National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

VMware AirWatch Mobile Device Management v9.1

Report Number: CCEVS-VR-VID10733-2017
Version 1.0
January 9, 2017

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Sheldon Durrant, Lead Validator
MITRE

Jerome Myers, Senior Validator
Aerospace Corporation

Common Criteria Testing Laboratory

Christopher Gugel, CC Technical Director
Bradley Isbell
Christopher Rakaczky

Booz Allen Hamilton (BAH)
Annapolis Junction, Maryland

Table of Contents

1 EXECUTIVE SUMMARY 4
2 IDENTIFICATION 5
3 ASSUMPTIONS AND CLARIFICATION OF SCOPE 6
4 ARCHITECTURAL INFORMATION 8
5 SECURITY POLICY 11
6 DOCUMENTATION 15
7 EVALUATED CONFIGURATION 16
8 IT PRODUCT TESTING 17
9 RESULTS OF THE EVALUATION 19
10 VALIDATOR COMMENTS 21
11 ANNEXES 22
12 SECURITY TARGET 23
13 LIST OF ACRONYMS 24
14 TERMINOLOGY 25
15 BIBLIOGRAPHY 26

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of VMware AirWatch Mobile Device Management v9.1 provided by VMware, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Booz Allen Hamilton, Inc. Common Criteria Testing Laboratory (CCTL) in Annapolis Junction, Maryland, United States of America, and was completed in January 2017. The information in this report is largely derived from the Evaluation Technical Report (ETR), Assurance Activity Report (AAR), and associated test reports, all written by Booz Allen. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements set forth in the Protection Profile for Mobile Device Management, version 2.0 (MDMPP) and Extended Package for Mobile Device Management Agents, version 2.0 (MDMAPP).

The Target of Evaluation (TOE) is the VMware AirWatch Mobile Device Management version 9.1 comprising the VMware AirWatch MDM Server 9.1, and VMware AirWatch MDM Agent version 9.1. The physical boundary for the TOE is VMware AirWatch MDM Server (including MAS) installed on Microsoft Windows 2012 R2 and the VMware AirWatch MDM Agent installed on an Apple iOS 9 or 10 device.

The TOE identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4), as interpreted by the Assurance Activities contained in the MDMPP and MDMAPP documents. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report is consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes, and reviewed the individual work units of the ETR and AAR for the MDMPP and MDMAPP Evaluation Activities and CEM work units. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory’s findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the *VMware AirWatch Mobile Device Management Security Target, Version 1.0*, dated December 27, 2016 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profiles containing Assurance Activities, which are interpretations of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliance List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1 – Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	VMware AirWatch Mobile Device Management version 9.1 comprising the VMware AirWatch MDM Server 9.1, and VMware AirWatch MDM Agent version 9.1
Protection Profile	Protection Profile for Mobile Device Management, version 2.0 Extended Package for Mobile Device Management Agents, version 2.0 (including all applicable NIAP Technical Decisions)
Security Target	VMware AirWatch Mobile Device Management Security Target, Version 1.0, dated December 27, 2016
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "VMware AirWatch Mobile Device Management" Evaluation Technical Report v1.0 dated January 9, 2017
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	VMware, Inc.
Developer	VMware, Inc.
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Annapolis Junction, Maryland
CCEVS Validators	Sheldon Durrant, MITRE Jerome Myers, Aerospace Corporation

3 Assumptions and Clarification of Scope

3.1 Assumptions

The following assumptions about the operational environment are made regarding its ability to provide security functionality.

- The TOE relies on network connectivity to carry out its management activities. The TOE will robustly handle instances when connectivity is unavailable or unreliable.
- The MDM Server relies upon a trustworthy platform and local network from which it provides administrative capabilities. The MDM server relies on the this platform to provide a range of security-related services including reliable timestamps, user and group account management, logon and logout services via a local or network directory service, remote access control, and audit log management services to include offloading of audit logs to other servers. The platform is expected to be configured specifically to provide MDM services, employing features such as a host-based firewall, which limits its network role to providing MDM functionality.
- One or more competent, trusted personnel who are not careless, willfully negligent, or hostile, are assigned and authorized as the TOE Administrators, and do so using and abiding by guidance documentation.
- Mobile device users are not willfully negligent or hostile, and use the device within compliance of a reasonable Enterprise security policy.
- The MDM Agent relies upon Mobile platform and hardware evaluated against the MDFPP and assured to provide policy enforcement as well as cryptographic services and data protection. The Mobile platform provides trusted updates and software integrity verification of the MDM Agent.

3.2 Threats

The following lists the threats addressed by the TOE.

- **T.MALICIOUS_APPS –** An administrator of the MDM or mobile device user may inadvertently import malicious code, or an attacker may insert malicious code into the TOE or OE, resulting in the compromise of TOE or TOE data.
- **T.NETWORK_ATTACK –** An attacker may masquerade as MDM Server and attempt to compromise the integrity of the mobile device by sending malicious management commands.
- **T.NETWORK_EAVESDROP –** Unauthorized entities may intercept communications between the MDM and mobile devices to monitor, gain access to, disclose, or alter remote management commands. Unauthorized entities may intercept unprotected wireless communications between the mobile device and the Enterprise to monitor, gain access to, disclose, or alter TOE data.
- **T.PHYSICAL_ACCESS –** The mobile device may be lost or stolen, and an unauthorized individual may attempt to access OE data.

3.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the Protection Profile for Mobile Device Management, version 2.0 and Extended Package for Mobile Device Management Agents, version 2.0, including all relevant NIAP Technical Decisions. A subset of the “optional” and “selection-based” security requirements defined in the MDMPP and MDMAPP are claimed by the TOE and documented in the ST.

- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not “obvious” or vulnerabilities to security functionality not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. All other functionality provided by the devices needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

The evaluated configuration of the TOE is comprised of two MDM Server components and an MDM Agent component. Two MDM Server components exist because the evaluated configuration of the TOE is to deploy it in an on-premises configuration, which requires a secondary instance of the MDM Server residing outside the organization’s firewall in a demilitarized zone (DMZ) where it is exposed to external network traffic from the internet. The TOE includes all the code that enforces the functions identified (see Section 5).

4 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

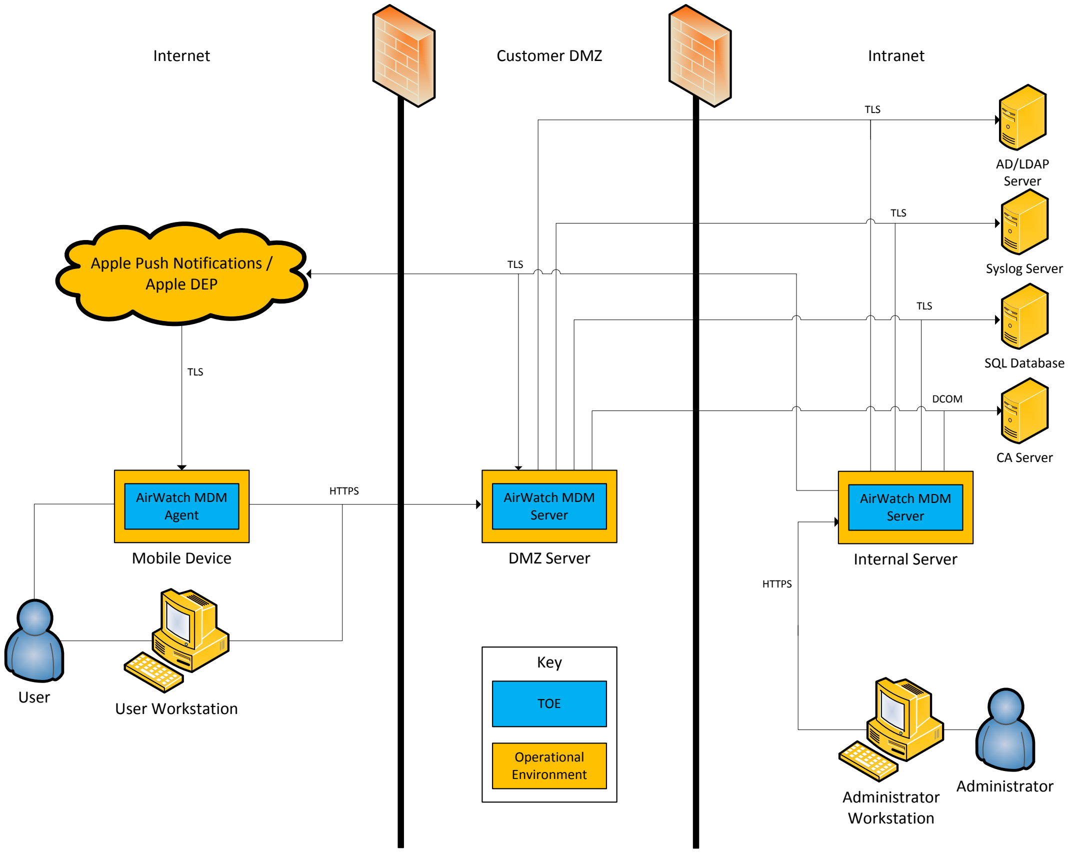
4.1 TOE Introduction

The TOE is a Mobile Device Management product and is comprised of two MDM Server components and an MDM Agent component. Two MDM Server components exist because the evaluated configuration of the TOE is to deploy it in an on-premises configuration, which requires a secondary instance of the MDM Server residing outside the organization's firewall in a demilitarized zone (DMZ) where it is exposed to external network traffic from the internet. The MDM Server component provides a centralized enterprise level management capability for a collection of mobile devices running the VMware AirWatch MDM Agents. It also provides a Mobile Application Store (MAS) Server that allows managed devices to download apps from a trusted repository that resides within the organization managing the device. The management functionality includes management of Administrators and users, mobile device enrollment, mobile device status, mobile device compliance and policy management, and application management. Administrators access the VMware AirWatch MDM Server through the Admin Console interface in order to manage users, policies, and devices. Users access the VMware AirWatch MDM Server through the Self-Service Portal, which allows them to perform administrative functions relating to their own devices.

The MDM Server runs on a Microsoft Windows Server 2012 R2 operating system and authentication to the MDM Server is provided by the Active Directory/LDAP service. The MDM Server also provides local authentication for initial setup and to mitigate a denial of service in the event the Active Directory/LDAP service is unavailable. The MDM Server stores audit data locally in a SQL database but can send audit records via a TLS encrypted trusted channel to a remote Syslog Server for remote storage.

In the evaluated configuration, the MDM Agent runs on a mobile device running one Apple iOS 9 or 10. The communication channel between the MDM Agent and the MDM Server is protected by TLS. Apple DEP is used to enroll the device with the MDM Server so that it can be managed by the MDM Server. Also, the MDM Agent provides status and policy information about the mobile device to the MDM Server. Figure 1 depicts the network configuration of the TOE.

Figure 1: Typical TOE Deployment



As depicted in Figure 1, the TOE consists of two VMware AirWatch MDM Server instances and one or more instances of the VMware AirWatch MDM Agent running on mobile devices. The expected deployment of the TOE is to have an on-premises deployment with two instances of the VMware AirWatch MDM Server running: one in the deploying organization's DMZ and one behind the firewall. The external server hosts the Self-Service Portal so that enterprise users can enroll and manage their own devices from outside the firewall and the Admin Console resides behind the firewall. The internal server communicates indirectly with the DMZ server through querying/modifying the SQL database used by both instances. The connection between the MDM Agent devices and the MDM Server is also protected by HTTPS. The connections between the MDM Server and the Syslog Server/RDBMS and between the MDM Server and AD/LDAP are protected with TLS. The MDM Server is also connected to a CA server in the internal network via DCOM for the purposes of performing mutual authentication.

4.2 Physical Boundaries

The TOE is comprised of software and the following table describes its components in the evaluated configuration:

Table 2 – Evaluated Components of the TOE

Component	Definition
VMware AirWatch MDM Server on Microsoft Windows 2012 R2 (including MAS)	MDM Server Component
VMware AirWatch MDM Agent on Apple iOS 9* (VID 10695)	MDM Agent Device
VMware AirWatch MDM Agent on Apple iOS 10**	MDM Agent Device

*VID 10695 certified iOS 9.2. However, since minor releases are covered by Assurance Maintenance and best practice is to use patched software, iOS 9.3 was tested.

**At the time of publication, Apple iOS 10 has not been certified on the NIAP PCL. The TOE was tested on this OS platform in order to ensure its compatibility with future certified products.

As shown in Figure 1, the TOE boundary on the end user mobile devices includes only the VMware AirWatch MDM Agent itself; the actual devices (using the A7 processor) have been evaluated against the Mobile Device Fundamentals Protection Profile under the Validation ID numbers identified in Table 4 above.

The TOE resides on a network and supports (in some cases optionally) the following hardware, software, and firmware in its operational environment:

Table 3 – Operational Environment Components

Component	Usage/Purpose Description for TOE performance
Windows Server 2012 R2	Underlying platform on which the VMware AirWatch MDM Server is installed.
Apple iOS 9 or 10	Underlying device (using the A7 processor) on which the VMware AirWatch MDM Agent is installed.
Certification Authority (CA) Server	The MDM Server component of the TOE connects to the CA Server via DCOM during device enrollment so that the TOE can provide each device with a unique certificate generated by the CA Server.
Microsoft SQL Enterprise	The TOE's RDBMS database, used to store configuration settings.
Syslog Server	The MDM Server component of the TOE connects to the Syslog Server to persistently store audit data for the MDM Server's own operation as well as the audit data collected from the MDM Agents that it manages.
Windows Server 2012 R2 Active Directory Certificate Services	Certificate Authority providing certificate services for the TOE.
Windows Server 2012 R2 Active Directory / LDAP Server	Identity store that defines users for device enrollment and administrator accounts for access to the Admin Console.

5 Security Policy

5.1 Security Audit

[SERVER] The MDM Server component of the TOE creates audit records for all of the auditable events found in Table 13 that are relevant to the MDM Server. It also audits its own startup and shutdown and administrative activities. Audit data is generated for configuration of the MDM Server itself as well as Server-initiated management activities that affect one or more managed mobile devices. The MAS Server also generates audit records when it experiences a failure to push or update an application on a managed mobile device. The audit records contain the subject identity and date and time of the auditable event. Other security-relevant information is included in the audit records as needed, depending on the function that is being audited. The audit records are stored locally in an SQL database and are transferred to a remote Syslog database over a TLS encrypted trusted channel. Audit records can be viewed on the Administrator Console.

The MDM Server can issue ‘compliance policies’ to managed mobile devices. Compliance policies are used to compare the configuration, status, or characteristics of a mobile device against a certain baseline and can be used to generate an alert to an Administrator if an anomaly is detected. The Administrator can also request on-demand connectivity status updates through the use of push notifications.

[AGENT] MDM Agent audit records are created as long as the underlying mobile device is powered on. The MDM Agent generates audit records for the activities it performs as a result of its interactions with the MDM Server or as a result of stored policy information. The MDM Agent generates audit records for security-relevant activity whenever the underlying mobile device is powered on. The MDM Agent facilitates alerting by providing data to the MDM Server on a periodic basis. The MDM Server can then analyze this data (or the absence of data in the case of periodic reachability events) in order to determine if anomalous behavior is occurring.

5.2 Cryptographic Support

The MDM Server and the MDM Server platform use cryptography provided by the cryptographic algorithms found in the CNG.sys (CMVP certificate #2356) and BCryptPrimitives.dll (CMVP certificate #2357) cryptographic modules for the Windows Server 2012 platform. The MDM Server uses cryptography to establish TLS and TLS/HTTPS trusted channels and paths to ensure secure communications of data in transit. This includes the use of RSA, Diffie-Hellman (DH) and Elliptic Curve Diffie-Hellman (ECDH) key establishment techniques. The MAS Server is integrated with the MDM Server so it uses the same cryptography.

The following table contains the CAVP algorithm certificates corresponding to the server CMVP certificates #2357 and #2356, as well as the agent CMVP certificates #2594 and #2827. In the evaluated configuration, the MDM Agent was tested on devices using the A7 processor running Apple iOS 9 and 10 (both 64-bit). The algorithm certificates are the same for cert. #2357 and #2356 except where indicated:

Table 4 –CAVP References

Algorithm	**CAVP Cert. # (Server)**	**CAVP Cert. # (iOS 9)**	**CAVP Cert. # (iOS 10)**
AES	2832	3686	4255
DRBG	489	993	1353
DSA (certificate #2357 only)	855	N/A	N/A
ECDSA	505	781	1003
HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384	1773	2432	2829
KAS ECC, KAS FFC	47	N/A	N/A
RSA	1487, 1493, 1519	1908	2314
SHA-1, SHA-256, SHA-384, SHA-512	2373	3100	3531

5.3 Identification and Authentication

[SERVER] The MDM Agent registers with the MDM Server so that it can be enrolled into management by the MDM Server. The user that is performing the enrollment must have a user account on the MDM Server so that they can access the Self-Service Portal and so that they are recognized by the system. This can either be a basic username/password defined on the MDM Server or a centrally defined Active Directory/LDAP credential.

Administrators (through the Admin Console) and users (through the Self-Service Portal) cannot access the MDM Server without being authenticated. Administrators and users can view the configured pre-authentication warning banner and query the MDM Server’s software version number prior to authentication, but all other TSF-mediated actions require authentication. In the event of a forgotten password, the TSF provides the ability to send a password reset email which requires a security question to be answered.

The MDM Server interfaces with the underlying Windows Server 2012 platform to provide certificate validation services via Microsoft Authenticode. Certificates are used for TLS/HTTPS authentication, code signing for software updates, code signing for integrity verification, and signing of MDM policies. In the evaluated configuration, the TOE will be loaded with organizational certificates that were generated in the Operational Environment; the TSF is not responsible for certificate generation.

[AGENT] During the enrollment process, the MDM Agent records the MDM Server’s DNS name and full URL with hostname. The MDM Agent also receives a certificate that is used to validate signed policies that are transmitted from the MDM Server. Similar to the MDM Server, the MDM Agent relies on the underlying platform to perform certificate validation.

5.4 Security Management

[SERVER] The TSF provides separate administrative interfaces for Administrators and for users. Administrators use the Admin Console to manage users, policies, and devices, while users use the Self-Service Portal to perform actions related to their own devices. Device enrollment can be initiated by either Administrators or by users. Regardless of the administrative interface that is used to perform an action that affects an MDM Agent, the interface the MDM Server uses to communicate with the MDM Agent is the same. The MDM Server can be used to transmit specific commands to a managed device such as forcibly locking the device, initiating a wipe operation, or sending a push notification. The MDM Server can also define policies (known as profiles) that specify the configuration settings for a device. These configuration settings can include functionality such as configuration of the password policy and what settings are applied to WiFi connections. The functionality that is configurable by the MDM Server is dependent on what the iOS platform provides the ability for third-party software to configure. The MDM Server also may transmit these policies either to the MDM Agent residing on the managed device or directly to the device itself, depending on the functionality being configured. All policy data sent from the MDM Server is signed using ECDSA with either SHA-256 or SHA-512 depending on whether it goes to the OS platform itself or to the TOE MDM Agent that resides there.

The MDM Server also allows for configuration of its own functions. This includes functionality such as defining Administrators and groups, defining the types of devices that are permitted to enroll, defining the communications period for periodic reachability events with managed devices, and configuration of the pre-authentication warning banner. The MDM Server also provides Administrators with the ability to query audit records as well as information about the managed devices.

The MDM Server also includes the MAS Server functionality, which provides the ability to grant or deny access to specific applications stored on the MAS Server to devices or groups of devices. The MAS Server is accessed through the same Admin Console interface as the MDM Server, so the administrative roles defined for both components are the same.

[AGENT] The MDM Agent communicates with the underlying OS platform to validate signed policy updates when they are received. Apple DEP is responsible for enrolling the device into management and preventing user-directed unenrollment. The MDM Agent is also responsible for receiving policy updates and forwarding them to the underlying platform, depending on what function is being managed by the update. Some MDM Server-initiated functionality is communicated directly to the platform rather than through the MDM Agent.

5.5 Protection of the TSF

The communications between the MDM Server and MDM Agent are protected using HTTPS. If the TOE's operational environment is such that multiple copies of the same MDM Server are deployed inside and outside of an organization's DMZ, then the communications between these components is also protected by HTTPS.

The TOE verifies the digital signatures of executables and .dlls using Microsoft's Authenticode making use of X.509v3 certificates. In addition, the MDM Server uses FIPS validated cryptographic modules which perform their own integrity checks at startup.

The TOE performs updates of its software and verifies the digital signatures of the updates prior to installing them.

5.6 TOE Access

The TOE displays a pre-authentication banner for the Admin Console and the Self-Service Portal. This can be customized by Administrators to fit the needs of the organization deploying the TOE.

5.7 Trusted Path/Channels

The trusted communication channels between the MDM Server and the device running the MDM Agent, the syslog audit server, AD/LDAP authentication server and the SQL database server are trusted communications channels which make use of TLS or TLS/HTTPS as the protection mechanism, depending on the interface.

The MDM Server platform uses TLS/HTTPS to provide a trusted path between itself and remote Administrators (through the Admin Console) and users (through the Self-Service Portal).

6 Documentation

The vendor provided the following guidance documentation in support of the evaluation:

- VMware AirWatch Mobile Device Management Supplemental Administrative Guidance, Version 1.0, dated January 3, 2017
- VMware AirWatch Installation Guide
- VMware AirWatch Mobile Device Management Guide
- VMware AirWatch iOS Platform Guide
- Generating and Reviewing an APNS Certificate for AirWatch
- VMware AirWatch Directory Services Guide
- VMware AirWatch Integration with Microsoft ADCS via DCOM
- VMware AirWatch Reports, Analytics, and Syslog Guide
- VMware AirWatch Apple Device Enrollment Program Guide
- VMware AirWatch On-Premises Configuration Guide

7 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is two MDM Server version 9.1 components and an MDM Agent version 9.1 component. Two MDM Server components exist because the evaluated configuration of the TOE is to deploy it in an on-premises configuration, which requires a secondary instance of the MDM Server residing outside the organization’s firewall in a demilitarized zone (DMZ) where it is exposed to external network traffic from the internet.

To use the product in the evaluated configuration, the product must be configured as specified in the *VMware AirWatch Mobile Device Management Supplemental Administrative Guidance v1.0* document.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the proprietary *Evaluation Technical Report for a Target of Evaluation "VMware AirWatch Mobile Device Management" Evaluation Technical Report v1.0, dated January 9, 2017*, as summarized in the publicly available *Assurance Activity Report for a Target of Evaluation "VMware AirWatch Mobile Device Management" Evaluation Technical Report v1.0, dated January 9, 2017*.

8.1 Test Configuration

The evaluation team conducted testing at AirWatch's Atlanta, GA facility on an isolated network. The evaluation team configured the TOE according the *VMware AirWatch Mobile Device Management Supplemental Administrative Guidance, Version 1.0* (AGD) document for testing. The evaluation team set up a test environment for the independent functional testing that allowed them to perform the assurance activities against the TOE over the SFR relevant interfaces.

The TOE was configured to communicate with the following environment components:

- Windows Server 2012 R2
- Apple iOS 9 or 10
- Microsoft SQL Enterprise 2008 R2
- Syslog Server (syslog-ng version 3.8.0alpha0)
- Windows Server 2012 R2 Certificate Authority (CA)
- Windows Server 2012 R2 Active Directory Certificate Services
- Windows Server 2012 R2 Active Directory / LDAP Server

The following test tools were installed on a separate workstation (management workstation)

- WireShark version 2.2.3
- Ettercap version 0.8.2

*Only the test tools utilized for functional testing have been listed.

8.2 Developer Testing

No evidence of developer testing is required in the Evaluation Activities for this product.

8.3 Evaluation Team Independent Testing

The test team's test approach was to test the security mechanisms of the TOE by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. The ST and the independent test plan were used to demonstrate test coverage of all SFR testing assurance activities as defined by the MDMPP and MDMAPP for all *security relevant* TOE external interfaces. TOE external interfaces that will be determined to be *security relevant* are interfaces that

- change the security state of the product,
- permit an object access or information flow that is regulated by the security policy,
- are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- invoke or configure a security mechanism.

Security functional requirements were determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface. The evaluation team tested each interface for all relevant behavior of the TOE that applied to that interface.

8.4 Evaluation Team Vulnerability Testing

The evaluation team created a set of vulnerability tests to attempt to subvert the security of the TOE. These tests were created based upon the evaluation team's review of the vulnerability analysis evidence and independent research. The evaluation team conducted searches for public vulnerabilities related to the TOE. A few notable resources consulted include securityfocus.com, the cve.mitre.org, and the nvd.nist.gov.

Upon the completion of the vulnerability analysis research and initially discovering no known vulnerabilities, the team identified several generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration.

The team tested the following areas:

- Eavesdropping on Communications
- Port Scanning
- Web Interface Vulnerability Identification

The TOE successfully prevented any attempts of subverting its security.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all Evaluation Activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the TOE to be Part 2 extended, and meets the SARs contained the PP. Additionally the evaluator performed the Evaluation Activities specified in the MDMPP and MDMAPP.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL, and are augmented with the validator's observations thereof.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the VMware AirWatch Mobile Device Management product that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally the evaluator performed an assessment of the Evaluation Activities specified in the MDMPP and MDMAPP in order to verify that the specific required content of the TOE Summary Specification is present, consistent, and accurate.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally the evaluator performed the Evaluation Activities specified in the MDMPP and MDMAPP related to the examination of the information contained in the TOE Summary Specification.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally the evaluator performed the Evaluation Activities specified in the MDMPP and MDMAPP related to the examination of the information contained in the operational guidance documents.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Evaluation Activities in the MDMPP and MDMAPP and recorded the results in a Test Report, summarized in the Evaluation Technical Report and sanitized for non-proprietary consumption in the Assurance Activity Report.

The validator reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the MDMPP and MDMAPP, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE. The evaluation team also ensured that the specific vulnerabilities defined in the MDMPP and MDMAPP were assessed and that the TOE was resistant to exploit attempts that utilize these vulnerabilities.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis requirements in the MDMPP and MDMAPP, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team’s test activities also demonstrated the accuracy of the claims in the ST.

The validation team’s assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Evaluation Activities in the MDMPP and MDMAPP, and correctly verified that the product meets the claims in the ST.

10 Validator Comments

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *VMware AirWatch Mobile Device Management Supplemental Administrative Guidance, Version 1.0,* dated January 3, 2017.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the product needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

The security target for this product's evaluation is *VMware AirWatch Mobile Device Management Security Target, Version 1.0*, dated December 27, 2016.

13 List of Acronyms

Acronyms / Abbreviations	Definition
CC	Common Criteria
CPU	Central Processing Unit
DEP	[Apple] Device Enrollment Program
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure over a bidirectional TLS encrypted tunnel
IP	Internet Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MAS	Mobile Application Store
MDM	Mobile Device Management
NIAP	National Information Assurance Partnership
OS	Operating System
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
UI	User Interface

14 Terminology

Term	Definition
Administrator	An individual that has the ability to manage some aspect of mobile device configuration using the Admin Console.
AirWatch Administrator	The class of TOE Administrators that allows comprehensive access to the AirWatch environment, excluding the Administration tab under System Configuration.
Application Management	The class of TOE Administrators that provides the ability to deploy and manage internal and public apps for managed devices.
End User	An individual who possesses a mobile device that is managed by AirWatch and who has limited authority to perform management functions using the Self-Service Portal
Role	The level of access given to Administrator accounts. The TOE comes with pre-defined roles but new roles with custom sets of privileges can be created.
System Administrator	The class of TOE Administrators that have complete access to an AirWatch environment, including access to Password and Security settings, Session Management and AirWatch Admin Console audit information contained in the Administration tab under System Configuration.

15 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 4.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. VMware AirWatch Mobile Device Management Security Target, Version 1.0, dated December 27, 2016
6. VMware AirWatch Mobile Device Management Supplemental Administrative Guidance, Version 1.0, dated January 3, 2017