the RAP is provided by the Controller. This configuration can be performing with the following commands:

```
ntp

authenticate
```

```
authentication-key <keyid> sha1 <keyvalue>
server {<ip>|<ip6>} {[iburst|key] <keyid>}
trusted-key
```

The TOE supports the usage of NTPv4. If multiple NTP servers need to be configured, the above commands can be re-entered or the Security Administrator can navigate to the WebUI Configuration > System > General > Clock page. Click the '+' under NTP servers and fill in the information to set additional time sources.

To tunnel NTP through IPsec, the Security Administrator should specify the interface used to communicate with the NTP server. This can be done under NTP settings by specifying the IP address of an NTP server that is allowed within the scope of a configured IPsec policy. Ensure an IPsec policy has been applied to the VLAN with proper routing. When generating the authentication-key, SHA-1 must be used in the evaluated configuration. The TOE by default does not accept broadcast or multicast NTP packets.

2.2.6 FCS_IPSEC_EXT.1

2.2.6.1 FCS_IPSEC_EXT.1.1/2

RFC 4301 references an explicit Security Policy Database (SPD) with rules for DISCARD, BYPASS, and PROTECT. ArubaOS does not implement an explicit SPD, but equivalent behavior may be obtained using firewall policies and "routing" ACLs. RAP devices do not support the ability to configure an SPD and all traffic transits the IPsec tunnel.

The access-list in the following configuration defines the behavior with rules for PROTECT BYPASS and DISCARD. Note that the traffic that is to be protected is defined in an ipsec-map. The ipsec-map defines traffic that will be encrypted in an IPsec connection. The access-list determines whether traffic will be permitted or denied. If traffic is permitted, it is then processed to see if the traffic is encrypted in IPsec. If the traffic matches the rules defined in the ipsec-map, then the traffic will be encrypted. Otherwise, it will bypass the tunnel and proceed in plaintext.

```
ip access-list session spd-test
     host 192.168.144.153 any icmp echo permit log
     host 192.168.144.153 any tcp 22 deny log
     network 1.1.1.0 255.255.255.0 any any permit log
     any network 1.1.1.0 255.255.255.0 any permit log
     host 192.168.144.154 any any permit log
     any host 192.168.144.154 any permit log
     any any any deny log
```

The 1st rule is a BYPASS rule using the ICMP echo-request which allows plaintext traffic from 192.168.144.153. The 2nd rule is a DISCARD (deny) rule to discard SSH traffic from

192.168.144.153. The 3rd, 4th, 5th and 6th rules are PROTECT (permit) rules to allow encrypted traffic to flow through the IPsec tunnel. The final rule is a default deny rule.

These rules can be modified as needed for explicit control over tunneled and non-tunneled traffic. Note: Most deployments will not make use of this feature, as ALL traffic to a specific destination will typically be tunneled. The sample config file at the end of this document does NOT contain examples from this section.

The configuration above provides SPD control for inbound wired traffic. For wireless or VPN client users (not tested as part of the Common Criteria evaluation), multiple ACLs may be sequenced with a user-role container, simplifying this configuration.)

The access control lists used by the TOE are read in hierarchical order. When traffic enters or exits the TOE, the first applicable rule in the ACL is applied. Any rule below the initially triggered rule is not applied. Note that if an access rule is applied, a duplicate cannot be entered. If the administrator applied a permit rule and then enters a deny rule with the same parameters, the deny rule will replace the permit rule and vice versa.

2.2.6.2 FCS_IPSEC_EXT.1.3

The TOE supports IPsec in tunnel mode. The following configuration shows an example of a site-to-site IPsec VPN tunnel:

```
crypto-local ipsec-map 10.10.20.1 100
  version v2
  set ikev2-policy 10009
  peer-ip 192.168.2.1
  vlan 2
  src-net 172.16.1.0 255.255.255.0
  dst-net 10.10.20.0 255.255.255.0
  set transform-set "default-gcm256"
  set pfs group20
  set security-association lifetime seconds 420
  set security-association lifetime kilobytes 30000
  pre-connect enable
  trusted enable
  uplink-failover disable
  force-natt disable
  set ca-certificate root-ca
  set server-certificate server-cert
```

Running the following command will show that both transport and tunnel mode can be used in negotiation, however only tunnel mode is allowed in the evaluated configuration:

```
show crypto ipsec transform-set

Transform set default-transform: { esp-aes128 esp-sha-hmac }
    will negotiate = { Transport, Tunnel }
```

Additionally, the following command can be used under the crypto-local ipsec-map to force tunnel mode to be the only option offered. However, it is not necessary with the above configuration since it is used by default.

```
  force-tunnel-mode
```

With this command present, the crypto map would show the following:

```
Transform set transform-tunnel: { esp-aes128 esp-sha-hmac }
    will negotiate = { Tunnel }
```

2.2.6.3 FCS_IPSEC_EXT.1.4

IPsec cipher suites are configured on the Mobility Controller using transform-sets. These are ordered lists of ciphers - the controller will attempt each one in order until one is successfully negotiated with the peer. The command "show crypto ipsec transform-set" will display the configured transform sets. Algorithms are not configurable on RAP devices.

ArubaOS provides pre-configured transforms that meet three of the Common Criteria requirements. Note that the Advanced Cryptography License must be installed in order to have access to AES-GCM. The default transforms are:

```
Transform set default-gcm256: { esp-aes256-gcm  }

Transform set default-gcm128: { esp-aes128-gcm  }

Transform set default-aes: { esp-aes256 esp-sha-hmac }
```

ESP algorithms are contingent on the certificate in use for RAP devices. For RSA, AES-CBC-128/256 is used. For ECDSA, AES-GCM-128/256 is used with NIST P-256 and AES-GCM-256 is used with NIST P-384.

Note: The TOE's IPsec ESP protocol implementation supports only HMAC-SHA-1. The IKE protocol supports truncated versions of HMAC-SHA-1, HMAC-SHA-256 and HMAC-SHA-384.

To configure AES-CBC-128, add a new transform set:

```
(config) #crypto ipsec transform-set aes128 esp-aes128 esp-sha-hmac
```

The transform sets above are referenced directly by name when creating a site-site IPsec tunnel, as shown in FCS_IPSEC_EXT.1.2. For RAP devices (non site-to-site), dynamic-maps are used to order the list of transform sets. The command "show crypto dynamic-map" will list these. The number assigned to the dynamic-map indicates the priority - a lower number will be matched before a higher number. To create a single dynamic-map which incorporates all required transform sets for evaluation, configure the following:

```
(config) #crypto dynamic-map cc-required 1
(config-dynamic-map)#  set transform-set default-gcm256 default-gcm128
default-aes aes128
```

The resulting dynamic-map:

```
Crypto Map Template"cc-required" 1
         IKE Version: 2
         IKEv2 Policy: DEFAULT
         Security association lifetime seconds : [300 -86400]
         Security association lifetime kilobytes: N/A
         PFS (Y/N): Y (Use the 384-bit Diffie Hellman elliptic curve
group
         Transform sets={ default-gcm256, default-gcm128, default-aes,
aes128 }
```

This dynamic-map will be revisited in future sections. Note that SA lifetimes have not yet been set in this example; this will be done further in this document.

PFS has been enabled in this example. Although the VPNGW PP-Module does not mandate the use of Perfect Forward Secrecy, it is a security best-practice. To enable PFS:

```
(config-dynamic-map)#  set pfs group20
```

2.2.6.4 FCS_IPSEC_EXT.1.5

Only IKEv2 is supported by the TOE. NAT-T (NAT Traversal) is supported by Mobility Controllers and RAP to transport packets over UDP port 4500 rather than using IPsec native encapsulation.

For inbound connections where the controller is the IKE responder, NAT-T is supported by default. To disable, install a firewall rule that blocks UDP 4500.

For outbound connections in a site-to-site VPN tunnel, NAT-T is configured in the ipsec-map described in FCS_IPSEC_EXT.1.2. To force NAT-T rather than allowing it to be negotiated, issue the following command:

```
(config) #crypto-local ipsec-map 10.10.20.1 100
(config-ipsec-map)#  force-natt enable
```

To specify the IKEv2 policy:

```
(config) #crypto isakmp policy <priority>
(config-isakmp) #version v2
```

2.2.6.5 FCS_IPSEC_EXT.1.6

IKE policies are matched in numerical order, with lower numbers having higher priority. A number of IKE policies are pre-configured - to view these, issue the command "show crypto isakmp policy".

Default policies may not be deleted, but may be disabled. To disable a policy:

```
(config) #crypto isakmp policy <policy>
(config-isakmp)# disable
```

It is recommended that when deployed as a VPN gateway, **all** default IKE policies be disabled, and only user-defined policies configured for use.

To configure an IKEv2 policy that uses AES-256, issue the following commands:

```
(config) # crypto isakmp policy 100
(config-isakmp)# encryption aes256
(config-isakmp)# hash sha
(config-isakmp)# version v2
```

To configure AES128, adjust the encryption to ‘encryption aes128’. To configure HMAC-SHA-256, adjust the hash to ‘sha2-256-128’.

2.2.6.6 FCS_IPSEC_EXT.1.7/8

For IKEv2 SA, lifetimes are configured in the IKE policies in seconds (300-86400 seconds). Thus, the lifetime can be set within 1-24 hours. To adjust a previously-created IKE policy for a 24-hour lifetime (this is the default value), issue the following commands:

```
(config) # crypto isakmp policy 100
(config-isakmp)# lifetime 86400
```

For IKEv2 Child SA, lifetimes are configured in the ipsec-map (for site-to-site). The lifetime for the security association (SA) is configured in seconds (300-86400 seconds). Thus, the lifetime can be set within 1-8 hours. Child SA lifetimes may also be configured based on the number of bytes transmitted.

The lifetime is configured using the following commands:

```
(config) #crypto-local ipsec-map 10.10.20.1 100
(config-ipsec-map)# set security-association lifetime seconds 28800
(config-ipsec-map)# set security-association lifetime kilobytes <value>
```

or the dynamic-map (for RAP devices):

```
(config) #crypto dynamic-map cc-required 1
```

```
(config-dynamic-map)#  set security-association lifetime seconds 28800
```

Note: volume-based limits are not supported for dynamic maps.

RAP devices will always initiate a rekey at 7200 seconds for CHILD_SA and 28800 seconds for IKE_SA. This behavior occurs even when the Mobility Controller sets a higher rekey limit for RAP connections. If the Mobility Controller sets a limit lower than these thresholds, then the controller will initiate a rekey.

2.2.6.7 FCS_IPSEC_EXT.1.9/10

No configuration required to meet these requirements.

2.2.6.8 FCS_IPSEC_EXT.1.11

Aruba Mobility Controllers support DH groups 14, 19, and 20. To configure, modify the IKE policy:

```
(config) # crypto isakmp policy 100
(config-isakmp)# group 20
```

For RAP devices, DH groups used are dependent on the certificate in use. For RSA certificates, Group 14 is used. For ECDSA NIST P-256 certificates Group 19 is used, and for ECDSA NIST P-384 certificates Group 20 is used.

2.2.6.9 FCS_IPSEC_EXT.1.13

ArubaOS supports both RSA and ECDSA certificates. Note that the Advanced Cryptography License must be installed to make use of ECDSA.

Loading of certificates onto the controller for both authentication to peers and for verification of other peers can be done by navigating to ‘Configuration > System > Certificates’ on the controller.

Additional information on importing certificates is described in the “Managing Certificates” section of the ArubaOS User Guide. Minimally, both a "server certificate" and a "trusted root CA" certificate must be loaded onto the controller in order to perform IPsec operations. Once these certificates are loaded on the controller, configure them for use in IPsec with VPN peers:

For RAP devices, the Controller identity certificate and RAP device trust anchor can be set by executing the following:

```
(config) #crypto-local isakmp server-certificate "server-cert"
(config) #crypto-local isakmp ca-certificate "trusted-root-ca-cert"
```

For a site-to-site VPN tunnel:

```
(config) #crypto-local ipsec-map 10.10.20.1 100
(config-ipsec-map)#  set server-certificate server-cert
(config-ipsec-map)#  set ca-certificate root-ca
```

To configure an IKE policy to authenticate RSA certificates sent by peers, use the following command:

```
(config) #crypto isakmp policy 100
(config-isakmp)# authentication rsa-sig
```

To configure an IKE policy for ECDSA-384 authentication, use the following command:

```
(config) #crypto isakmp policy 100
(config-isakmp)# authentication ecdsa-384
```

ECDSA-256 may be supported by replacing "384" with "256".

Administrators should take care to configure IKE/IPsec policies so that the strength of the IKE association is greater than or equal to the strength of the IPsec tunnel (for example, by always using AES-256). However, if a misconfiguration is made, the controller will reject the security association along with generating an audit log message.

2.2.6.10 FCS_IPSEC_EXT.1.14

The TOE does not support SAN extension. For VPN gateway functionality, Mobility Controllers only support DN. For connections between RAP devices and Mobility Controllers, only IP addresses in the CN field are supported.

To configure the TOE reference identifier for the distinguished name of the peer for VPN gateway functionality, an administrator may use the following commands on the controller:

```
(config) #crypto-local ipsec-map testmap 1
(config-submode)#peer-cert-dn
     <peer-dn>       Subject-Name DN string of the Peer's Certificate
```

For the channel between the Mobility Controller and RAP device, the expected IP of the controller must be set on the RAP device to restrict the RAP device to connecting to expected/known controllers only. This can be achieved by using the "*provision-ap*" command with the "*cert-DN <ip_address>"* parameter.

For the VPN gateway channel, to ensure appropriate compliance within the evaluated configuration, the administrator should generate a CA chain with one Root CA and two Intermediate CAs. The channel between a Mobility Controller and RAP only requires a CA chain containing one Root and one Leaf.

2.2.7 FCS_RBG_EXT.1

No configuration required.

2.2.8 FCS_SSHS_EXT.1

SSH access requires that you configure an IP address and a default gateway. No configuration is needed to specify the permitted algorithms after 'fips enable' has been set. The controller will attempt negotiations using AES128-CBC, AES256-CBC, AES128-CTR, and AES256-CTR encryption algorithms in conjunction with HMAC-SHA1, HMAC-SHA1-96, and HMAC-SHA2-256 MAC algorithms. The controller will also negotiate SSH-RSA, RSA-SHA2-256, and RSA-SHA2-512 public-key algorithms and the following key exchange methods: ecdh-sha2-nistp256, ecdh-sha2-nistp384.

To view configuration for SSH, the following command can be used:

```
show ssh
```

To configure the SSH server, the following commands can be used:

```
ssh disable_dsa
```

```
ssh disable-kex dh
```

```
ssh mgmt-auth {public-key [username/password]|username/password [public-key]}
```

To configure authentication for SSH using public key (SSH-RSA), the following commands can be used:

```
ssh mgmt-auth public-key
```

```
mgmt-user ssh-pubkey client-cert ssh-pubkey cli-admin root
```

SSH rekey intervals are non-configurable and are set to a maximum time interval of one (1) hour or 512M, whichever occurs first.

2.2.9 FCS_TLSS_EXT.1

No configuration is required to set the permitted cipher suites or the associated key agreement parameters once 'fips enable' has been entered on the controller. The TOE performs key establishment with DH parameters over NIST curve secp256r1. The controller negotiates using TLSv1.2 and the following ciphersuites:

- RSA:
    - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
    - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
    - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
    - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- ECDSA:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

To view configuration for TLS, the following command can be used:

```
show web-server profile
show web-server statistics
```

The following commands can be used to configure the TLS web-server profile:

```
web-server profile
absolute-session-timeout <30-3600>
mgmt-auth username/password
session-timeout <30-3600>
ssl-protocol tlsv1.2
web-max-clients <25-320>
web-https-port-443
switch-cert <name>
```

2.3 Communication (FCO)

2.3.1 FCO_CPC_EXT.1

To configure and register a Remote Access Point with a Controller, the following steps need to be followed:

1) Bring the Controller online in Standalone mode
2) Install the licenses on the Mobility Controller and ensure ‘Feature Enabled’ checkboxes are ticked
3) Establish the connection between the Remote AP and Controller
4) Create a user role for the Remote AP user
5) Configure the VPN Pool
6) Define the AP Group and settings
7) Whitelist the Remote AP
8) Provision the Remote AP

To configure the Controller to use an IPsec tunnel with a Remote Access Point for both initial registration and ongoing communications, the following high-level procedure is used:

1) Admins define an IPsec policy for supported algorithms for RAP devices based on their certificate type they have been provisioned with. This is described in section 2.2.6.3.
2) Admins create a dynamic-map for RAP devices as described in section 2.2.6.3 and connect the IPsec transform policy to it.
3) An IKEv2 policy must be configured as described in sections 2.2.6.4 through 2.2.6.8;
4) No explicit IKEv2 profile is needed because the Controller and RAP devices will automatically select an appropriate IKEv2 policy and dynamic-map contingent on the use of a specific provisioned certificate type.
5) RAP certificates are configured according to sections 2.2.6.9 and 2.2.6.10 with specific provisioning instructions provided in section 2.4.6.1 for RAP devices.

Full details on these procedures can be found in the User Guide under the Section “Remote Access Points”.

To disable a Remote AP, the Security Administrator would only need to disable the user role, VPN pool, or AP group. Alternatively, the Security Administrator can remove the Remote AP from the whitelist. Mobility Controllers will not respond to a disabled RAP device.

If during the provisioning process the connection between the Controller and Remote AP is interrupted, the process will halt and will resume once connectivity is re-established. If the operational channel (FPT_ITT.1) is unintentionally broken, the connection will be retried automatically.

IPsec is used by the Controller and Remote APs for both initial registration and ongoing communications between the components. No other protocol is used for this communication in the evaluated configuration.

Note: RAP devices are shipped with a pre-configured unique RSA certificate by default but can be configured to use custom certificates at the administrator’s discretion. See section 2.4.6.1 for more information.

2.4 Identification and Authentication (FIA)

2.4.1 FIA_AFL.1

All configuration related to administrative login is configured using "aaa password-policy mgmt". Note that if the remote authentication server locks out a user, the local account with the same name will not be marked as locked. However, the local user will not be able to authenticate when configured authenticate against the remote authentication server. To configure failed authentication lockout that will lock an administrative account for five minutes, when five failed login attempts occur in a three minute period, use the following commands:

```
(config) #aaa password-policy mgmt
(Mgmt Password Policy) #password-lock-out 5
(Mgmt Password Policy) #password-lock-out-time 5
```

```
(Mgmt Password Policy) #enable
```

An admin account that is configured to use public key authentication will not be locked out.

It may take up to one minute for a locked out account to become accessible again once the configured lockout period has elapsed.

2.4.2 FIA_PMG_EXT.1

Administrative password policies are configured under “aaa password-policy mgmt”.

```
(config) #aaa password-policy mgmt
(Mgmt Password Policy) #password-min-length 8
(Mgmt Password Policy) #password-min-lowercase-characters 1
(Mgmt Password Policy) #password-min-uppercase-characters 1
(Mgmt Password Policy) #password-min-special-characters 1
(Mgmt Password Policy) #password-min-digit 1
(Mgmt Password Policy) #enable
```

Any combination of upper and lower case letters, numbers, and the following special characters can be used when configuring passwords: !, @, #, $, %, ^, &, *, (,), _, and +.

The ‘password-min-length’ field can be configured, per the guidance in the evaluated configuration, to restrict length from a minimum of 8 characters. The ArubaOS 8.x CLI Reference Guide and TOE permit configuration of a minimum length of 8 characters but to ensure compliance a length of 8 characters or greater must be used.

Once configured, the TOE only permits the use of strong passwords which should be greater than 8 characters in length and contain a sufficiently unique set of characters representative of all character types described in this section.

2.4.3 FIA_UAU.7

No configuration required.

2.4.4 FIA_UAU_EXT.2

Configure administrative users with “mgmt-user”. For example, to add a read-only user with the username “ops”, use the following command:

```
(config) # mgmt-user ops read-only
Password:***************
Re-Type password:***************
```

2.4.5 FIA_UIA_EXT.1

A warning banner may be configured as follows. Ensure that no line is longer than 255 characters.

```
#configure terminal
Enter Configuration commands, one per line. End with CNTL/Z


(config) #banner motd =
Enter TEXT message [maximum of 4095 characters].
Each line in the banner message should not exceed 255 characters.
End with the character '='.


You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only. By using this IS (which includes
any device attached to this IS), you consent to the following conditions:
-The USG routinely intercepts and monitors communications on this IS for
purposes including, but not limited to, penetration testing, COMSEC
monitoring, network operations and defense, personnel misconduct (PM),
law enforcement (LE), and counterintelligence (CI) investigations.
-At any time, the USG may inspect and seize data stored on this IS.
-Communications using, or data stored on, this IS are not private, are
subject to routine monitoring, interception, and search, and may be
disclosed or used for any USG-authorized purpose.
-This IS includes security measures (e.g., authentication and access
controls) to protect USG interests -- not for your personal benefit or
privacy.
-Notwithstanding the above, using this IS does not constitute consent to
PM, LE or CI investigative searching or monitoring of the content of
privileged communications, or work product, related to personal
representation or services by attorneys, psychotherapists, or clergy, and
their assistants. Such communications and work product are private and
confidential. See User Agreement for details
=
```

The TOE banner can also be configured via the MC WebUI by navigating to:

“Configuration > System”. Click on the ‘Admin’ tab and modify the ‘Login banner text’ field as necessary.

The TOE permits authentication by an administrator through SSH or Web UI over TLS or via a serial console (direct) connection to the CLI. Authentication is permitted through username/password and public key authentication (for SSH) via local authentication or by a remote authentication server (RADIUS/TACACS+). Authentication to the TOE through a wireless connection does not permit administration by default.

Instructions on configuration RADIUS server authentication can be performed through the Mobility Controller by following the guidance in the Section ‘Enabling RADIUS Server Authentication’ in the ArubaOS User Guide.

Instructions for configuring TACACS+ can also be found in the User Guide under the Section ‘Configuring a TACACS+ Server’.

No user can perform any actions prior to successful authentication to the TOE outside of viewing the warning banner as defined under FTA_TAB.1 and above.

Local console access should remain physically proximate to the device. It is not recommended that console interfaces be connected to remote consoles or serial-over-lan devices.

Once remote authentication is enabled, the local password recover user, which is enabled by default, should be disabled.

To accomplish this, enter the following configuration:

```
(config) #password-recovery-disable
```

2.4.6 FIA_X509_EXT.1/2

Certificate Signing Requests (CSRs) may be generated by the controller. This process is described in the ArubaOS User Guide. Best practice is to generate the CSR on the controller, then load the resulting certificate after issuance by the CA. This protects the private key from disclosure. If the private key is generated externally, the controller can also accept a certificate/key combination in the form of a PKCS#12 file.

ArubaOS validates the extendedKeyUsage field in accordance with certificates presented for OCSP responses. ArubaOS does not claim FCS_TLSC_EXT.x or X.509 certificates for trusted updates, making no claim to the rules specified under FIA_X509_EXT.1.1/Rev. These claims are trivially satisfied.

ArubaOS supports certificate revocation checking using OCSP.

When a root CA or intermediate CA certificate is loaded on the controller, an automatic Revocation Check Point (RCP) section is created in the configuration file. These may be shown using "show crypto-local pki rcp". For each RCP, the revocation check method may be configured, and must be set to ocsp. When OCSP has been specified, then an OCSP responder URL and OCSP responder certificate must be specified. In addition, an administrator may configure the behavior if an OCSP responder is unreachable - treat the certificate as valid or treat the certificate as revoked.

To verify OCSP responses, ArubaOS requires that the responses be signed, and requires that the nonce extension be supported by the OCSP responder. Signed responses are verified using the "OCSP Responder" certificate. Two methods are supported: direct trust and delegated trust. For

direct trust, the signing certificate of the OCSP responder must be loaded onto the controller through the WebUI Certificate Management section, and its name configured in the relevant RCP. When used, the controller makes a direct comparison between the signer certificate included in the OCSP response, and the OCSP responder certificate that was loaded - they must be exactly the same certificate. Direct Trust is cumbersome in environments where the OCSP responder certificate expires frequently. An alternative is Delegated Trust. In this method, the "OCSP Responder" type certificate must still be loaded into the controller, in the same way just described. However, the certificate should be the *Issuing CA certificate* for the CA that issues a signing certificate to the OCSP responder. When this type of configuration is performed, ArubaOS will examine the certificate in the OCSP response, then chain one level up to see if that certificate was issued by the CA configured in the RCP. Note, OCSP does not support multiple levels of certificate chaining for delegated trust, so the direct issuer of the OCSP responder's signing certificate must be configured In the RCP. If multiple levels of certificate checking will be performed (e.g. for a peer's IPsec certificate and one level up to an Intermediate CA) then a separate RCP must be configured for each, along with an appropriate OCSP responder certificate.

The validity of peer certificates will be checked upon establishment of connections. Any server certificates uploaded to the TOE will be checked at that time.

The following configuration demonstrates revocation checking against a three-level PKI. Delegated trust is in use for validating OCSP responses. The OCSP responder is the same for both levels, and the OCSP responder's signing certificate is issued directly by the root CA, as shown in the example below.

```
crypto-local pki TrustedCA intermediate-ca ecdsa-intermediate.cer
crypto-local pki TrustedCA root-ca ecdsa-root-ca.cer
crypto-local pki OCSPResponderCert ocsp-root ecdsa-root-ca.cer
crypto-local pki rcp "intermediate-ca"
  ocsp-url "http://ocsp.domain.com/ocsp"
  ocsp-responder-cert "ocsp-root"
  revocation-check ocsp
!
crypto-local pki rcp "root-ca"
  ocsp-url "http://ocsp.domain.com/ocsp"
  ocsp-responder-cert "ocsp-root"
  revocation-check ocsp
```

For site-to-site IPsec tunnels, the peer certificate DN is configured in the ipsec-map, as shown in the example below:

```
crypto-local ipsec-map 10.10.20.1 100
     peer-cert-dn
"/C=US/ST=CA/L=Sunnyvale/O=ArubaNetworks/OU=TestLab/CN=192.168.2.1/emailA
ddress=nobody@arubanetworks.com"
```

Note: It may be difficult to determine the exact DN to configure, simply by looking at a peer's certificate. Attempting to establish an IPsec tunnel while examining the log file (possibly after enabling "logging level debugging security") will generally show the exact DN string that must be configured, once it is received from the peer.

RAP devices can be configured to use an IP address for the CN field. To set the CN, the "*provision-ap*" command must be used with the "*read-bootinfo*" and "*cert-dn*" parameters.

To configure the behavior in the event an OCSP responder cannot be reached, use the "server-unreachable" keyword under the RCP configuration. To conform with the evaluated configuration, the behavior must be to reject the certificate and shall be configured as follows:

```
(config) #crypto-local pki rcp intermediate-ca
(RCP-intermediate-ca) #server-unreachable revoke-cert
```

To configure delegated trust on the TOE for OCSP verification of each CA, ensure that CA certificates are uploaded as bundles. The following procedures should be followed:

1. Create a full CA bundle, from the leaf's issuing CA to the rootca.
2. Upload that as a trustedCA bundle.
3. Upload the same CA bundle as an OCSP responder cert.
4. Click on the RCP for the full CA bundle.
5. Ensure that the correct OCSP responder cert is selected.
6. Input the OCSP responder URL for the top most intermediary CA in the bundle.
7. For the next CA bundle, remove the top most intermediary CA and save it as a new bundle.
8. Repeat above steps until you're left with just the rootca.

In addition to the 'revoke-cert' command specified above, information for configuration of OCSP can be found in the ArubaOS 8.10 User Guide, Page 311, Section 'Understanding OCSP and CRL'.

Additional information on the configuration of CA certificates in the Mobility Controller trust store can be found in the ArubaOS 8.10.0.0 User Guide section '*Management Access'* sub-section '*Managing Certificates'.*

2.4.6.1 Provisioning Custom Certificates on the RAP

To properly load a custom certificate on to the RAP for session negotiations, the following steps should be followed:

(1) Configure Aruba Controller to provision RAPs with EC certificates

Using the Mobility Controller GUI:

a. **Create RAP group/node**

i. Navigate to Managed Network and create the new RAP group/node

b. **Generate controller Certificate Signing Request (CSR)**
    i. Navigate to the Managed Network → RAP group/node → Configuration → System → Certificates → CSR.
c. **Import the CA and Server Certificates**
    i. Once the CSR has been signed by the Certificate Authority, navigate to the Managed Network → RAP group/node → Configuration → System → Certificates → Import Certificates to import the signed server certificates.
    ii. Repeat the previous steps to import the Root and Intermediate certificates.
d. **Configure the RAP VPN Pool** – See FCS_IPSEC_EXT.1
e. Define IKE Server Certificate and CA Certificate
    i. Navigate to the Managed Network → RAP group/node → Configuration → Services → VPN → General VPN to select the server certificate for Server-certificate for VPN clients.
    ii. Navigate to the Managed Network → RAP group/node → Configuration → Services → VPN → Certificates for VPN Clients and add the CA and Server certificates for CA Certificate Assigned for VPN Clients.
f. **Define IKE Policy and IPSEC Dynamic Map** – See FCS_IPSEC_EXT.1
g. Define rap-prov-role User Role
    i. Navigate to the Managed Network → RAP group/node → Configuration → Roles & Policies → Roles to create a new user role. Select the new user role and add the acl rules below above.
h. Create a AAA authentication profile for RAP provisioning
    i. Navigate to the Managed Network → RAP group/node → Configuration → Authentication → AAA Profiles → AAA to create a new AAA profile. Select the new AAA profile and select the rap-prov-role user role defined in the previous step for the Initial role.
i. Define Wired AP profile for RAPs
    i. Navigate to the Managed Network → RAP group/node → Configuration → System → Profiles → AP → AP wired port to create a new AP wired port profile. Select the new AP wired port profile and select the AAA profile that was created in the previous step.
    ii. Select *Wired AP* under the new *AP wired port* profile created in previous step, and create a new *Wired AP* profile. Check *Wired AP enable,* and select bridge for the *Forward mode*.
j. Create RAP Provision AP Group
    i. Navigate to the Managed Network → RAP group/node → Configuration → AP Group to create a new AP group for provisioning the RAP with custom certificate.
k. Select the Wired Port for the AP group
    i. Click on the username in the upper right corner of the screen → Preferences, and check Show advanced profiles.
    ii. Selected the new RAP Provision AP Group, and navigate to Managed Network → RAP group/node → Configuration → AP Group → Profiles → AP → Ethernet interface 1 port configuration. Select the AP wired port profile created in the previous step.
l. Whitelist RAP MAC address
    i. To manually update the RAP whitelist, navigate to Managed Network → Configuration → Access Points → Whitelist → Remote AP Whitelist. The RAP's wired MAC address can be located on the label on the RAP.

m. Initial RAP provisioning

i. Navigate to Managed Network → RAP group/node → Configuration → Access Points → Campus Aps, select the AP, click Provision button, select the RAP provision group, select Remote for Deployment, and select certificate for Authentication method. For Virtual Mobility Managers or Virtual Mobility Controller, select self-signed for Trust anchor

(2) Provision RAP with EC certificates

Using the RAP WebUI:

a. On the Certificate Tabs, you can first generate a CSR file. Then, click on “save CSR” file and submit it to your Certificate Authority

b. Once you have obtained the CA and RAP Certificate (signed by the same CA as the Controller), import the CA and RAP certificate on the Certificates tab. When you successfully upload the certs, you should see the two messages in Green: Custom CA Certificate: Present and Custom RAP Certificate: Present

c. Reboot the RAP (under Connectivity tab or unplug the power), and it should now reconnect to the Controller using the Custom EC Certificates that has been installed

Note: This step uses the local RAP WebUI interface which is considered to be an out-of-scope interface for this evaluation and must only be used when not in the evaluated configuration during initial set-up or when taken out of service for maintenance purposes.

(3) Verify that the RAP is using the EC certificates

a. You can verify that the RAP is connected to the Controller with the custom certificate by looking at the output of the show ap database status up command

(4) Reprovision the RAP into the production AP group

a. After confirming the RAP is authenticating to the controller using the EC certificate, the RAP should be reprovisioned to the production RAP AP group.

2.4.7 FIA_X509_EXT.3

An example of the commands that can be used to generate a certificate sign request are provided below:

```
crypto pki
csr rsa
key_len 2048
common_name <common_val>
country <country>
organization <org>
unit <org_unit>
```

To export the request, you may show the CSR with the follow command:

```
Show crypto pki csr
```

Before creating a CSR, the administrator must ensure that the CN, country, O, and OU have been set as identified above.

2.5 Security Management (FMT)

2.5.1 FMT_MOF.1/ManualUpdate

See FPT_TUD_EXT.1 for information. No configuration is required to restrict updates to administrator role.

2.5.2 FMT_MOF.1/Services

An administrator with the management role of “root” has full privileges to enable or disable services on the TOE. The “root” role maps to the Security Administrator role.

An administrator can start and stop remote syslog services. This service can be enabled or disabled by following the guidance found throughout this document as well as in the ArubaOS 8.10 User Guide. Starting and stopping this service can be performed through policy configuration.

2.5.3 FMT_MTD.1/CoreData

An administrator with the management role of “root” has full privileges to modify, add, and delete configuration and user accounts. The “root” role maps to the Security Administrator role.

2.5.4 FMT_MTD.1/CryptoKeys

An administrator with the management role of “root” has full privileges to modify, add, and delete configuration and user accounts. The “root” role maps to the Security Administrator role. An administrator can manage all X.509 certificates, server certificates, and SSH public keys as defined within the ArubaOS 8.10 User Guidance and the specified sections of this document. Additionally, an administrator seeking to regenerate all persistent device keys can perform a ‘wipe out flash’ to zeroize keys. The TOE will regenerate these keys upon restart.

Please note that wipe out flash will also perform a reset of the configuration and should only be performed when planning to decommission the device or reconfigure it from factory settings.

Specific information relating to each cryptographic security parameter can be found within the FIPS Security Policy, located on the CMVP website: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3552

2.5.5 FMT_SMF.1

No additional configuration required. Please reference the Aruba OS User Guide for a full list of configuration instructions through the CLI and Web GUI.

2.5.6 FMT_SMR.2

No additional configuration required.

2.6 Packet Filtering (FPF)

2.6.1 FPF_RUL_EXT.1

The EP lists several requirements to test packet filtering behavior. All configuration for these tests is performed using the "ip access-list session" command. The ArubaOS User Guide contains extensive documentation on how firewall rules are configured. To summarize:

For a wired interface: Configure a single ACL and apply it to a physical interface or VLAN interface. For example, to block ICMP "ping" on an Ethernet port:

```
(config) #ip access-list session block-icmp
(config-sess-block-icmp)#any any icmp echo deny log
(config-sess-block-icmp)#exit
(config) #interface gigabitethernet 1/2
(config-if)#ip access-group block-icmp session
```

Use the "log" keyword In the firewall rule to ensure that hits against this rule appear in the audit log.

For a user (Wi-Fi or VPN): Any user session that appears in "show user-table" has a role and firewall policy associated with it, as long as the PEF-NG or PEF-V license is installed. Configuration of user roles is described extensively in the ArubaOS User Guide. Mapping a user into a particular role is normally performed at the time of authentication, through one of the "aaa" policies, and may be based on a default role or may be based on attributes returned from an authentication server. Once a user session is placed into a role, firewall policies (one or more) are applied. Firewall policies contain one or more firewall rules. The following is an example of a role/policy configuration:

```
(config) #ip access-list session filter_http
(config-sess-filter_http)#user network 172.16.1.0 255.255.255.0 svc-http
permit
(config-sess-filter_http)#user network 172.16.2.0 255.255.255.0 svc-http
permit
(config-sess-filter_http)#user any svc-http deny log
(config-sess-filter_http)#exit
(config) #ip access-list session filter_smtp
(config-sess-filter_smtp)#user any svc-smtp deny log
(config-sess-filter_smtp)#exit
(config) #user-role example_role
(config-role) #session-acl filter_http
```

```
(config-role) #session-acl filter_smtp
(config-role) #session-acl allowall
```

To see the resulting policy, issue the command "`show rights example_role`".

ArubaOS supports standard, extended, and session ACLs. Only session ACLs are stateful.

By default, ArubaOS does not enforce a full three-way TCP handshake before permitting traffic – this is an optimization for Wi-Fi mobility. To enable enforcement of a full TCP handshake, configure the system as follows:

```
(config) #firewall enforce-tcp-handshake
```

To enable enforcement of TCP sequence numbers:

```
(config) #firewall enforce-tcp-sequence
```

To process ICMP packets statefully, enable stateful ICMP processing:

```
(config) #firewall enable-stateful-icmp
```

To statefully follow TCP session teardown, enable the following feature:

```
(config) #firewall prohibit-rst-replay
```

Perform similar configuration for IPv6:

```
(config) #ipv6 firewall enforce-tcp-handshake
(config) #ipv6 firewall prohibit-rst-replay
(config) #ipv6 firewall enable-stateful-icmp
```

The ArubaOS User Guide contains a full description of how firewall rules are configured. This guidance provides a summary. Firewall rules are configured according to a common general pattern:

```
(config) #ip access-list session <name>
(config-sess-<name>)# <source> <destination> <service> <action> <extended
action> <position>
```

Rules should be configured in order from highest priority to lowest; enforcement is based on a first-match principle where the first rule that matches a traffic flow is applied, and further rules are not processed. The <position> field may be used to insert new rules somewhere other than at the end of a policy.

The following shows several examples of different rules that may be configured, which should give the reader a flavor of what is possible. Context-sensitive help is available in the ArubaOS CLI at any time by typing the ? character.

The following examples demonstrate the use of these commands.

ICMPv4:

```
(config) #ip access-list session FFW_RUL_EXT_1_3
(config-sess-FFW_RUL_EXT_1_3)#any any icmp echo deny
(config-sess-FFW_RUL_EXT_1_3)#any network 10.0.0.0 255.0.0.0 icmp port-
unreachable permit
(config-sess-FFW_RUL_EXT_1_3)#host 172.16.52.1 any icmp traceroute permit
```

```
(config-sess-FFW_RUL_EXT_1_3)#any any icmp 3 permit
(config-sess-FFW_RUL_EXT_1_3)#any any svc-icmp deny log
```

Note: In the final example, the alias “svc-icmp” was used. This is a firewall alias which is defined using the keyword “netservice”. In the standard ArubaOS config file, svc-icmp is defined as follows:

```
netservice svc-icmp 1
```

This indicates that it is IP protocol 1 (ICMP). The “netservice” definition does NOT indicate network services (listeners) that are enabled on the mobility controller – they are used only for convenience when defining firewall rules.

ICMPv6:

```
(config-sess-FFW_RUL_EXT_1_3)#ipv6 any any icmpv6 echo-request deny
(config-sess-FFW_RUL_EXT_1_3)#ipv6 any network 2004:10:09::0/64 icmpv6 port-
unreachable permit
(config-sess-FFW_RUL_EXT_1_3)#ipv6 host 2006:03:23::123 any icmpv6 hop-limit-
exceeded permit
(config-sess-FFW_RUL_EXT_1_3)#ipv6 any any icmpv6 nb-adv permit
(config-sess-FFW_RUL_EXT_1_3)#ipv6 any any icmpv6 nb-solicitation permit
```

IPv4:

```
(config-sess-FFW_RUL_EXT_1_3)#any network 10.2.3.0 255.255.255.0 any permit
(config-sess-FFW_RUL_EXT_1_3)#host 1.2.3.4 any any deny log
(config-sess-FFW_RUL_EXT_1_3)#any network 10.2.4.0 255.255.255.0 17 permit
```

IPv6:

```
(config-sess-FFW_RUL_EXT_1_3)#ipv6 any network 2001:42:65::0/64 any permit
(config-sess-FFW_RUL_EXT_1_3)#ipv6 any network 2001:42:66::0/64 17 deny log
```

TCP:

```
(config-sess-FFW_RUL_EXT_1_3)#any any tcp source 53 dest 65 permit
(config-sess-FFW_RUL_EXT_1_3)#any any tcp 80 permit
```

UDP:

```
(config-sess-FFW_RUL_EXT_1_3)#any any udp source 1234 dest 5678 permit
(config-sess-FFW_RUL_EXT_1_3)#any any udp 53 permit
```

The TOE can be configured to restrict the distinct interface (ie. the external port where the applicable network traffic was received or will be sent) and the.following protocols and associated attributes:

- ICMPv4
  - Source address
  - Destination Address
  - Type
  - Code
- ICMPv6
  - Source address
  - Destination Address
  - Type

    - Code
- IPv4
    - Source address
    - Destination Address
    - Transport Layer Protocol
- IPv6
    - Source address
    - Destination Address
    - Transport Layer Protocol
    - IPv6 Extension header type
- TCP
    - Source address
    - Destination Address
    - Source Port
    - Destination Port
- UDP
    - Source address
    - Destination Address
    - Source Port
    - Destination Port

Once a firewall policy is defined, it may be assigned to an interface. The following examples show a firewall policy being applied to a physical Ethernet port, and to a VLAN interface.

```
(config) #interface gigabitethernet 1/3
(config-if)#ip access-group FFW_RUL_EXT_1_3 session
(config-if)#interface gigabitethernet 1/2
(config-if)#ip access-group FFW_RUL_EXT_1_3 session vlan 2
```

The following commands can be used to ensure TCP sequencing is properly enforced:

```
firewall enforce-tcp-handshake
firewall enforce-tcp-sequence
firewall prohibit-rst-replay
ipv6 firewall enforce-tcp-handshake
ipv6 firewall enforce-tcp-sequence
ipv6 firewall prohibit-rst-replay
```

The TOE provides stateful session firewalls for communication sent through its interfaces. The Aruba Policy Enforcement Firewall (PEF) provides context-based controls to enforce application-layer security and prioritization. With PEF, IT can enforce network access policies that specify who may access the network, with which mobile devices and which areas of the network they may access.

The TOE implements a full stateful firewall instance around every user, tightly controlling what the user is permitted to do and providing separation between user classes.

For the highest level of network security, Mobility Controllers support client-to-data center encryption, whether providing Wi-Fi services or VPN tunneling. The TOE provides a unified point for authentication, encryption and policy enforcement. When session access control lists are configured with logging

specified, traffic sent through the session will be logged in syslog and recorded within statistical counters that can be viewed by an administrator.

The following commands can be used to ensure proper handling of traffic with addresses identified as 'reserved for future use'.

```
firewall deny-reserved-ip
ipv6 firewall deny-reserved-ip
```

The TOE blocks the following protocols by default:

- IPv6
  - Protocol 135
  - Protocol 140

All other protocols are supported and allowed during normal operation of the TOE.

The Mobility Controller should be configured with a default Access Control List to ensure that traffic not otherwise matching a configured allow rule is dropped (implicit deny/drop). To ensure logging of traffic, the following rule should be applied as the last rule of an ACL to drop and log all unwanted traffic:

```
(config-sess-ACL)#any any any deny log
```

All rules should contain 'log' as shown above to ensure all traffic is properly captured. Below is additional information on configuration of access controls for the traffic sent through the TOE:

1) The firewall will automatically drop invalid fragments. If logging of these packet drops is needed, configure "*firewall log-ip-error" and "ipv6 firewall log-ip-error*".
2) ArubaOS does not automatically determine which packets should be allowed through an interface. Configure a firewall rule with a source containing the network's address, and apply it to the inbound interface.
3) ArubaOS, because it may operate as a router, does not automatically determine which source addresses are acceptable to pass through an interface. Configure firewall rules appropriately to determine which source addresses are accepted through an interface.
4) Define a firewall rule to reject traffic with a source of a local broadcast address. This rule is useful only for local subnets, since the mobility controller has no knowledge of the broadcast address for remote networks.
5) Define a firewall rule to reject traffic with a source address that falls within the multicast range of 224.0.0.0 through 239.255.255.255. This can be done using the following rule:
   ```
   network <IP address> <Subnet> any any deny log
   ipv6 network <IPv6 address> any any deny log
   ```
6) Define a firewall rule to reject traffic with a source address that is defined as a loopback address. This can be done using the following rule:
   ```
   network <IP address> <Subnet> any any deny log
   ```
7) Define a firewall rule to reject traffic with a source address that is defined as a link-local address. This can be done using the following rule:
   ```
   ipv6 network <IPv6 address> any any deny log
   ipv6 any network <IPv6 address> any deny log
   ```
   Note: This will prevent other devices on the same subnet from communicating with the mobility controller through link-local addressing.

8) To configure the firewall to reject traffic that is using reserved IPv4 address space, configure the following:
```
firewall deny-reserved-ip
```
9) To configure the firewall to reject traffic that is using reserved IPv6 address space, configure the following:
```
ipv6 firewall deny-reserved-ip
```
10) Please note that for each internal interface, external network addresses should be configured to be blocked from the internal network interface. For each external network interface, the internal network addresses should be blocked from communicating with the interface. This can be done by explicitly permitting communication between internal network subnets and applying a deny rule on each external network interface for communication to an internal network address (an example is shown below):
```
Internal Rule:
ipv6 network 2001:192:168:144::/112 2001:192:168:124::/112 any permit
ipv6 network 2001:192:168:144::/112 any any deny
External Interface:
ipv6 network any 2001:192:168:144::/112 any deny
```

The TOE access control lists function in a hierarchical structure. If a rule is applied at the beginning of the ACL, it will take priority over any rule following it. For instance, if an access rule denies a specific IP address and a later rule permits a subnet that contains the specific host, the initial rule denying that specific IP will be applied and traffic from that IP address will be dropped.

Note: If a rule is applied permitting or denying traffic, applying the inverse of this rule will overwrite the pre-existing rule. The TOE will not allow inverse rules to be applied. Additional information for access rule lists can be found within the Aruba AOS 8.10 User Guide.

An access control list must be applied to all in-use interfaces in the evaluated configuration. If traffic is sent to an interface and no rule within the ACL applied to that interface matches the packet in-transit, the packet will be dropped.

To ensure logging of traffic, the following rule should be applied as the last rule of an ACL to drop and log all unwanted traffic:
```
(config-sess-ACL)#any any any deny log
```

All unsolicited messages are dropped by default. This can be tracked within “authmgr” warning logs.

By default, TCP sequence numbers are ignored. The following commands can be used to ensure TCP sequencing is properly enforced:
```
firewall enforce-tcp-handshake
```

The command ‘enforce-tcp-handshake’ prevents data from passing between two clients until the three-way TCP handshake has been performed, at a upper limit of 8 half-open TCP connections.
```
firewall enforce-tcp-sequence
```

The command ‘enforce-tcp-sequence’ enforces the TCP sequence numbers for all packets.

When applied, the TOE will monitor traffic sent through the TOE and drop half-open TCP connections.To monitor if traffic has been dropped, an administrator can enter the following command:

```
Show datapath frame
This will identify a counter next to the entry "Drop due to max half syns."
```

ICMPv4 Code 134 is an unsolicited router advertisement which is discarded/dropped by the controller. All other traffic is handled based upon access control lists configured on the TOE.

2.7 Protection of the TSF (FPT)

2.7.1 FPT_APW_EXT.1

No additional configuration required.

2.7.2 FPT_ITT.1 & FPT_ITT.1/Join

No additional configuration required. See Section '*FCO_CPC_EXT.1'* for establishing connections between TOE components.

2.7.3 FPT_FLS.1/SelfTest (VPNGW)

No configuration required. For additional information, see section 2.7.6.

2.7.4 FPT_SKP_EXT.1

No additional configuration required.

2.7.5 FPT_STM_EXT.1

Mobility controllers require clock synchronization using NTPv4 in order to generate reliable timestamps. To specify an NTP server:

```
(config) # ntp server <IP address>
(config) # ntp server <IP address>
(config) # ntp server <IP address>
```

Additionally, an administrator can configure a manual system time with the following command:

```
(config) # clock set <year> <month> <day> <HH:MM:SS>
```

The TOE supports configuration of 3 NTP time sources. Multiple time servers can be configured with the use of the 'ntp server' command shown above.

If a remote NTP server is used, the administrator must ensure that the connection is protected via pre-shared keys or IPsec. The TOE, by default, does not accept broadcast and multicast NTP

packets. More NTP options, including authentication, are configurable using the following command syntax:

```
(config) #ntp authenticate
(config) #ntp authentication-key <key-id> sha1 <key-secret>
(config) #ntp trusted-key <key-id>
(config) #ntp server <ipaddr> <iburst> <key>
(config) #ntp server <server IP> <iburst key> <key>
```

See the ArubaOS 8.10.0.0 User Guide section '*Configuring NTP Authentication'* for more information.

2.7.6 FPT_TST_EXT.1

No configuration required.

The module performs at power-on the Cryptographic Algorithm Self-Tests (CASTs), Pre-Operational Self-Tests (POSTs), and Conditional self-tests. After the cryptographic algorithm, pre-operational (including integrity tests), and conditional self-tests are successfully concluded, the module automatically transitions to the operational state and is operating in the approved mode of operation by default. While the module is executing the cryptographic algorithm and pre-operational self-tests, services are not available, and input and output are inhibited. In addition, the module also performs Conditional self-tests. All cryptographic algorithm self-tests are run at power-up, prior to the first operational use of the cryptographic algorithm.

If a self-test fails, the TOE will immediately halt operation and enter an error state thereby preventing potentially insecure operations (i.e., maintaining a secure state). The Mobility Controller and RAP devices will reboot after a self-test failure. During reboot, memory is re-initialized, which wipes all keys and user data. If a self-test failure continues to occur, the controller or RAP device will continue to reboot repeatedly and will require return to manufacturer. The error output of a failed self-test will appear as follows: "FIPS Aruba Cryptographic asymmetric key KAT failure, main: FIPS_powerupSelfTest failed." If a firmware image fails its integrity check, the TOE will load the previous image (if one is present). An error will be output during boot in this instance stating that the firmware validation failed.

The local console for Mobility Controller and RAP devices can be reviewed to determine which component has failed a self-test. Mobility Controllers maintain health status information for each connected RAP device. For devices not marked as 'connected', an investigation and review of the local console can determine if the RAP device has experienced an issue.

If the issue continues, the administrator should contact support at http://support.arubanetworks.com.

2.7.7 FPT_TST_EXT.3

No configuration required.

2.7.8 FPT_TUD_EXT.1

On Mobility Controllers, use the command "*show version*" to show the currently executing version of firmware/software and the command "*show image version*" to show both the currently executing and loaded but inactive/backup versions of firmware/software.

For RAP devices use the command "show ap image version" to view the currently executing firmware/software version. RAP devices can only have one version of software/firmware loaded and running at any given time.

Upgrades to both the Mobility Controller and RAP devices are performed through the controller. Security Administrators perform updates to the RAP by downloading the update to the Mobility Controller. Note: All images (for MC & RAP devices) are bundled into the single downloaded image file.

When the RAP attempts to connect, the controller will push the new updated image to the RAP to install and reboot immediately. The controller will not allow a connection from the RAP unless they are running on the same version of ArubaOS.

Use the "copy" command to download new firmware images from an FTP or TFTP server and to select the system partition to which the image file is copied. Note that the administrator should first ensure that the `boot system partition <partition_id>` command is correctly set to specify the system partition number that the controller should use during the next reboot. The following CLI commands transfer the ArubaOS image file:

```
copy tftp:<tftphost><filename>system:partition[0|1]}
copy ftp:<ftphost><user><filename>system:partition{0|1}
```

An option is provided to reboot the device with the transferred image file.

From the WebUI, navigate to Maintenance>Software Management>Upgrade page to upload an ArubaOS image from a local filesystem. Specify the system partition to which the image file is copied and choose whether the device should be rebooted when the image file is transferred. Click Upgrade.

The validation of the Mobility Controller and RAP images are performed at start-up when the image is loaded. ArubaOS images are integrity-protected through two methods:

1. ArubaOS images are digitally signed using RSA 2048-bit signature validation. The mobility controller will check the digital signature immediately after downloading a new firmware image and will refuse to install an image whose digital signature does not match.
2. Mobility controllers also check the digital signature of an ArubaOS image when booting. The controller will refuse to boot a corrupted ArubaOS image file.

If digital signature verification fails, the TOE will enter into an error state. The TOE's error state will allow direct console access only, where an administrator can change to a new file partition or TFTP a new image and re-boot.

If digital signature verification succeeds, the TOE will proceed with the installation of the image or continue booting into the normal operating state.

2.8 TOE Access (FTA)

2.8.1 FTA_SSL.3

For remote administrative sessions, an idle timeout period may be configured to disconnect idle sessions.

The timeout value for the CLI can be configured to between 1 and 3600 seconds. To disable, set to 0. The default value is 15 minutes. To configure the timeout value, use the following command:

```
(config) #loginsession timeout <value-in-seconds>
```

The idle timeout value for the WebUI can be configured in the Web UI by navigating to Configuration>System>Admin>Admin Authentication Options and setting the 'Idle session timeout' value to between 30 and 3600 seconds.

2.8.2 FTA_SSL.4

No configuration required. An administrator can terminate their own session by exiting the SSH session or logging out from the Web UI session. To enforce a timeout interval, please see Section '*FTA_SSL_EXT.1*' below.

2.8.3 FTA_SSL_EXT.1

For local administrative sessions via the CLI, an idle timeout may be set to disconnect idle sessions. The timeout value can be configured to between 1 and 3600 seconds. To disable, set to 0. The default value is 15 minutes. To configure the timer value, use the following command:

```
(config) #loginsession timeout <value-in-seconds>
```

2.8.4 FTA_TAB.1

See FIA_UIA_EXT.1.1 above for a description of how to configure a notice and consent banner message.

2.9 Trusted Path/Channels (FTP)

2.9.1 FTP_ITC.1 & FTP_ITC.1/VPN (VPNGW)

ArubaOS supports IPsec as the inter-TSF trusted channel. This channel is to be used between a Mobility Controller and a) a syslog server, b) a RADIUS or TACACS server, c) an NTP server, d) remote VPN Gateways/Peers.

To establish an IPsec channel, the following must first be configured:

- An IKEv2 policy must be configured as described in sections 2.2.6.4 through 2.2.6.8;
- An IPsec transform policy must be configured as described in section 2.2.6.3;
- An IKEv2 profile must be configured to connect the IKEv2 policy and IPsec transform policy as described in section 2.2.6.2.

Note: The ‘src-net’ and ‘dst-net’ properties specify the selectors for IPsec traffic which directly impact the IP addresses selected to communicate over the IPsec channel.

When configuring an IPsec channel, the IP address configured for the trusted IT entity (eg. Syslog, NTP, RADIUS, and Remote VPN gateways/peers) must comply with the ‘src-net’ and ‘dst-net’ ranges defined in the IKEv2 profile for the TOE to enforce the use of IPsec.

If for any reason a connection is unintentionally broken, the TOE will re-establish the connection once connectivity is restored. If the timeout period has expired, re-authentication/re-negotiation is required.

2.9.2 FTP_TRP.1/Admin

Communication between a Mobility Controller and a remote administrator may be protected by TLS/HTTPS (when using the Web-based interface via web browser) or SSH (when using the command-line interface via ssh client). All remote administration must take place over one of these interfaces.

For tunneling over IPsec, the administrator must ensure that the workstation in the IT environment that is being used is recognized as an IPsec peer to the TOE so that the IPsec tunnel can be used. The precise instructions to ensure that the specific administrative client can be used (web browser or SSH client) depends on the third-party IPsec software being used on the workstation and the administrative client. Refer to section 2.9.1 for instructions on establishing an appropriate IPsec tunnel to the workstation.

The administrator must ensure that the ssh client and/or web browser in use is compatible with the algorithms claimed in the Security Target.

No configuration is required on RAP devices once all components have been placed into evaluated configuration, therefore no admin interfaces are available on RAP devices once this state is achieved.

3 Reference Documents

The Guidance documentation for ArubaOS can be found in its entirety at the link below:

https://asp.arubanetworks.com/downloads;fileTypes=DOCUMENT;products=Aruba%20Mobility%20Gateways;softwareMajorVersions=8.10

a) ArubaOS 8.x Command-Line Interface Reference Guide, 2023

b) ArubaOS 8.10.0.0 User Guide, Revision 14, 2023

c) ArubaOS 8.10.0.0 Syslog Reference Guide

d) Aruba 303H Series Hospitality Access Points Installation Guide, March 2017

e) Aruba 503H Series Hospitality Access Points Installation Guide, July 2020

f) Aruba AP-505H Access Points Installation Guide, May 2023

g) Aruba 7200 Series Controller Installation Guide, 0511169-06 | July 2015

h) Aruba 9004 Gateway Installation Guide, Revision 03 | June 2021