MOBILEIRON CORE v9.x MDM SUPPLEMENTAL PROCEDURES

Version 1, Release 3

28 July 2017

Developed by MobileIron 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 MobileIron 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 MobileIron MDM.

1.2 Mobile Policy Review

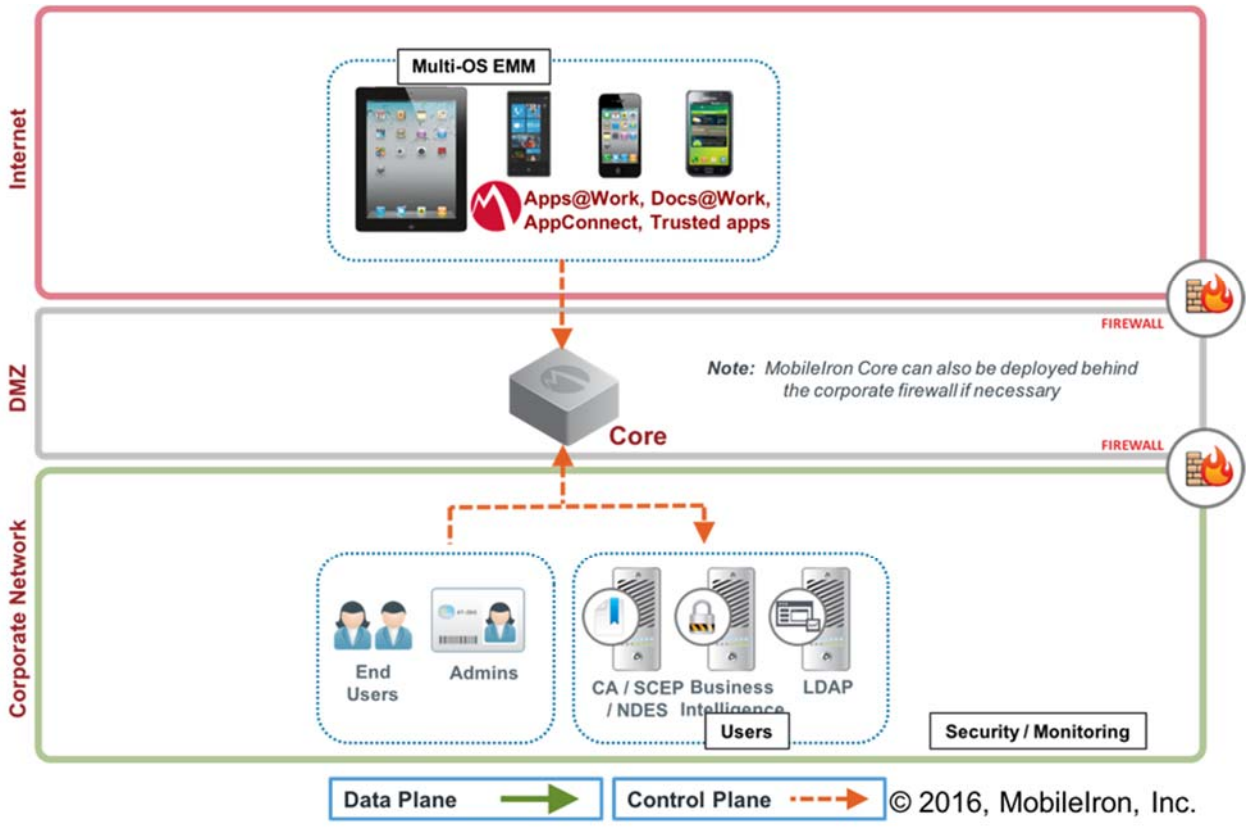
Detailed policy guidance is available on the DISA Information Assurance Support Environment (IASE) website located at http://iase.disa.mil/stigs/mobility/Pages/policies.aspx.

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

2. MOBILEIRON MDM SOFTWARE SECURITY AND CONFIGURATION INFORMATION

2.1 MobileIron MDM Architecture

Figure 2-1: MobileIron Core MDM Architecture



2.2 MobileIron MDM Software Components

Table 2-1: MobileIron Core Components

Component	Description
Mobile@Work for Android	MobileIron MDM Agent for Android
MobileIron Core	MobileIron MDM Server

2.3 MobileIron MDM Required Firewall Ports

Table 2-2: Required Ports and Services

From	To	Port (TCP)	Description
Administrators	MDM Server	22	SSH
Mobile Devices	MDM Server	80	HTTP
Mobile Devices	MDM Server	443	HTTPS

From	To	Port (TCP)	Description
Administrators	MDM Server	8443	HTTPS-alt

2.4 PKI Considerations

In order to implement over-the-air (OTA) provisioning of a DoD mobile device, an authenticated and encrypted tunnel can be set up between the mobile device and the mobile device management (MDM) server. The mobile device and MDM server must support the same root certificate authority to set up a mutually authenticated trusted tunnel between both end points. In order for the mobile device to support the current DoD root Certificate Authority, DoD Root CA 3, the mobile device needs to natively, out-of-the-box, trust the current DoD root Certificate Authority, or the certificate will need to be side-loaded on the mobile device, which is not scalable in an Enterprise environment. Unfortunately, few, if any mobile devices natively trust this root CA. Alternately, since there is a path of trust between DoD Root CA 3 and the Federal Common Policy Certificate Authority (FCPCA), a mobile device that natively trusts the FCPCA, can authenticate the MDM if either the MDM server or web service used by the MDM (for example IIS, Apache) pushes down a path to the FCPCA to the mobile device during the TLS handshake.

The MobileIron MDM's web service is provided by Apache. A Local Admin on the MDM can manage these certificates through the Web UI's System Manager, by navigating to the “Security” tab and selecting Certificate Mgmt. They can then upload a PKCS12 file containing the server's certificate and all CA certificates in the path from the DoD PKI Issuing CA (e.g. DoD ID SW CA 37) to Federal Common Policy.