IBM MAAS360 WITH WATSON V10.X MDM SUPPLEMENTAL PROCEDURES

Version 1, Release 2

26 April 2019

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

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. IBM MAAS360 SOFTWARE SECURITY & CONFIGURATION INFORMATION

1.1 IBM MaaS360 with Watson Overview

MaaS360 was built from the ground up as a 100 percent dedicated Software as a Service (SaaS) cloud solution. The actual implementation of MaaS360 is done completely over the air, so it is extremely lightweight and easy for basic Unified Endpoint Management. Optional[1] "Cloud Extender" software integrations on the customer premise can create a hybrid implementation of MaaS360 when desired to address specific customer use cases.

1.1.1 MaaS360 Solution Overview

Architecture – Collection of many virtualized application servers running on VMware ESX in the IBM MaaS360 FedRAMP Data Center

Database – Oracle Enterprise Edition

Software Updates – Major (approximately 12 per year) plus daily doses

Available Services – Management and security of smartphones, tablets, laptops, desktops, wearables, and Internet of Things (IoT) devices along with their data and apps

APNS Messaging – MaaS360 Cloud to APNS to Device

Google Cloud Messaging – MaaS360 Cloud to GCM to Device

MaaS360 iOS App – IBM MaaS360 App on Apple App Store

Android App – IBM MaaS360 on Google Play Store

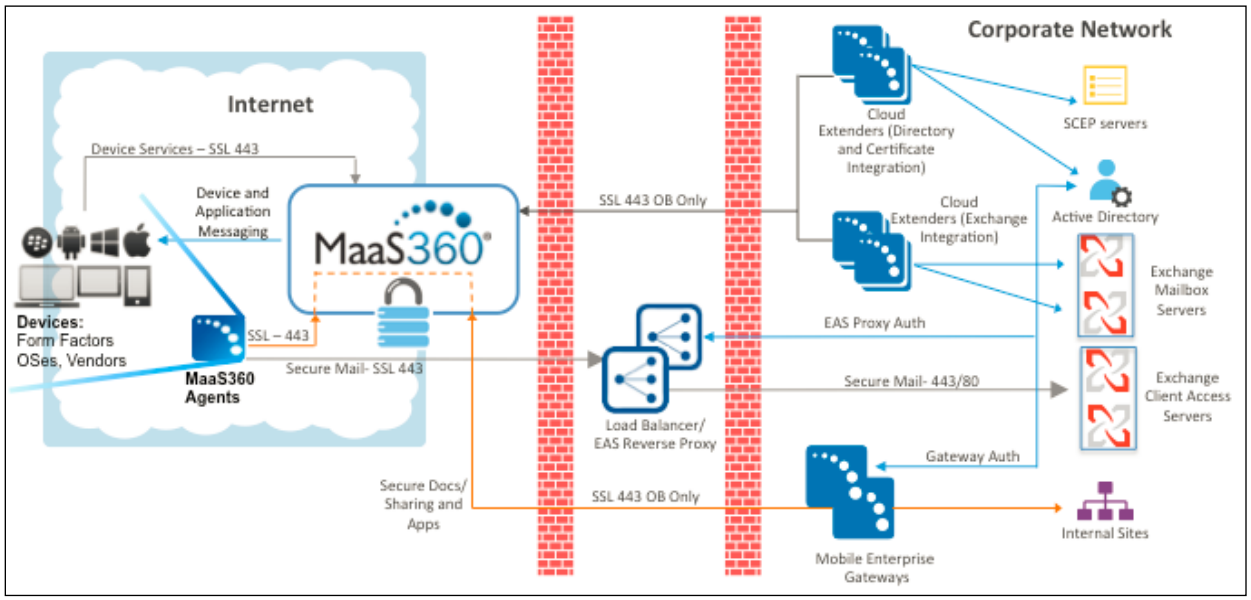
Windows App – IBM MaaS360 on Windows App Store

1.2 IBM MaaS360 Architecture

The following information and diagram depict a representative implementation for the MaaS360 SaaS solution. Optional software components will vary based on customer environment and use case requirements.

[1] In this case "optional" means the MaaS360 server can be deployed without the Cloud Extender component. However, Cloud Extender is a required component for all DoD deployments (see requirements V-82169/M360-10-007700 and V-82171/M360-10-007800).

Figure 1-1: SaaS Cloud Deployment Applications



Note: Figure 1-1 applies to a FedRAMP Moderate/DoD Cloud Security Model Impact Level 2 (IL 2) deployment. Once IBM MaaS360 with Watson receives Impact Level 4/5 certification, a new diagram will be added with the appropriate architecture that includes the Secure Cloud Computing Architecture (SCCA)/Cloud Access Point (CAP) for those appropriate levels.

1.3 IBM MaaS360 MDM Software Components

Table 1-1: IBM MaaS360 MDM Software Components

Component	Description
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 Cloud Extender	The Cloud Extender is an integration component that connects MaaS360 to various enterprise applications within the 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

Component	Description
	corporate network or DMZ. It provides access from mobile devices to behind-the-firewall resources on the enterprise network without VPN access, such as SharePoint, Windows File Shares, or intranet sites.
MaaS360 Email Access Gateway	MaaS360 Email Access Gateway (EAG) is a highly secure, scalable, and high-performance enterprise-grade reverse proxy solution that can control the ActiveSync traffic flow to the enterprise email environment.
MaaS360 VPN	IBM MaaS360 VPN is a virtual private network (VPN) solution that enables users to connect seamlessly to their enterprise network from mobile devices. The solution consists of the VPN server software and the client for mobile devices and supports features such as Device VPN, On-Demand VPN, Always on VPN, Per-App VPN, and split tunneling.

1.4 IBM MaaS360 Required Firewall Ports

Table 1-2: 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
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

From	To	Port (TCP)	Description
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
Email Access Gateway	Email Server	443	Access to corporate email server from EAG public interface. Internal firewalls rules may need to be opened to enable this connectivity
IBM MaaS360 VPN	LDAP	Port 389 for LDAP Port 636 for LDAP over SSL Port 3268 for Global Catalog (Microsoft Active Directory) Port 3269 for Global Catalog over SSL (Microsoft Active Directory)	Authenticate session requests. Internal firewall rules may need to be opened to enable this authentication connectivity
IBM MaaS360 VPN	Internal Server	UDP 1194 (default) or as configured	Pass device traffic to 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

1.5 IBM MaaS360 User Identification, Authentication, and Enrollment

The 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. IBM MaaS360 supports a variety of certificate-based authentication requirements.

1.6 IBM MaaS360 Mobile Device Configuration and Policy Management

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 to be sent if out of compliance and organizational-defined actions to be taken for devices found to be out of compliance.

1.7 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.

1.8 Provisioning Derived Credentials

The need to provision derived credentials benefits from some MDM features that are not required to support other functionality. This section describes these features for Android and iOS.

1.8.1 Android

Starting with Android P, some key management APIs require key management applications to be configured as a device owner, profile owner, device owner delegate, or profile owner delegate. To support the full range of options, MDMs should support the setCertInstallerPackage interface of the DevicePolicyManager class.

1.8.2 Apple iOS

On iOS, to enable third-party apps to use derived credentials, the key sharing interface of the Purebred application should be leveraged. The key sharing interface is a use of Apple's document provider extensions to share PKCS 12 objects between a key management application and an application desired to use keys. Sample code is available at https://github.com/purebred.

For iOS 12, depending on the MDM vendor and the use of the iOS provided mail client for work email, a managed Exchange payload with the following settings set to "True" can be leveraged to allow users to select Purebred-issued credentials for signed and encrypted email:

SMIMESigningUserOverrideable;
SMIMESigningCertificateUUIDUserOverrideable;
SMIMEEncryptByDefaultUserOverrideable;
SMIMEEncryptionCertificateUUIDUserOverrideable