IBM MaaS360 v2.3.x MDM
SUPPLEMENTAL PROCEDURES

Version 1, Release 1

26 February 2016

Developed by IBM 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 DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

1. SECURITY READINESS REVIEW 1

1.1 General 1
1.2 Mobile Policy Review...1

2. IBM MAAS360 SOFTWARE SECURITY AND CONFIGURATION INFORMATION...2

2.1 IBM MaaS360 Overview 2
2.2 IBM MaaS360 Architecture 2
2.3 IBM MaaS360 MDM Software Components 4
2.4 IBM MaaS360 Required Firewall Ports...4
2.5 IBM MaaS360 User Identification, Authentication, and Enrollment 5
2.6 IBM MaaS360 Mobile Device Configuration and Policy Management.......................6
2.7 IBM MaaS360 Mobile Application Management..6

LIST OF FIGURES

Page
Figure 2-1: MaaS360 Solutions Comparison.. 2
Figure 2-2: SaaS Cloud Deployment 3
Figure 2-3: On-Premise Deployment... 3

1. SECURITY READINESS REVIEW

1.1 General

When conducting a MaaS360 Security Readiness Review (SRR), the Team Lead and the assigned Reviewer identify security deficiencies and provide data from which to predict the effectiveness of proposed or implemented security measures associated with MaaS360.

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.

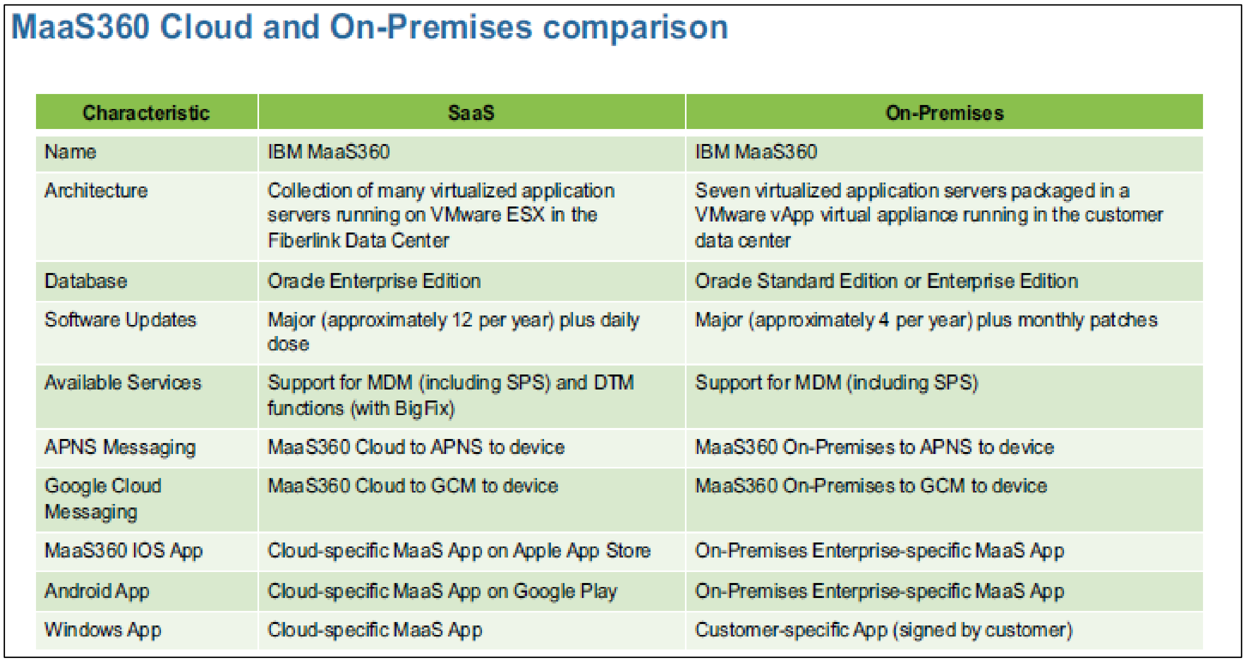
Use the Mobility Policy STIG and the CMD Management Policy STIG to review the MaaS360 MDM asset.

2. IBM MAAS360 SOFTWARE SECURITY AND CONFIGURATION INFORMATION

2.1 IBM MaaS360 Overview

The implementation of MaaS360 can take on a variety of forms based on the size and complexity of the deployment. MaaS360 has been available as a cloud solution for many years. IBM MaaS360 On-Premises contains the same features and functions as the cloud-based product, but it is packaged to be deployed in a customer datacenter instead of an IBM datacenter. MaaS360 On-Premises is packaged in a VMware virtual appliance.

Figure 2-1: MaaS360 Solutions Comparison



MaaS360 Cloud and On-Premises comparison

Characteristic	SaaS	On-Premises
Name	IBM MaaS360	IBM MaaS360
Architecture	Collection of many virtualized application servers running on VMware ESX in the Fiberlink Data Center	Seven virtualized application servers packaged in a VMware vApp virtual appliance running in the customer data center
Database	Oracle Enterprise Edition	Oracle Standard Edition or Enterprise Edition
Software Updates	Major (approximately 12 per year) plus daily dose	Major (approximately 4 per year) plus monthly patches
Available Services	Support for MDM (including SPS) and DTM functions (with BigFix)	Support for MDM (including SPS)
APNS Messaging	MaaS360 Cloud to APNS to device	MaaS360 On-Premises to APNS to device
Google Cloud Messaging	MaaS360 Cloud to GCM to device	MaaS360 On-Premises to GCM to device
MaaS360 IOS App	Cloud-specific MaaS App on Apple App Store	On-Premises Enterprise-specific MaaS App
Android App	Cloud-specific MaaS App on Google Play	On-Premises Enterprise-specific MaaS App
Windows App	Cloud-specific MaaS App	Customer-specific App (signed by customer)

2.2 IBM MaaS360 Architecture

The following information and diagrams depict a representative implementation for MaaS360 installations through Software as a Service (SaaS) and On-Premise solutions. Specific installations will vary on customer environment and deployment requirements.

Figure 2-2: SaaS Cloud Deployment

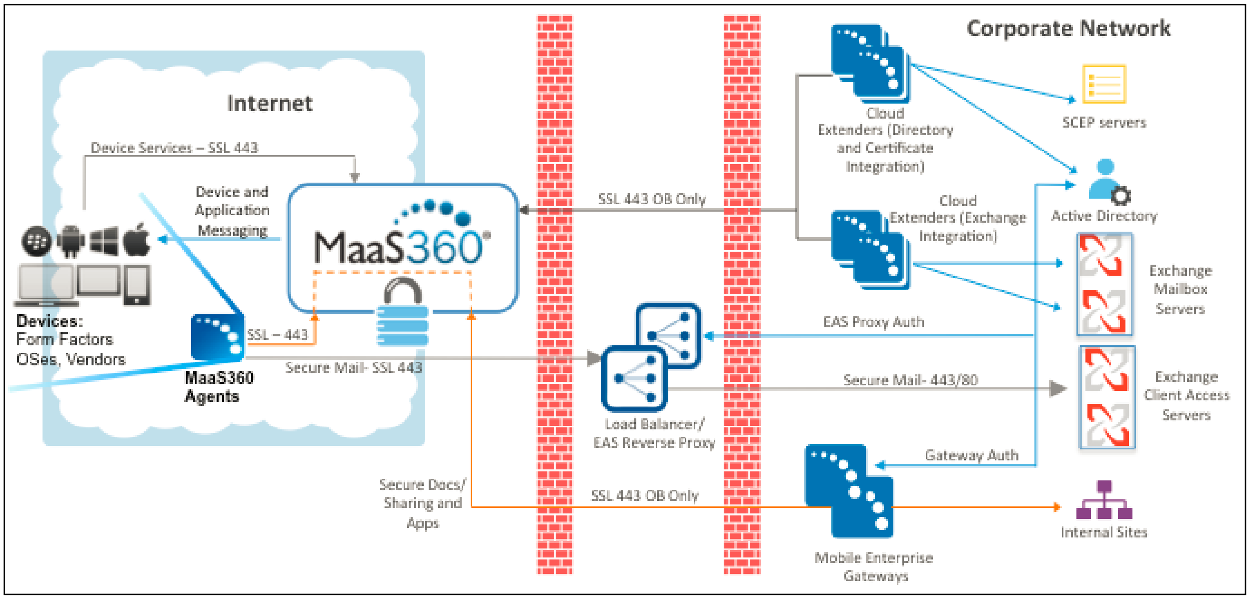
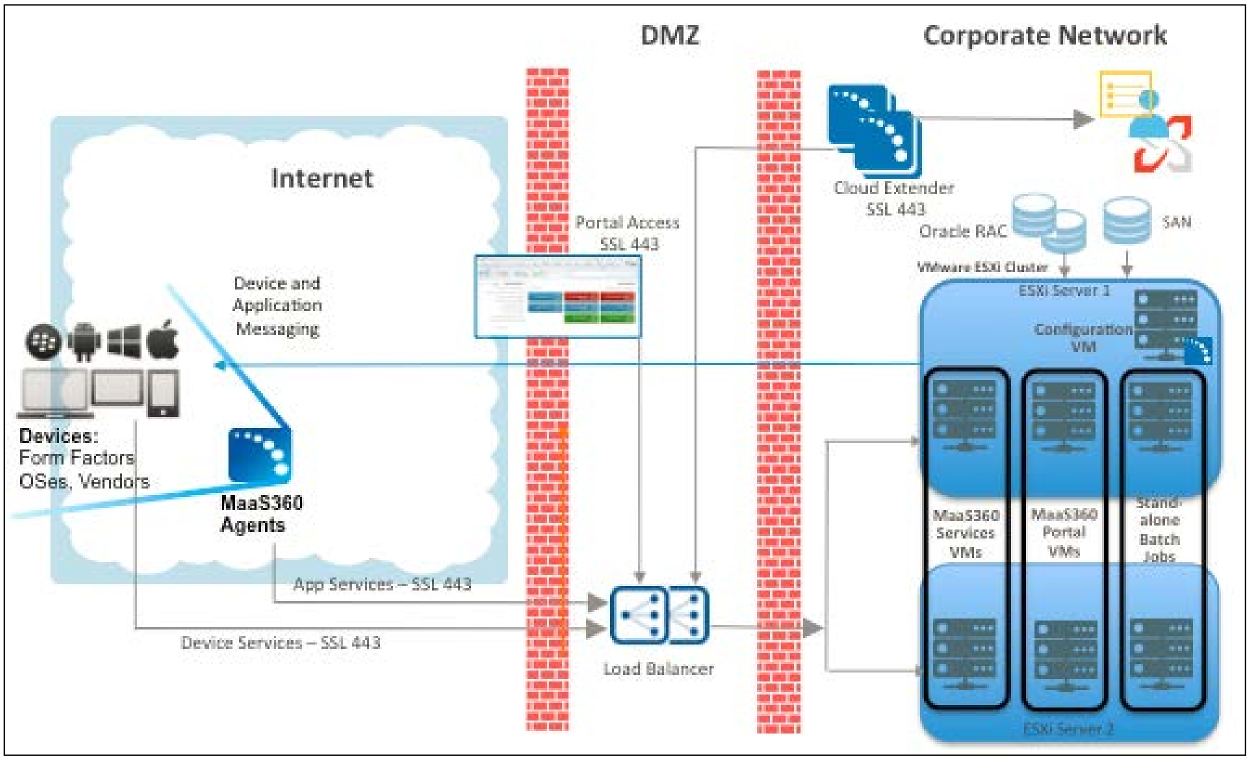

Internet
Device Services – SSL 443
Device and Application Messaging
MaaS360
SSL – 443
Devices:
Form Factors
OSes, Vendors
MaaS360 Agents
Secure Mail- SSL 443
SSL 443 OB Only
Load Balancer/ EAS Reverse Proxy
Secure Docs/ Sharing and Apps
SSL 443 OB Only
Corporate Network
Cloud Extenders (Directory and Certificate Integration)
SCEP servers
Cloud Extenders (Exchange Integration)
Active Directory
Exchange Mailbox Servers
EAS Proxy Auth
Secure Mail- 443/80
Exchange Client Access Servers
Gateway Auth
Internal Sites
Mobile Enterprise Gateways

Figure 2-3: On-Premise Deployment



2.3 IBM MaaS360 MDM Software Components

Component	Description
MaaS360 Administration Console	This is the configuration VM used to deploy and administrate the MaaS360 Portal Console.
MaaS360 Portal Console	This is the console used by administrators to manage end-user devices, device enrollment, policy creations, policy pushes, and other device management functionality.
MaaS360 Agents	This is software installed directly on the end user's device that allows MaaS360 to manage the device by communications between the agent and the MaaS360 Portal.
MaaS360 Database	MaaS360 creates four databases on the Oracle database server: VPN2, which is a real-time transactional database that hosts device data and data for most portal workflows; AGILINK, which is a database that is the primary point of entry for new account information; EDW, which is a data warehouse for supporting reports; and P03, which is a database for log processing.
MaaS360 Cloud Extender	The Cloud Extender is an optional integration component that connects MaaS360 to various enterprise applications within your environment: Active Directory or LDAP Servers, Simple Certificate Enrollment Protocol (SCEP) servers, Blackberry Enterprise Servers (BES 5 only), Exchange ActiveSync, Lotus Traveler servers, etc.
MaaS360 Mobile Enterprise Gateway	The Mobile Enterprise Gateway is an optional integration component that is installed in the corporate network or DMZ. It provides access from mobile devices to behind-the-firewall resources on your enterprise network without VPN access, such as SharePoint, Windows File Shares, or Intranet Sites.

2.4 IBM MaaS360 Required Firewall Ports

From	To	Port (TCP)	Description
IBM MaaS360	Oracle DB	1521 (default or as configured	Device, account, and reporting storage
IBM MaaS360	DNS	53, 123	Name resolution

From	To	Port (TCP)	Description
IBM MaaS360	SMTP	25	Outgoing mail notifications
IBM MaaS360	Apple Push Notification Service (APNS)	2195, 2196	iOS device notifications
IBM MaaS360	Google Cloud Messaging Service	5228, 5229, 5230	Android device notifications
IBM MaaS360	Microsoft Notification Server	80, 443	Windows Phone device notifications
IBM MaaS360	Apple App store, Google Play store, Windows App store	443	App store interactions
IBM MaaS360	SMS Gateway	2775 (default) or as configured	Custom SMS gateway interactions
IBM MaaS360	NFS Server	2049	NFS server interactions
IBM MaaS360	NTP Server	UDP 123 (default) or as configured	NTP server time synchronizations
SNMP Clients	IBM MaaS360	161	SNMP client interaction with the virtual appliance
Cloud Extender	IBM MaaS360	443	Upload account and management data to the virtual appliance
Cloud Extender	IBM MaaS360	Customer Configured	Query internal services for directory and account data
Mobile Enterprise Gateway	Internal Enterprise Services	Customer Configured	Pass device traffic to the internal network
Managed Devices	Mobile Enterprise Gateway	443	Send device traffic to the internal network
Managed Devices	IBM MaaS360	443	Report device data to virtual appliance
Administration Console	IBM MaaS360	8443	Configure and manage the virtual appliance

2.5 IBM MaaS360 User Identification, Authentication, and Enrollment

For SaaS and On-Premise, customer’s user identification, authentication, and enrollment does not change due to platform. This is all done through the MaaS360 console by creating users within the console or connecting to a customer’s Active Directory using Cloud Extender and creating users authenticated through a customer’s back-end authentication mechanism.

2.6 IBM MaaS360 Mobile Device Configuration and Policy Management

For SaaS and On-Premise, a customer's mobile device configurations and policy management do not change due to type of implementation. All management of device configurations and policy management are handled in the MaaS360 console. Administrators can create different policies based on groups, devices, or other organizational preferences. These configurations and policies are pushed down to managed devices and monitored for compliance, while also allowing for alerts sent if out of compliance and organizational-defined actions taken for devices found to be out of compliance. **Note**: Two host-based firewall requirements (IM360-01-010400 and IM360-01-010500) are applicable for only the On-Premise implementation.

2.7 IBM MaaS360 Mobile Application Management

MaaS360 can provide whitelists and blacklists for applications, as well as act as the Mobile Application Store (MAS) if the customer chooses that option. Distribution of application and monitoring for application compliance can be done through the MaaS360 console as well.