MARCH2016

Aruba Mobility Controller with Aruba OS 6.4.3.4-FIPS

Product Description

The Aruba Mobility Controller (MC) is a network device that serves as a gateway between wired and wireless network and provides command and control over Access Points (APs) within a wireless network. Aruba OS 6.4.3.4-FIPS is the underlying operating system of the MC.

Evaluation Scope

The scope of the ASD Cryptographic Evaluation (ACE) included the following functionality:

- Authentication
- Data confidentiality
- Data integrity

Common Criteria Certification – Summary

The product was found to meet the requirements of the Australian Signals Directorate approved Network Devices Protection Profile (NDPP) v1.1.

ASD Findings and Recommendations

ASD performed a cryptographic evaluation on the product in addition to the Common Criteria evaluation.

As the product has successfully completed an ACE, it can be used to downgrade the requirements of PROTECTED data in transit to those of UNCLASSIFIED, in accordance with the Australian Government Information Security Manual (ISM).

When choosing wireless products, agencies should be aware that the security of any WPA2 Enterprise wireless network is dependent on each of the network components and how they interact with each other. WPA2 Enterprise wireless networks typically comprise of three main elements:

- Supplicant software: software that supports the 802.1X protocol, and is therefore able to authenticate to a wireless Access Point (AP) or Ethernet switch.
- Wireless LAN Controllers and Wireless Access Points: devices that relay data between the supplicant software and the RADIUS server.
- RADIUS servers: back-end management servers used for authentication, authorisation and accounting purposes.

Agencies using Aruba MC as part of a PROTECTED wireless network MUST adhere to the following recommendations:

1. The Aruba MC product must be used in conjunction with supplicant software that has successfully completed an ACE.
2. Devices running supplicant software take on the classification of the network they are connected to and MUST be protected accordingly.
3. The Aruba MC-to-RADIUS connection MUST be either:
    i) Provided via a wired link that has been accredited to communicate data classified at the same level of the wireless network, or
    ii) Be encapsulated with an additional layer of encryption (on top of the RADIUS encapsulation). *Note: if this option is used, network encryption products (e.g. IPsec or SSL VPN products) that have successfully completed an ACE MUST be used to provide the additional layer of encryption.*
4. Agencies MUST use WPA2 in Enterprise mode.

5. Agencies MUST use AES-CCMP for data confidentiality and integrity of all wireless network traffic.
6. Mutual authentication MUST be performed via EAP-TLS with X.509 certificates for both supplicant and Aruba MC authentication.
7. Certificates for both a device and user accessing a wireless network MUST NOT be stored on the same device.
8. Agencies MUST use a certificate authority product or Hardware Security Module (HSM) that has completed an ACE to generate X.509 certificates.
9. Certificates used to grant access to a classified network take on the classification of the network and MUST be protected accordingly.
10. Agencies using the Aruba MC as part of an UNCLASSIFIED wireless network SHOULD refer to the Wireless Local Area Network section within the ISM.

Recommendations given in this Consumer Guide take precedence over those in the ISM where there is a conflict.

Contact Details

Australian government customers with questions regarding this advice should contact ASD Advice and Assistance at asd.assist@defence.gov.au or by calling 1300 CYBER1 (1300 292 371).

ISM

The advice given in this document is in accordance with the Information Security Manual 2015. Australian government agencies are reminded to periodically check the latest release date of the ISM at www.asd.gov.au/infosec/ism/

Consumer Guide

This Consumer Guide was issued by ASD during March 2016.