VMWARE (VMW) AIRWATCH (AW) v9.x MDM SUPPLEMENTAL PROCEDURES

Version 1, Release 2

24 April 2020

Developed by VMware and DISA for the DoD

Trademark Information

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. SECURITY READINESS REVIEW

1.1 General

When conducting a VMware AirWatch security review, the reviewer or auditor will identify security deficiencies and provide data from which to predict the effectiveness of proposed or implemented security measures associated with the AirWatch MDM.

1.2 Mobile Policy Review

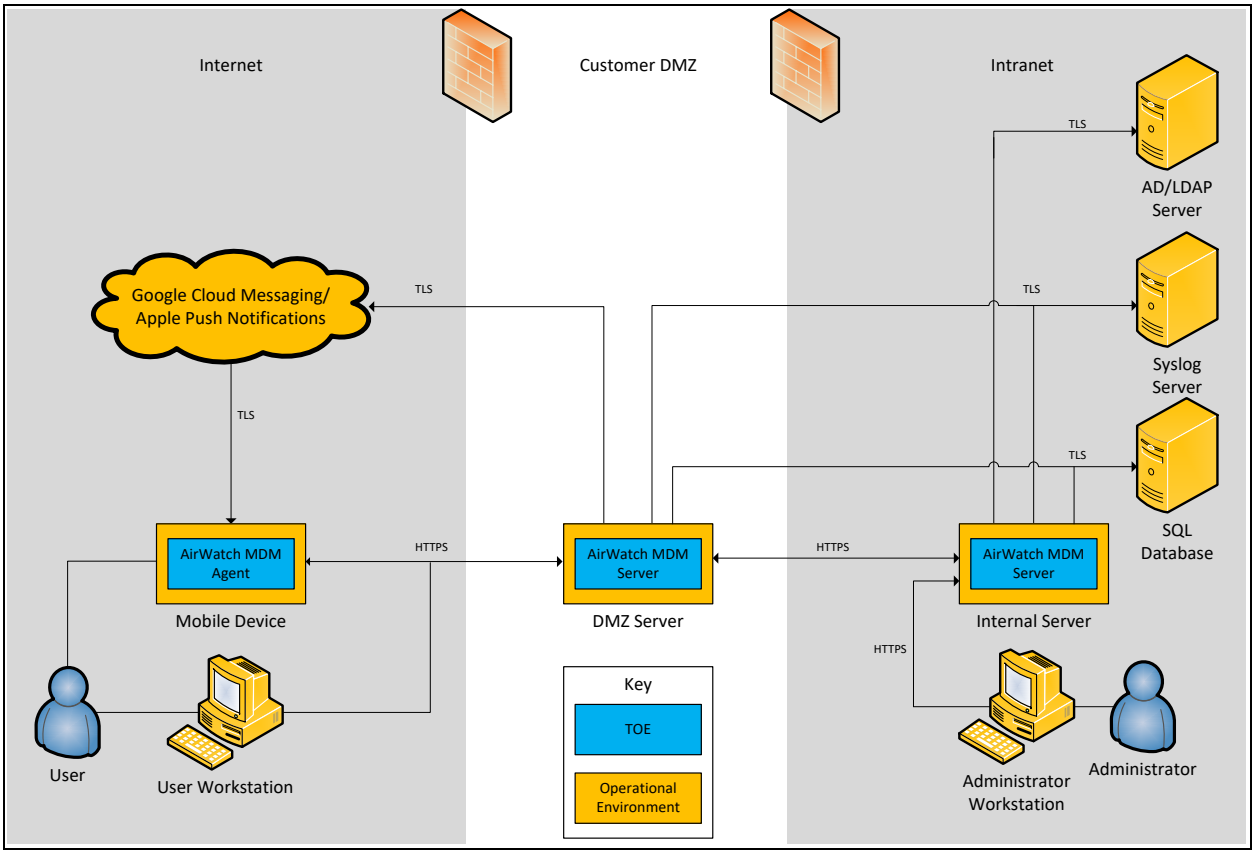
Detailed policy guidance is available on the DISA Information Assurance Support Environment (IASE) website located at http://iase.disa.mil/stigs/mobility/Pages/policies.aspx.

Use the Mobility Policy STIG and the CMD Management Policy STIG to review the AirWatch MDM asset.

2. AIRWATCH MDM SOFTWARE SECURITY AND CONFIGURATION INFORMATION

2.1 AirWatch MDM Architecture

Figure 2-1: AirWatch MDM Architecture



2.2 MDM Software Components

Table 2-1: AirWatch Core Components

Component	Description
AirWatch MDM Agent Application	AirWatch Agent application installed on the mobile device to communicate with the AirWatch MDM Server
AirWatch MDM DMZ Device Services Server	AirWatch application server installed within DMZ for external communication to mobile devices
AirWatch MDM Internal Network Console Server	AirWatch application server installed within internal network for hosting the Administration Console
AirWatch SQL Database Server	AirWatch SQL Database installed on internal network to house MDM configuration data

2.3 AirWatch MDM Required Firewall Ports

Table 2-2: Required Ports and Services

From	To	Port	Description
Native Mobile Device MDM Agent, AirWatch MDM Agent, and User Workstation	AirWatch MDM DMZ Device Services Server	443 (TLS/HTTPS)	TLS/HTTPS communication between mobile device and AirWatch MDM Agent application to MDM Server
AirWatch MDM DMZ Device Services Server	AirWatch Internal Network Console Server	443 (TLS/HTTPS)	Communication from AirWatch DMZ Server to Console Server
AirWatch MDM DMZ Device Services Server	AirWatch SQL Database Server	1433 (TCP)	Communication from AirWatch DMZ Server to AirWatch SQL Database Server
AirWatch Internal Network Console Server	AirWatch MDM DMZ Device Services Server	443 (TLS/HTTPS)	Communication from AirWatch Console Server to DMZ Server
AirWatch Internal Network Console Server	AirWatch SQL Database Server	1433 (TCP)	Communication from AirWatch Internal Console Server to Internal AirWatch SQL Database Server
AirWatch Internal Network Console Server	Enterprise LDAP or Directory Server	686/3269 (TLS/HTTPS)	Communication from AirWatch Console Server to LDAP or Directory Server
AirWatch Internal Network Console Server	External Auditing Server	Customizable to Organization Requirement (TLS)	TLS connection via Syslog from AirWatch Console Server to Enterprise External Auditing Server
Internal Network Workstations	AirWatch Internal Network Console Server	443 (TLS/HTTPS)	Communication from internal network workstations to AirWatch Console