COMMON CRITERIA CONFIGURATION GUIDANCE

ARUBA OS 8.10 SUPPLEMENTAL GUIDANCE

Aruba Mobility Conductor with ArubaOS 8.10-FIPS

Version 2.6
June, 2023

a Hewlett Packard Enterprise company

www.arubanetworks.com

CONTENTS

1 Introduction

This document serves as a supplement to the official Aruba user guidance (documentation), consolidating configuration information specific to the Common Criteria Network Device Collaborative Protection Profile 2.1.

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 conductor, 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.

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 Evaluated Platforms

The following platforms are covered under the evaluated configuration:

- MCR-HW-1K-F1
- MCR-HW-5K-F1
- MCR-HW-10K-F1

1.2 Version Information

This document covers Aruba Mobility Conductors running ArubaOS 8.10. Customers are advised to use the newest available 8.X release to take advantage of defect fixes, which may include fixes for security vulnerabilities.

1.3 Aruba Firewall high-level concepts

In an ArubaOS, 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 Conductor 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 Conductor 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 Conductor 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 and CLI Reference Guide for full details on roles, firewall policies, authentication, and user management.

1.4 Acceptance Procedures

Upon delivery of the TOE, 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 the product has been received in the packaging provided from HPE Aruba Networking.

(2) Review the packaging slip/label and ensure that the product as delivered is listed within the Security Target.

(3) After verification, remove the product from the packaging and place it within a secure storage location to prevent access from unauthorized individuals.

(4) Connect power and serial console to the device 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.

1.5 Preparatory Guidance

Before installing the Aruba Mobility Conductor, 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 Conductor with its time data over an IPsec-encrypted trusted channel
- A syslog server is available and capable of supporting TLS-encrypted syslog
- 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 Conductor properly and securely.

1.6 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)
- Cryptographic Support (FCS)
- Identification and Authentication (FIA)
- Security Management (FMT)
- 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. If 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.

Requirement	Auditable Events	Additional Content
FAU_GEN.1	Startup and Shutdown of the Audit function Password Resets Managing Cryptographic Keys Administrative login and logout: see FIA_UIA_EXT.1 Changes to TSF Data: See FMT_SMF.1	None

Startup and Shutdown of Audit Function

Oct 10 23:58:11 2022 cli[32430]: USER:admin@serial NODE:"/mm/mynode" COMMAND:<no logging 1.1.1.249 > -- command executed successfully
Oct 10 23:58:20 2022 cli[32430]: USER:admin@serial NODE:"/mm/mynode" COMMAND:<logging 1.1.1.249 severity debugging> -- command executed successfully

Password Resets

Jan 11 09:45:50 2023 ArubaConductor-HW-1K <ArubaConductor-HW-1K 192.168.100.250> profmgr[9416]: USER:admin@192.168.1.135 NODE:"/mm/mynode" COMMAND:<mgmt-user admin root node / > -- command executed successfully

Jan 11 09:45:50 2023 ArubaConductor-HW-1K authmgr[9425]: <124004> <9425> <DBUG> <ArubaConductor-HW-1K 192.168.100.250> cmdtype=2, len=115, cmd='USER:admin@192.168.1.135 NODE:"/mm/mynode" COMMAND:<mgmt-user admin root node / > -- command executed successfully '

Managing Cryptographic Keys

May 16 16:03:22 2023 ArubaConductor-HW-1K <ArubaConductor-HW-1K 192.168.100.250> profmgr[9320]: USER:admin@192.168.1.135 NODE:"/mm/mynode" COMMAND:<crypto pki csr rsa key_len 2048 common_name services.example.com country CA state_or_province Austin city Texas organization HPE Aruba Networking unit ATA email admin@example.com > -- command executed successfully

Apr 19 16:54:40 2023 ArubaConductor-HW-1K <ArubaConductor-HW-1K 192.168.100.250> cli[3761]: USER:admin@192.168.1.135 NODE:"/mm/mynode" COMMAND:<set ca-certificate RootCA-ECDSA > -- command executed successfully

Apr 19 16:54:46 2023 ArubaConductor-HW-1K <ArubaConductor-HW-1K 192.168.100.250> cli[3761]: USER:admin@192.168.1.135 NODE:"/mm/mynode" COMMAND:<set server-certificate TOE-VPN-ECDSA > -- command executed successfully

Apr 21 20:09:54 2023 ArubaConductor-HW-1K <ArubaConductor-HW-1K 10.222.7.140> profmgr[9328]: USER:admin@10.222.7.136 NODE:"/mm/mynode" COMMAND:<no crypto-local pki TrustedCA RootCA-RSA > -- command executed successfully

FAU_GEN.2	None	None
FAU_STG_EXT.1	None	None
FCS_CKM.1	None	None
FCS_CKM.2	None	None
FCS_CKM.4	None	None
FCS_COP.1/DataEncryption	None	None
FCS_COP.1/Hash	None	None
FCS_COP.1/KeyedHash	None	None
FCS_COP.1/SigGen	None	None
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Reason for failure.

Jul 28 19:28:24 2022 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:

FCS_IPSEC_EXT.1	Failure to establish an IPsec SA.	Reason for failure.

Oct 11 00:37:22 2022 isakmpd[3947]: <103063> <3947> <DBUG> |ike| 192.168.145.249:500-> I <-- Notify: NO_PROPOSAL_CHOSEN spi={67790220aa016a9f 0000000000000000} np=SA

FCS_NTP_EXT.1	Configuration of a new time server Removal of configured time server	Identity if new/removed time server

Configuration of new time server

May 27 14:11:22 2023 profmgr[5703]: USER:admin@192.168.144.4 NODE:"/mm/mynode" COMMAND:<ntp server 192.10.1.13 > -- command executed successfully

Removal of configured time server

May 27 14:18:47 2023 profmgr[5703]: USER:admin@192.168.144.4 NODE:"/mm/mynode" COMMAND:< no ntp server 192.10.1.13 > -- command executed successfully

FCS_RBG_EXT.1	None	None

FCS_SSHS_EXT.1	Failure to establish an SSH session.	Reason for failure.
Oct 11 01:59:46 2022 sshd[7305]: <199801> <7305> <INFO> |sshd| Failed password for admin from 192.168.144.249 port 36920 ssh2		
FCS_TLSS_EXT.1	Failure to establish a TLS Session.	Reason for failure.
Feb 25 08:02:01 2023 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:		
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).
Nov 6 14:01:10 2022 ArubaConductor-HW-1K aaa[3483]: <125027> <3483> <DBUG> <Aruba7030 192.168.144.201> mgmt-auth: admin, failure, , 0 Nov 6 14:01:10 2022 ArubaConductor-HW-1K aaa[3483]: <125050> <3483> <DBUG> <Aruba7030 192.168.144.201> [aaaMsg.c:1316] Determining the existing sessions for user: admin with configured max_sessions 0 Nov 11 16:40:54 2022 ArubaConductor-HW-1K stm[3609]: <501103> <3609> <WARN> <Aruba7030 192.168.144.201> Blacklist add: 74:9e:f5:ff:a5:e9: Reason: auth-failure		
FIA_PMG_EXT.1	None	None
FIA_UAU.7	None	None
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
See FIA_UIA_EXT.1		
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
Oct 11 00:09:18 2022 sshd[24685]: <199801> <24685> <DBUG> |sshd| debug1: userauth-request for user admin service ssh-connection method password Oct 11 00:09:18 2022 sshd[24685]: <199801> <24685> <INFO> |sshd| Accepted password for admin from 192.168.144.249 port 36904 ssh2 Feb 28 02:11:41 2023 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 2023 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 01:34:15 2023 cli[29241]: USER: admin has logged in using serial. Feb 28 01:37:53 2023 webui[3800]: USER: admin has logged in from 192.168.144.253. Feb 28 01:48:27 2023 cli[30967]: USER: admin connected using serial has logged out. Feb 28 01:50:15 2023 cli[32640]: USER: admin has logged in using serial.		

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. Identification of certificates added, replaced, or removed as trust anchor in the TOE's trust store
Feb 28 00:43:34 2023 isakmpd[3949]: <103063> <3949> <DBUG> |ike| 192.168.145.249:4500-> ike2_state.c (7792): errorCode = ERR_CERT_FAILED_VERIFY_ROOTCA Apr 20 17:14:50 2023 ArubaConductor-HW-1K certmgr[9191]: <118003> <9191> <DBUG> <ArubaConductor-HW-1K 192.168.100.250> type = 0, namestr = RootCA-RSA, fullname = /flash/certmgr/TrustedCA/RootCA-RSA tmpname = /tmp/certmgr/TrustedCA/RootCA-RSA, certfnamestr = ca-rsa.cert.pem Apr 20 17:15:48 2023 ArubaConductor-HW-1K <ArubaConductor-HW-1K 192.168.100.250> profmgr[9328]: USER:admin@192.168.1.130 NODE:"/mm/mynode" COMMAND:<crypto-local pki TrustedCA RootCA-RSA ca-rsa.cert.pem > -- command executed successfully		
FIA_X509_EXT.2	None	None
FIA_X509_EXT.3	None	None
FMT_MOF.1/Functions	None	None
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update.	None
May 15 06:10:01 2023 ArubaConductor-HW-1K <ArubaConductor-HW-1K 192.168.100.250> cli[11989]: USER:admin@0.0.0.0 NODE:"/mm/mynode" COMMAND:<copy scp: 10.100.100.100 root /srv/ftp/ArubaOS_MM_8.10.0.2-FIPS_84367 system: partition 1 > -- command executed successfully		
FMT_MTD.1/CoreData	None	None
FMT_MTD.1/CryptoKeys	None	None
FMT_SMF.1	All management activity of TSF Data	None
Feb 28 01:29:42 2023 cli[22014]: USER:admin@serial NODE:"/mm/mynode" COMMAND:<write mem> -- command executed successfully		
FMT_SMR.2	None	None
FPT_APW_EXT.1	None	None
FPT_SKP_EXT.1	None	None
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. See also application note on FPT_STM_EXT.1)	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).
Aug 26 10:28:58 2022 ArubaConductor-HW-1K < ArubaConductor-HW-1K 192.168.100.250> 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 2022 ArubaConductor-HW-1K < ArubaConductor-HW-1K 192.168.100.250> cli[18263]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<clock set 2020 august 26 10 28 58 > -- command executed successfully		
FPT_TST_EXT.1	None	None
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure).	
Jan 9 00:34:31 2023 upgradeImageNew: <399816> <7592> <ERRS> || Image Header Validation failed Jan 9 00:34:31 2023 upgradeImageNew: Image verification: Image header sign not found Feb 18 20:33:47 2023 cli[5877]: USER:admin@serial NODE:"/mm/mynode" COMMAND:<copy tftp: 192.168.144.253 C_ArubaOS_70xx_8.2.2.2-FIPS_69148 system: partition 0 > -- command executed successfully		
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None
May 19 15:50:57 2023 ArubaConductor-HW-1K <ArubaConductor-HW-1K 192.168.100.250> cli[13032]: USER: admin connected from 192.168.1.135 has logged out. Reason: Idle timeout Apr 20 16:03:20 2023 ArubaConductor-HW-1K <ArubaConductor-HW-1K 192.168.100.250> webui[9273]: TLS session with client 192.168.1.135 is terminated due to idle session time out.		
FTA_SSL.4	The termination of an interactive session.	None
Feb 28 02:26:52 2023 webui[3800]: USER: admin connected from 192.168.144.253 has logged out. Feb 28 02:57:47 2023 sshd[15323]: <199801> <15323> <INFO> |sshd| Close session: user admin from 192.168.144.253 port 51968 id 0		
FTA_SSL_EXT.1	(if 'lock the session' is selected) Any attempts at unlocking of an interactive session. (if 'terminate the session' is selected) The termination of a local session by the session locking mechanism.	None
Interactive: Feb 28 03:00:52 2023 webui[3800]: USER: admin has logged in from 192.168.144.253. Feb 28 03:05:49 2023 webui[3800]: USER: admin connected from 192.168.144.253 has timed out. Local: Feb 28 02:23:45 2023 cli[8023]: USER: admin has logged in using serial. Feb 28 02:24:42 2023 cli[8023]: USER: admin connected using serial has logged out. Reason: Idle timeout		
FTA_TAB.1	None	None

<table>
<tr><td>FTP_ITC.1</td><td>Initiation of the trusted channel.

Termination of the trusted channel.

Failure of the trusted channel functions.</td><td>Identification of the initiator and target of failed trusted channels establishment attempt.</td></tr>
<tr><td colspan="3">Initiation:

Oct 11 01:52:12 2022 isakmpd[3922]: <103076> <3922> <DBUG> |ike| IKEv2 IPSEC Tunnel created for peer 192.168.144.243:50750

Termination:

Feb 27 14:46:53 2023 isakmpd[3949]: <103102> <3949> <INFO> |ike| IKE SA deleted for peer 192.168.145.249

Failure:

Oct 11 01:36:37 2022 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</td></tr>
<tr><td>FTP_TRP.1/Admin</td><td>Initiation of the trusted path.

Termination of the trusted path.

Failure of the trusted path functions.</td><td>None</td></tr>
<tr><td colspan="3">Initiation:

Jul 28 11 01:59:46 2022 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

Feb 28 01:37:53 2023 webui[3800]: USER: admin has logged in from 192.168.144.253.

Termination:

Feb 27 10:52:23 2023 webui[3800]: USER: admin connected from 192.168.144.3 has timed out.

Feb 28 02:57:47 2023 sshd[15323]: <199801> <15323> <INFO> |sshd| Close session: user admin from 192.168.144.253 port 51968 id 0

Failure:</td></tr>
</table>

Jul 28 19:28:24 2022 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:

Jul 28 11 01:59:46 2022 sshd[7305]: <199801> <7305> <error> |sshd| Failed to refresh ssh public key authorized keys file

All Administrative actions are audited by the TOE. As noted within the Syslog Guide for 8.X (https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-c05321932), the Conductor 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 Conductor through the serial port, changed logging levels, loaded new software onto partition 1, then updated the system clock.

(host) #show audit-trail

Jul 4 21:53:54 2022 cli[1439]: USER:admin@serial COMMAND: -- command executed successfully

Jul 4 22:20:22 2022 cli[1439]: USER:admin@serial COMMAND: -- command executed successfully

Jul 4 22:31:00 2022 fpcli: USER:admin@10.240.104.135 COMMAND: -- command executed successfully

By default, the Conductor 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**.

A full record of audit records generated by the Conductor can be found at the following link:

https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/Command/Core_Download/Default.aspx?EntryId=32318

2.1.2 FAU_GEN.2

No configuration required.

2.1.3 FAU_STG_EXT.1

Local storage space for audit logs is limited on a Mobility Conductor. 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.

To configure an external syslog server:

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

The connection between the Mobility Conductor 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 Conductor) 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 Conductor to the syslog server.

2.2 Cryptographic Support (FCS)

2.2.1 FCS_CKM.1

No configuration required. Ensure the Conductor 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. Information on configuration X.509 can be found in Section 2.5.10 through Section 2.5.12.

2.2.2 FCS_CKM.2

No additional configuration is required. The TOE will use the correct algorithms when operated in FIPS mode.

2.2.3 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’. This command will overwrite the entire flash with an alternating pattern. The Conductor must be restored through TFTP after this process. In addition, files in the flash can be zeroized using the ‘write erase all’ command.

For further details on sanitizing systems, request the document “Identification of Non-Volatile Storage and Sanitization of System Components” from Aruba Networks.

2.2.4 FCS_COP.1

For FCS_COP.1/DataEncryption, FCS_COP.1/SigGen, FCS_COP.1/Hash, and FCS_COP.1/KeyedHash, the below information is applicable.

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

(config)# fips enable

2.2.5 FCS_HTTPS_EXT.1

No configuration is required. The TOE will function as an HTTPS server, compliant to RFC 2818, when operating under FIPS mode.

2.2.6 FCS_NTP_EXT.1

Mobility Conductors 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>

To remove any of the configured servers, the following command can be used:

(config) # no ntp server <IP address>

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.

The TOE supports the usage of NTPv4 by default. In addition to usage of the above CLI commands, 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.

The TOE must be configured to use NTP through IPsec. The Security Administrator should specify the interface used to communicate with the NTP server. This can be done under NTP using the 'source' command with arguments 'source <loopback>' or 'source <vlanid>'. 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.

2.2.7 FCS_IPSEC_EXT.1

2.2.7.1 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.

In the following configuration, ICMP echo-request traffic from Client A to Client C takes the BYPASS action. All other ICMP traffic between the same hosts takes the PROTECT action. HTTP traffic is dropped.

```
ip access-list route spd-test
  host <IP address> host <IP address> icmp echo forward
  host <IP address> host <IP address> svc-icmp  route ipsec-map <IP
address>
  host <IP address> host <IP address> svc-http  route tunnel 10
interface vlan <vlanid>
     ip address <IP address> <subnet>
     operstate up
     ip access-group "spd-test" in
!
```

Modify these rules as needed if explicit control over tunneled and non-tunneled traffic is needed. 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.

2.2.7.2 FCS_IPSEC_EXT.1.3

ArubaOS supports both 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
```

For additional assurance that only tunnel mode is used, the following command should be used under the crypto-local ipsec-map to force tunnel mode to be the only option offered..

```
  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 }
```

2.2.7.3 FCS_IPSEC_EXT.1.4

IPsec cipher suites are configured using transform-sets. These are ordered lists of ciphers - the Conductor 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.

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 }
```

Note: The TOE's IPsec ESP protocol implementation supports only HMAC-SHA-1. The IKE protocol supports HMAC-SHA-1, HMAC-SHA-256 and HMAC-SHA-384 (see FCS_IPSEC_EXT.1.6 below).

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 IPsec VPN clients (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-EP does not mandate the use of Perfect Forward Secrecy, it is a security best-practice. To enable PFS:

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

2.2.7.4 FCS_IPSEC_EXT.1.5

IKEv2 is supported for use in the evaluated configuration. NAT Traversal (NAT-T) is supported for both. NAT-T transports packets over UDP port 4500 rather than using IPsec native encapsulation.

For inbound connections where the Conductor 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
```

2.2.7.5 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)# version v2
```

To configure AES128, adjust the encryption to ‘encryption aes128’.

To configure HMAC-SHA-256 or HMAC-SHA-384, adjust the hash to ‘sha2-256-128’ or ‘sha2-384-192’.

2.2.7.6 FCS_IPSEC_EXT.1.7/8

Phase 1 (IKE) lifetimes are configured in the IKE policies. To adjust the 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
```

Phase 2 (IPsec) lifetimes are configured in the ipsec-map (for site-to-site):

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

or the dynamic-map (for client VPN):

```
(config) #crypto dynamic-map cc-required 1
(config-dynamic-map)#  set security-association lifetime seconds 28800
```

SA lifetimes may also be configured based on the number of bytes transmitted. Replace the keyword "seconds" with "kilobytes" in the above configuration and supply the lifetime value. Both time-based and volume-based lifetimes may be configured simultaneously.

2.2.7.7 FCS_IPSEC_EXT.1.9/10

No configuration required to meet these requirements.

2.2.7.8 FCS_IPSEC_EXT.1.11

ArubaOS supports DH groups 14, 19, and 20. To configure, modify the IKE policy:

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

2.2.7.9 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 Conductor for both authentication to peers and for verification of other peers is described in the User Guide. Minimally, both a "server certificate" and a "trusted root CA" certificate must be loaded onto the Conductor in order to perform IPsec operations. Once these certificates are loaded on the Conductor, configure them for use in IPsec. For use with dynamic VPN clients:

```
(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 Conductor will reject the security association along with generating an audit log message.

When the IPsec connection is configured to use pre-shared keys, the administrator can follow the following steps to configure a pre-shared key on the TOE:

To configure the key, pick one of the following options:

```
(config) #crypto-local isakmp key DEADBEEF01010202abc!@# address 0.0.0.0
netmask 0.0.0.0
```

When configuring the pre-shared key, the administrator must ensure that the PSK is between 6-160 characters, contains at least one uppercase character, one lowercase character, one special character, and one digit. If the PSK is configured as a bit-based key, the ‘key-hex’ field should be used instead.

```
(config) #crypto-local isakmp key-hex DEADBEEF01010202ABA010 address
0.0.0.0 netmask 0.0.0.0
```

2.2.7.10 FCS_IPSEC_EXT.1.14

The TOE does not support SAN extension.

To configure the TOE reference identifier for the distinguished name of the peer, an administrator may use the following commands:

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

To ensure appropriate compliance within the evaluated configuration, the administrator should generate a CA chain with one Root CA and two Intermediate CAs. The OCSP configuration and information on this can be found under Sections 2.3.6 and 2.3.7.

2.2.8 FCS_RBG_EXT.1

No configuration required.

2.2.9 FCS_SSHS_EXT.1

SSH access requires that you configure an IP address and a default gateway. No configuration is needed to specific the permitted algorithms after 'fips enable' has been set. The conductor will attempt negotiations using AES128-CBC, AES256-CBC, AES128-CTR, and AES256-CTR.

To ensure correct configuration, un-claimed macs and key exchange algorithms must be disabled, leaving only:

Hmac-sha1, Hmac-SHA2-256

ECDH-sha2-nistp256, ECDH-sha2-nisp384

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

```
show ssh
```

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

```
ssh disable_dsa
```

```
Ssh disable-kex dh
```

```
Ssh disable-mac hmac-sha1-96
```

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

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

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

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

Full instructions on how to upload a X.509-containerized public key for SSH authentication are included in the ArubaOS 8.10 User Guide.

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

The host key is generated at install time. To regenerate an SSH host key, the administrator must gain support access to the shell and manually do so, or zeroize the appliance.

Note: The TOE does not support the "none" MAC algorithm.

2.2.10 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 Conductor. The Conductor negotiates using the following ciphersuites:

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

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>
ciphers high
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 Identification and Authentication (FIA)

2.3.1 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
```

When an account has been locked out for a specified duration, the process of unlocking the account may take up to 60 seconds beyond the configured lockout period that has been configured.

To ensure Security Administrators cannot be fully locked out from the TOE, a password recovery account can be configured that can be accessed via local console only to reset a Security Administrator account that has been locked out from the TOE.

To disable the recovery account, the following command should be executed on the local console:

```
password-recovery-disable
```

In the evaluated configuration, the default recovery account should be disabled.

2.3.2 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
```

The following special characters can be used when configuring passwords: `, ~, !, @, #, $, %, ^, &, *, (,), -, _, =, +, [,], {, }, \, |, ;, :, ‘, “, comma, <, >, period, /

Once configured, the TOE only permits the use of strong passwords.

2.3.3 FIA_UAU.7

No configuration is necessary to obscure feedback of passwords during login. Nothing will be echoed back on the console. For the web UI, the password characters will be represented by black dots.

2.3.4 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:
```

2.3.5 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
=
```

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
```

For configuration of the TOE login banner through the WebUI, the administrator should navigate to Configuration > System > Admin > Admin Authentication Options > Login banner text.

The TOE permits authentication by an administrator through SSH or Web UI over TLS. 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.

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 is directly via the serial console port only.

2.3.6 FIA_X509_EXT.1/2

Certificate Signing Requests (CSRs) may be generated by the Conductor. This process is described in the ArubaOS User Guide. Best practice is to generate the CSR on the Conductor, 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 Conductor can also accept a certificate/key combination in the form of a PKCS#12 file.

In the evaluated configuration, ArubaOS supports certificate revocation checking using OCSP. OCSP is the recommended method of revocation checking.

When a root CA or intermediate CA certificate is loaded on the Conductor, 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 may be set to none, crl, or ocsp. When OCSP has been specified, then an OCSP responder URL and OCSP responder certificate must be specified. In the evaluated configuration, the TOE does not accept certificates if an OCSP responder is unreachable.

For the purpose of verifying 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 Conductor through the WebUI Certificate Management section, and its name configured in the relevant RCP. When used, the Conductor 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 Conductor, 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.

For client VPN: ArubaOS will extract the User Principal Name field from the client certificate, and will pass it through an authentication/authorization process when this functionality has been enabled. Configuring authentication servers is described in the ArubaOS User Guide. VIA clients will be authenticated according to configuration found under "`aaa authentication via auth-profile`". Third-party VPN clients will be authenticated according to configuration found under "`aaa authentication vpn`". Both types of profiles are configured in a similar way. The following configuration allows the Conductor to perform authentication for VIA clients against a RADIUS server. After a client certificate has been validated, including revocation checking, the Conductor will pass the User Principal Name to a configured RADIUS server using an "authorize-only" transaction.

```
(config) #aaa authentication via auth-profile VIA_CERT_AUTH
(VIA Authentication Profile "VIA_CERT_AUTH") #cert-cn-lookup
(VIA Authentication Profile "VIA_CERT_AUTH") #server-group CPPM_CLUSTER
```

If authentication is not desired, set "cert-cn-lookup" to disabled.

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.

2.3.7 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.

When signing the certificate request, the RSA certificates for the TOE (and the peer) must be signed with sha1WithRSAEncryption.

2.4 Security Management (FMT)

2.4.1 FMT_MOF.1/ManualUpdate

See FPT_TUD_EXT.1 for information. No configuration is required to restrict updates to administrator role. Updates for the TOE should be performed through the CLI (SSH or Local Console).

2.4.2 FMT_MOF.1/Functions

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

2.4.3 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.

The trust anchor can be either self-signed or custom certificates installed on the Mobility Conductor. Full details on how the Security Administrator can configure CA certificates as the trust store can be found in the ArubaOS 8.x User Guide chapter *Management Access*, particularly the section regarding Managing Certificates.

Details on how to use the *set-trust-anchor* command are available in the ArubaOS 8.X CLI Reference Guide. To use a specific CA on the managing conductor, this must be enabled on the AP.

2.4.4 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.

2.4.5 FMT_SMF.1

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

2.4.6 FMT_SMR.2

No additional configuration required.

2.5 Protection of the TSF (FPT)

2.5.1 FPT_APW_EXT.1

No additional configuration required.

2.5.2 FPT_SKP_EXT.1

No additional configuration required.

2.5.3 FPT_STM_EXT.1

Mobility Conductors 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>
```

More NTP options, including authentication, are available. See the ArubaOS User Guide for more information.

The administrator must ensure the connection to the time server is secured with IPsec.

The TOE, by default, does not accept broadcast and multicast NTP packets.

2.5.4 FPT_TST_EXT.1

No configuration required.

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 Conductor 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 Conductor 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.

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

2.5.5 FPT_TUD_EXT.1

Use the command “show version” to view the active version and “show image version” to view the active version and loaded but inactive version.

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.

ArubaOS images are integrity-protected through two evaluated methods:

1. ArubaOS images are digitally signed using RSA 2048-bit signature validation. The Mobility Conductor 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 Conductors also check the digital signature of an ArubaOS image when booting. The Conductor will refuse to boot a corrupted ArubaOS image file.

No configuration is needed to achieve this requirement.

If the digital signature verification succeeds, the TOE console will note that the signature has been verified and note that the integrity check on the partition is '[OK]' (Passed). The TOE will continue through initial power on self-tests and after successful completion prompt for authentication.

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.

2.6 TOE Access (FTA)

2.6.1 FTA_SSL.3

For remote administrative sessions, an idle timeout may be set to disconnect idle sessions. The default value is 300 seconds (5 minutes). To configure the timer value, use the following:

For the SSH CLI:

```
(config) #loginsession timeout <value> sec
```

In the above command, <value> can be any number of seconds from 30 to 3600, inclusive. Additionally, the administrator can choose to configure the value from 1-60 minutes by excluding the 'seconds' parameter:

```
(config) #loginsession timeout <value>
```

```
Following configuration of the timeout command, the security
administrator should enter the following command to ensure the
configuration takes effect:
```

```
(config) #write memory
```

.

For the WebUI:

```
(config) #web-server profile
```

```
(Web server configuration) #session-timeout <val>
```

In the above command, <val> can be any number of seconds from 30 to 3600, inclusive.

In addition to the CLI, the administrator can configure the WebUI Idle Session timeout by navigating to Configuration > System > Admin >Admin Authentication Options. This parameter can be configured as either seconds or minutes (1-60 minutes, or 30-3600 seconds).

2.6.2 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 2.6.1 above.

To logout from the CLI, an administrator can just enter the 'exit' command. In order to logout from the WebUI session, the administrator should select their username in the top right corner and 'log out' from the dropdown menu.

2.6.3 FTA_SSL_EXT.1

For local administrative sessions, an idle timeout may be set to disconnect idle sessions. The default value is 300 seconds (5 minutes).

To configure the timer value, use the following at the CLI:

```
(config) #loginsession timeout <value> sec
```

In the above command, <value> can be any number of seconds from 30 to 3600, inclusive. Additionally, the administrator can choose to configure the value from 1-60 minutes by excluding the 'seconds' parameter:

```
(config) #loginsession timeout <value>
```

```
Following configuration of the timeout command, the security administrator should enter the following command to ensure the configuration takes effect:(config) #write memory
```

2.6.4 FTA_TAB.1

See FIA_UIA_EXT.1 above for a description of how to configure a notice and consent banner message.

2.7 Trusted Path/Channels (FTP)

2.7.1 FTP_ITC.1

ArubaOS supports IPsec as the inter-TSF trusted channel. This channel is to be used between a Mobility Conductors and a) a syslog server, b) an authentication server (RADIUS or TACACS+), c) NTPv4 server and d) VPN Gateway/Mobility Controller.

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

2.7.2 FTP_TRP.1/Admin

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

To access the SSH CLI interface:

1. Initialize the SSH client
2. For the hostname, specify the TOE IP and port 22.
3. Begin session establishment.
4. The administrator will be prompted for username and password/public key upon establishing a successful connection.

To access the local serial interface:

1. Configure the terminal or terminal emulation program to use the following communication settings: Baud: 9600, Data Bits: 8, Parity: None, Stop Bits: 1, Flow Control: None
2. Connect the terminal or PC/workstation to the serial port on the devices using an RS-232 serial cable. RJ-45 cable and DB-9 to RJ-45 adapter is required. The administrator may need a USB adapter to connect the serial cable to the PC.
3. After the connection initialized, the administrator will be able to continue through the CLI after entering valid credentials.

To access the WebUI, the administrator should navigate to their approved web browser and connect to https://<TOEIP:PORT> or the specified FQDN. Once connected, the administrator must authenticate to the device before proceeding with any further access requests.

The following browsers are officially supported for use with the ArubaOS WebUI:

- Microsoft Internet Explorer 11 on Windows 7 and Windows 8
- Microsoft Edge (Microsoft Edge 92.0.902.62 and Microsoft EdgeHTML 18.19041) on Windows 10
- Firefox (91.0) on Windows 7, Windows 8, Windows 10, and macOS
- Apple Safari 8.0 or later on macOS
- Google Chrome (92.0.4515.131) on Windows 7, Windows 8, Windows 10, and macOS

3 Reference Documents

The ArubaOS 8.10 user guide can be found in its entirety here:
https://www.arubanetworks.com/techdocs/ArubaOS-8.x-Books/810/ArubaOS-8.10.0.0-User-Guide.pdf

The ArubaOS 8.x CLI Reference Guide can be found in its entirety here:
ArubaOS 8.x CLI Reference Guide (arubanetworks.com)

These guides cover all ArubaOS platforms, such as Conductor, Controller, and APs.

The installation guide for Mobility Conductors can be located at:
Mobility Conductor Appliance Installation Guide (hpe.com)