CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR ARUBA MOBILITY CONTROLLER AND ACCESS POINT SERIES

Maintenance Update of Aruba Mobility Controller and Access Point Series, (ArubaOS version 6.4.3.0-FIPS)

Maintenance Report Number: CCEVS-VR-VID10569-2015

Date of Activity: 2 June 2015

References: Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0, 8 September 2008;

Aruba Mobility Controller and Access Point Series Impact Analysis Report Revision 1.0, March 26, 2015.

Documentation Updated: (List all documentation updated)

Security Target: Aruba Mobility Controller and Access Point Series Security Target, Version 1.1, 03/18/2015. Changes in the Security Target are:

- Updated identification of ST and maintained TOE.
- Additional appliance models.
- Updated list of features that are excluded from the evaluated configuration
- Updated CAVP and CMVP certification numbers to match the maintained TOE.
- Updated list the guidance documents.

Guidance Documentation: Changes in the maintained guidance documentation cover new features and feature modifications including bug fixes.

- ArubaOS 6.4.x User Guide, March 2015
- ArubaOS 6.3.x Command-Line Interface Reference Guide, October 2013
- ArubaOS 6.3.x Syslog Messages Reference Guide, July 2013
- ArubaOS 6.3 Quick Start Guide, May 2012
- ArubaOS 6.x MIB Reference Guide, June 2013.

Regression Tests: Aruba Mobility Controller and Access Point Series Common Criteria Regression Test Report, Version 1.0, Dated: 26 March 2015

Assurance Continuity Maintenance Report:

Leidos CCTL submitted an Impact Analysis Report (IAR) for Aruba to the CCEVS for approval in March 2015 and provided an updated package in April 2015. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated as a result of the changes and the security impact of the changes.

Changes to TOE:

Aruba Networks has revised the firmware OS in their hardware appliances and has added support for twelve new appliance models. Changes are summarized below:

- Aruba Networks has revised the firmware OS in their hardware appliances from ArubaOS version 6.3.1.5-FIPS to ArubaOS version 6.4.3.0-FIPS,
- The following appliance models was added to the TOE:
  - Aruba Mobility Controllers: Aruba 7005, 7010, 7024, 7030, 7205
  - Aruba Access Points: Aruba AP-204, AP-205, AP-214, AP-215, AP-274, AP-275, AP-277
- The functionality of the new models remains the same as prior models. The differences in the models include the number of ports, interfaces, throughput and processing speed, memory and storage. Although these models have different specifications (in terms of performance and capabilities), they all provide the same security functions described in the ST; therefore, they have been considered to be the same for the purposes of the ST description. There is no difference between the products and the TOE. Since the TOE is a WLAN access system, the physical boundary of each product that comprises the WLAN is the hard steel or plastic encasing.
- All appliance models have been FIPS 140-2 validated with ArubaOS version 6.4.3.0-FIPS and the certificate numbers are included in the updated Security Target.

Equivalency Discussion

The changes made to the TOE devices do not impact the functionality required under the WLAN PP. The addition of a USB is not claimed under the original SFRs or part of any SFRs in the PP, thus it would not impact the scope of the evaluation.

No functionality defined in the SFRs was impacted by the software update. As described in Section 1.1 of the Security Target, all devices run the same firmware version of ArubaOS and require the same licenses, which grant them the same functionality.

Please see the following documents:
http://www.arubanetworks.com/pdf/products/DS_7200Series.pdf
http://www.arubanetworks.com/pdf/products/matrix-mobility-controller.pdf
http://www.arubanetworks.com/pdf/products/DS_A620.pdf

http://www.arubanetworks.com/pdf/products/DS_A650651.pdf
http://www.arubanetworks.com/pdf/products/MAT_AP.pdf

As described in the guidance documents referenced above, the only differences between the devices are maximum APs, concurrent users, concurrent firewall sessions, concurrent IPSec sessions, throughput, power consumption, box dimensions, management ports (whether management through serial or serial-through-usb), power options, and gigabit port count. The tables below provide a detailed comparison of the devices, showing their equivalency.

Mobility Controller Equivalency

Mobility Controllers	Software Image	Maximum APs	Maximum RAPs	USB Connectivity	LCD Panel	Console Connectivity	Status LEDs	Ethernet Connectivity
620	6.4.3.0	8	8	1	No	Yes	Yes	Yes
650	6.4.3.0	16	16	4	No	Yes	Yes	Yes
3200	6.4.3.0	32	128	0	No	Yes	Yes	Yes
3400	6.4.3.0	64	256	0	No	Yes	Yes	Yes
3600	6.4.3.0	128	512	0	No	Yes	Yes	Yes
6000	6.4.3.0	128	1024	0	No	Yes	Yes	Yes
7005	6.4.3.0	16	16	1	Yes	Yes	Yes	Yes
7010	6.4.3.0	32	32	2	Yes	Yes	Yes	Yes
7024	6.4.3.0	32	32	1	Yes	Yes	Yes	Yes
7030	6.4.3.0	64	64	1	Yes	Yes	Yes	Yes
7205	6.4.3.0	256	256	1	Yes	Yes	Yes	Yes
7210	6.4.3.0	512	512	1	Yes	Yes	Yes	Yes
7220	6.4.3.0	1024	1024	1	Yes	Yes	Yes	Yes
7240	6.4.3.0	2048	2048	1	Yes	Yes	Yes	Yes

As shown in the table below, the only variation outside of performance functionality is the USB Port. The USB however only provides another method for upgrading the TOE directly on the box or connecting storage. This is ***not*** a feature claimed under the Protection Profile and is out of scope for testing. Updates were not performed using this functionality and do not impact the TOEs ability to implement a new update. Additionally, the LCD Panel is out-of-scope as well and does not fall under the scope of evaluation.

The key area of equivalency is for the functionality provided by the operating system and in this case, all devices run the same version of Aruba OS 6.4.3.0 and provide the same required functionality as documented under the protection profile.

Access Point Equivalency

Access Point	Software Image	Wi-Fi Standards	Radio Bands	Ethernet Connectivity	Console Connectivity
AP-92/93	6.4.3.0	802.11a/b/g/n	2.4GHz/5GHz	One	Yes
AP-104/105	6.4.3.0	802.11a/b/g/n	2.4GHz/5GHz	One	Yes
AP-114/115	6.4.3.0	802.11a/b/g/n	2.4GHz/5GHz	One	Yes
AP-134/135	6.4.3.0	802.11a/b/g/n	2.4GHz/5GHz	Two	Yes
AP-175	6.4.3.0	802.11a/b/g/n	2.4GHz/5GHz	One	Yes
AP-204/205	6.4.3.0	802.11a/b/g/n/ac	2.4GHz/5GHz	One	Yes
AP-214/215	6.4.3.0	802.11a/b/g/n/ac	2.4GHz/5GHz	One	Yes
AP-224/225	6.4.3.0	802.11a/b/g/n/ac	2.4GHz/5GHz	Two	Yes
AP-274/275	6.4.3.0	802.11a/b/g/n/ac	2.4GHz/5GHz	Two	Yes
AP-277	6.4.3.0	802.11a/b/g/n/ac	2.4GHz/5GHz	One	Yes
RAP-3WN	6.4.3.0	802.11	2.4GHz/5GHz	Three	Yes
RAP-5WN	6.4.3.0	802.11a/b/g/n	2.4GHz/5GHz	Five	Yes
RAP-108/109	6.4.3.0	802.11	2.4GHz/5GHz	Two	Yes
RAP-155	6.4.3.0	802.11	2.4GHz/5GHz	Five	Yes

As shown in the table above, the device functionality in respect to the Protection Profile is equivalent. All provide console connectivity, all run on the same Software Image, and all share the same necessary Wi-Fi Standards. The number of interfaces and support between radio bands is not a requirement of the PP. The necessary functionality is provided by each access point to provide connectivity to the Mobility Controllers in order to meet the requirements defined in the PP.

Summary of Product Changes:

The ArubaOS 6.4.3.0-FIPS updates represent a number of bug fixes as well as some new features, some of which are security related and are not included in the scope of this evaluation. There are also some minor appearance changes as well as other optimizations. For detailed information on the new features listed below, see the guidance documentation listed at the beginning of the report.

The following new features were added to the ArubaOS 6.4.3.0-FIPS:

- Support for the AP-205H Access Point, reflected in the Security Target.
- Support for the AP-228 Access Point, which is not included in the TOE.
- Support for the AP-277 Access Point, reflected in the Security Target.
- Warning Message for Containment Features, which does not affect the TOE.
- ARM - Anyspot Client Probe Suppression, which is a performance enhancement that does not affect the security functionality of the TOE.
- Branch Controller - Per-Interface Bandwidth Contracts, which does not affect the security functionality of the TOE.
- Branch Controller - Monitor WAN Health, which does not affect the security functionality of the TOE.
- Branch Controller - Uplink Routing using Next-Hop Lists, which does not affect the security functionality of the TOE.
- Branch Controller - Policy-Based Routing, which does not affect the security functionality of the TOE.
- Client Match - BSS Transition Management Support, which does not affect the security functionality of the TOE.
- Client Match - Multi-Media Sync-Up RT-1127, which does not affect the security functionality of the TOE.
- Client Match - Removing VBR Dependency on Probe Requests, which does not affect the security functionality of the TOE.
- Controller-Platform - 7024 Controller, reflected in the Security Target.
- Controller-Platform - 7205 Controller, reflected in the Security Target.
- AMON Message Size Changes on the Controller, which does not affect the security functionality of the TOE.
- Flexible Licensing for AP Controllers, which does not affect the security functionality of the TOE.
- Modem Support on 7000 Series Controllers, which does not affect the security functionality of the TOE.
- Username and Password Protection for the AP Console, which is not relevant to the security functionality of the TOE, given the operational environment defined physical protection.

- PhoneHome-Lite, which is specifically disabled in the evaluated configuration and is therefore not relevant to the TOE.
- Voice and Video - UCC Score for Lync Media Classification, which does not affect the security functionality of the TOE.
- Lync SDN API 2.1 Support, which does not affect the security functionality of the TOE.

The following new features were added to ArubaOS 6.4.2.4:

- USB Storage for CSR and Key Files, which does not affect the security functionality of the TOE.
- SFP/SFP+ modules, which do not affect the security functionality of the TOE.
- Modified Command show dotlx watermark, which does not affect the security functionality of the TOE.

The following new features were added to ArubaOS 6.4.2.3:

- AP-2xx Series High Density Optimization, which does not affect the security functionality of the TOE.
- L2 GRE Tunnel Group, which does not affect the security functionality of the TOE.
- MLD Snooping, which does not affect the security functionality of the TOE.
- New and modified Commands, which do not affect the security functionality of the TOE, including:
    - Show web-server statistics
    - ids-general-profile,
    - show web-server profile
    - web-server profile

- Clients exclusively using SSLv3 will fail to access the Captive Portal or the controller WebUI. Although this change is security relevant, it does not affect the does not affect the security of the product or modify any SFRs. SSL was not permitted in the previous evaluation, only the use of the [TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), and TLS 1.2 (RFC 5246)] protocols.

The following features were added to ArubaOS 6.4.2.2:

- Username Length Restriction, which restricts the maximum length of the controller management (SSH) username and password to 64 and 32 characters respectively. This command is security related, however, change does not affect the security of the product or modify any SFRs. The FIA_PMG_EXT.1.1 SFR requires a minimum password length shall be settable by the Authorized Administrator, and support passwords of 8 characters or greater.

The following features were added to ArubaOS 6.4.2.1:

- AP Power Mode on AP-220 Series, which does not affect the security functionality of the TOE.

The following features were added to ArubaOS 6.4.2.0:

- Support for the AP-210 Series, which is reflected in the Security Target.
- Enhanced Link Aggregation Support on AP-220 Series and AP-270 Series Access Points, which does not affect the security functionality of the TOE.
- Netgear AirCard 340U USB Modem Support, which does not affect the security functionality of the TOE.
- Netgear AirCard 341U USB Modem Support, which does not affect the security functionality of the TOE.
- VHT Support on AP-200 Series, AP-210 Series, AP-220 Series, and AP-270 Series Access Points, which does not affect the security functionality of the TOE.
- Channel 144 in Regulatory Domain Profile, which does not affect the security functionality of the TOE.
- Kernel Core Dump Enhancement, which does not affect the security functionality of the TOE.
- Web Content Classification, which is outside the scope of evaluation and its addition is not security relevant.
- RTLS Station Message Frequency, which is outside the scope of evaluation and its addition is not security relevant.
- Video Multicast Rate Optimization, which does not affect the security functionality of the TOE.

The following features were added to ArubaOS 6.4.1.0:

- Support for AP-103H, which is outside the scope of evaluation.
- Support for AP-200 Series, which is included in the Security Target.
- Downloadable Regulatory Table, which does not affect the security functionality of the TOE.
- 7000 Series Controllers, which is included in the Security Target.
- AirGroup, which does not affect the security functionality of the TOE.
- AP Fast Failover Support for Bridge-mode Virtual AP, which does not affect the security functionality of the TOE.
- DHCP Lease Limit on 7000 Series Controllers, which does not affect the security functionality of the TOE.
- Selective Multicast Stream, which does not affect the security functionality of the TOE.
- Authentication Profile based User Idle Timeout extends the existing range of available timeout values by one value. The modified implementation still satisfies FTA_SSL.3. Aruba updated ST section 6.8 and CLI Guide aaa profile to include the extended range. Regression testing confirmed the TOE behaves as specified for both the new value and the old range.

- Global Firewall Parameters, which is outside the scope of the evaluation and its addition is not security relevant.

The following features were added to ArubaOS 6.4.0.2:

- ArubaOS-AirWave Cross-Site Request Forgery Mitigation, which is outside the scope of the evaluation and its addition is not security relevant.
- EAP-MD5 Support, which is outside the scope of the evaluation.

The following features were added to ArubaOS 6.4.0.1:

- PhoneHome Reporting Enhancements, which is disabled in the evaluated configuration and is therefore outside the scope of the evaluation.

The following features were added to ArubaOS 6.4.0.0:

- Support for the AP-270 Series, which is included in the Security Target.
- Support for the AP-103, which is outside the scope of the evaluation.
- Hotspot 2.0, which is disabled in the evaluated configuration and is therefore outside the scope of the evaluation.
- AP-220 Series Enhancements, which does not affect the security functionality of the TOE.
- AP-130 Series Functionality Improvements when Powered Over 802.3af (POE), which is outside the scope of the evaluation.
- Franklin Wireless U770 4G Modem Support, which does not affect the security functionality of the TOE.
- Huawei E3276 LTE Modem Support, which does not affect the security functionality of the TOE.
- Authentication Server Limits, which does not affect the security functionality of the TOE.
- EAP-MD5 Support, which is outside the scope of the evaluation.
- AirGroup Default Behavior Changes, which does not affect the security functionality of the TOE.

The following features were added to ArubaOS 6.4:

- Additional AirGroup features, which did not affect the security functionality of the TOE.
- IPv6 features for performance and operational functionality, which did not affect the security functionality of the TOE.
- Palo Alto Networks Firewall Integration, which does not affect the security functionality of the TOE.
- Application Single Sign-On Using L2 Network Information, which is outside the scope of the evaluation.
- 802.11w Support, which is outside the scope of the evaluation.
- Ability to Disable Factory-Default IKE/IPsec Profiles, which does not affect the security

functionality of the TOE.

- AOS/ClearPass Guest Login URL Hash, which is disabled in the evaluated configuration and is therefore outside the scope of the evaluation.
- Authentication Server Load Balancing, which does not affect the security functionality of the TOE.
- Enhancements in the User Authentication Failure Traps, which is outside the scope of the evaluation.
- RADIUS Accounting on Multiple Servers, which is outside the scope of the evaluation.
- RADIUS Accounting for VIA and VPN Users, which is outside the scope of the evaluation.
- AP Platform Support for Spectrum Analysis, which is outside the scope of the evaluation.
- Voice and Video, which does not affect the security functionality of the TOE.
- MIB and Trap Enhancements, which does not affect the security functionality of the TOE.

The following features were added to ArubaOS 6.3.1.14:

- Addressing CVE-2014-3566 SSL vulnerability, which does not affect the security functionality of the TOE because SSL is excluded from the evaluation.

The following features were added to ArubaOS 6.3.1.13:

- UML295 Support, which does not affect the security functionality of the TOE.

The following features were added to ArubaOS 6.3.1.11:

- The ap-power-mode parameter under ap provisioning-profile is renamed to ap-poe-power-optimization, which does not affect the security functionality of the TOE..

The following features were added to ArubaOS 6.3.1.10:

- AP Power Mode on AP-220 Series, which does not affect the security functionality of the TOE.

The following features were added to ArubaOS 6.3.1.9:

- Channel 144 in Regulatory Domain Profile, which does not affect the security functionality of the TOE.
- Command show ap debug system-status was modified, which does not affect the security functionality of the TOE.

The following features were added to ArubaOS 6.3.1.7:

- ARM 3.0 Enhancements, which does not affect the security functionality of the TOE.
- Support for 340U and 341U Modems, which is outside the scope of the evaluation.
- Support of Multicast Rate, which does not affect the security functionality of the TOE.
- Commands firewall attack-rate and user-role were modified with no changes to security functionality.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security, and found the changes to be minor. Therefore, CCEVS agrees that the original assurance is maintained for the above-cited version of the product.