IVANTI ENDPOINT MANAGER MOBILE (EPMM) SUPPLEMENTAL PROCEDURES

Version 3, Release 1

24 October 2024

Developed by Ivanti and DISA for the DOD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by the Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

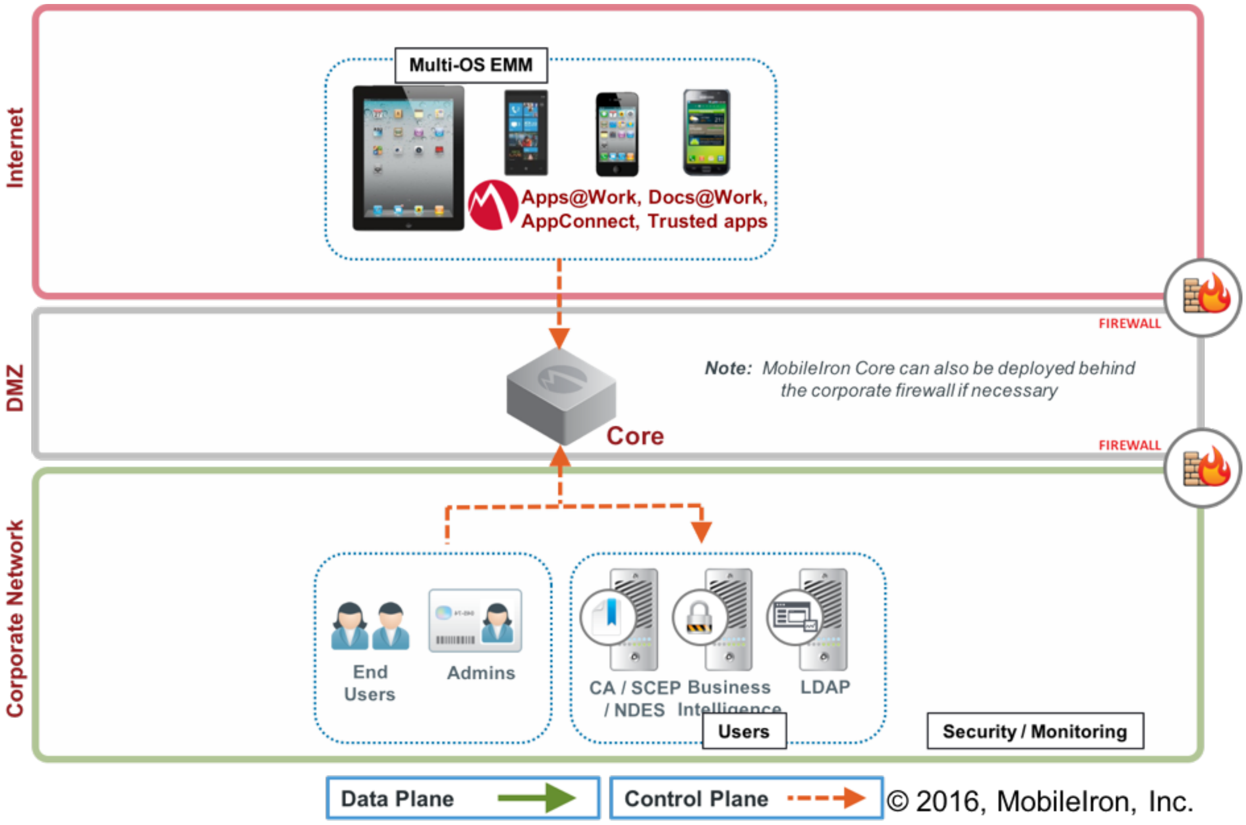
LIST OF FIGURES

Page

1. IVANTI EPMM SOFTWARE SECURITY AND CONFIGURATION INFORMATION

1.1 Ivanti EPMM Architecture

Figure 1-1: Ivanti EPMM Architecture[1]



1.2 Ivanti EPMM Software Components

Table 1-1: Ivanti EPMM Components

Component	Description
Mobile@Work for Android	Ivanti EPMM Agent for Android
Ivanti EPMM	Ivanti EPMM Server

1.3 Ivanti EPMM Required Firewall Ports

Table 1-2: Required Ports and Services

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

[1] Note: This figure uses the old product name (MobileIron Core MDM).

From	To	Port (TCP)	Description
Mobile Devices	MDM Server	443	HTTPS
Administrators	MDM Server	8443	HTTPS-alt
Mobile Devices	MAS (component of Core)	7443	HTTPS-alt

1.4 PKI Considerations

In order to implement over-the-air (OTA) provisioning of a Department of Defense (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 endpoints. In order for the mobile device to support the current DOD root Certificate Authority (CA), DOD Root CA 3, the mobile device must natively, out-of-the-box, trust the current DOD root CA. If not, the certificate must 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 or Apache) pushes down a path to the FCPCA to the mobile device during the TLS handshake.

The Ivanti EPMM 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.