Using Worklight Foundation as a development platform for building B2E apps to be deployed, secured and managed by MaaS360

Contents

MaaS360™ is an enterprise mobility management platform that you use to provision, secure, and manage the mobile devices in your enterprise as well as the applications you are building, whether they are in-house and public applications—all from a single portal—while minimizing risks to your organization.

As an enterprise mobile application platform, IBM® Worklight® lets you build, run and manage HTML5, hybrid and native mobile apps.

If you are using MaaS360 as the enterprise mobility management solution to enable your BYOD strategy and the Worklight platform for the development and management of mobile applications, this document will help you understand how to best use the products together and options that are available to you.

Introducing Worklight and MaaS360

MaaS360 is an IBM enterprise mobility management (EMM) platform that enables IT to deliver end-to-end security and management for devices, applications, documents, emails, and web access. Businesses use MaaS360 to provide their employees with secure access to corporate resources and information from corporate- or personally-owned mobile devices, without compromising the user experience, data security, or privacy. MaaS360 delivers maximum flexibility for bring your own device (BYOD) with a dual persona approach, multi-platform support, self-service enrollment, customized over-the-air configuration, automated policy enforcement, and secure distribution of applications and documents.

The main solution bundles of MaaS360 are:

MaaS360 Advanced Mobile Management
Enables organizations to manage and secure enterprise-owned and personal BYO smartphones, tablets, and laptops. It simplifies deploying private and public apps by delivering an easy-to-use enterprise app catalog with full security and operational lifecycle management.

MaaS360 Mobile Device Management
Streamlines the provisioning corporate-owned and employee-owned BYO devices over-the-air with features for enrollment, configuration, security policy management, and device actions such as locate, lock, and wipe.

MaaS360 Mobile Application Management
Simplifies the distribution, updating and management of private, public and purchased apps by delivering an easy-to-use enterprise app catalog with full security and operational lifecycle management across mobile device platforms

MaaS360 Mobile Expense Management
Enables organization-wide expense policies and proactively monitors and tracks mobile data and application usage to optimize mobile spend and shift the accountability more to departments and individual employees

MaaS360 Laptop Management
In addition to smartphones and tablets, MaaS360 manages Windows-based laptops, desktop and ultrabooks, and Apple MacBooks, iMacs and Mac Pros, delivering actionable information across all of your laptops and distributed PCs

MaaS360 Secure Productivity Suite
Delivers a comprehensive set of cross-platform solutions to isolate and contain work emails, web access and app data to prevent data leaks

MaaS360 Secure Mail

An intuitive personal information management (PIM) app with email, calendar and contacts for iOS, Android and Windows Phone devices

MaaS360 Secure Browser

A feature-rich web browser for secure access to intranet sites and web apps, and automated compliance of content policies for iOS, Android, and Windows Phone devices

MaaS360 Mobile Application Security

Provides a mobile application container with full operational and security management to protect against data leaks for iOS and Android devices

MaaS360 Secure Document Sharing

Configures a secure, encrypted container and productivity suite to distribute, view, create, edit, and share documents on mobile devices, giving organizations the control they need and employees the access they demand.

MaaS360 Mobile Content Management

Delivers a mobile document container for secure content collaboration with a robust set of lifecycle management capabilities to distribute, update, manage, and secure documents on iOS and Android devices

MaaS360 Secure Editor

An office productivity app to create, edit, and save documents on iOS and Android devices and designed to prevent corporate data leaks

MaaS360 Document Sync

Enables users to easily and securely synchronize content across managed iOS mobile devices

MaaS360 Mobile Enterprise Gateway

Offers simple, secure access to behind-the-firewall business resources, such as SharePoint, Windows File Share, intranet sites and databases without requiring changes to your network, firewall security configuration or device VPN

MaaS360 Mobile Enterprise Gateway for Browser

Delivers access to enterprise intranet and internal websites without requiring a full device level VPN connection on iOS and Android devices

MaaS360 Mobile Enterprise Gateway for Docs

Allows mobile devices outside of the enterprise network secure and seamless access to internal file stores without requiring a full device level VPN connection on iOS and Android devices

MaaS360 Mobile Enterprise Gateway for Apps

Enhances enterprise apps with secure and seamless access to internal data and resources without requiring a full device level VPN connection on iOS and Android devices

Two important elements will help you in this area: MaaS360 Mobile Application Management simplifies the distribution of applications to your employees and MaaS360 Mobile Application Security enables secure containment of corporate data in your applications.

IBM Worklight Foundation provides an open, comprehensive and advanced mobile application platform that can help you efficiently develop, run, and manage HTML5, hybrid, and native applications, using standards-based technologies and tools, mobile-optimized middleware, a variety of security mechanisms, and integrated management and analytics capabilities.

The main components of Worklight Foundation are:

Worklight Studio
The development environment of Worklight, an eclipse-based IDE that simplifies the development of multi-platform native or hybrid mobile applications.

Worklight Server
A mobile-optimized middleware that serves as a gateway between the mobile applications, back-end systems, and cloud-based services.

Worklight Device Runtime
A set of client-side application programming interface (API) that regroups functionality around application security / authentication, backend integration, mobile database for offline storage, push notification, cross-platform support and more.

Worklight Console
A web-based tool to administer and monitor mobile applications in production

Worklight Application Center
An enterprise app store that manages the distribution of production-ready mobile apps.

Building mobile applications for your employees that connect to enterprise services

IBM Worklight will help you build mobile applications for your employees. With the Worklight Studio development tools, IBM Worklight simplifies the creation of native applications (by using native SDK of the mobile platforms) and hybrid applications (by using web standards such as HTML5, CSS, and JavaScript™).
Adopting hybrid technologies for your employee-facing applications can help you build cross-platform applications more rapidly. Within a hybrid application, a large portion of the application

UI and logic will be written by using web standards and will run naturally across mobile platforms.
IBM Worklight will help you in all the phases of your development, providing many tools such as a WYSIWIG editor for building the application user interface, a simulator to preview and simulate the user interface under several form factors and functional testing tools to ensure that your mobile application is behaving as expected.
Building mobile applications is not only about building the user interface, but configuring access the back-end data of your enterprise in a secure way.

Some mobile applications run strictly offline with no connection to a back-end system, but most mobile applications connect to existing enterprise services to provide critical user-related functions. For example, employees might use their ‘expense report’ mobile application anywhere at anytime. Their reports will have to be processed through the back-end of the enterprise. To integrate a mobile application with enterprise services, you must use middleware, such as a mobile gateway. IBM Worklight can act as this middleware solution and make communication with back-end services easier and seamless.
To achieve this integration Worklight defines the notion of an adapter. Adapters are server-side code that is deployed on and serviced by the Worklight server component. An adapter connects the mobile application with the enterprise back-end service and performs any necessary application logic.

While Worklight provides an efficient mobile middleware to enable mobile applications to access services in your enterprise in a secured way, MaaS360 also helps employees to access corporate data and content through various ways on mobile devices.

MaaS360 Secure Productivity Suite and MaaS360 Secure Document Sharing, powered by MaaS360 Mobile Enterprise Gateway enable your employees to securely and seamlessly access corporate resources like email, contacts, calendar, documents, app data, and enterprise intranet at anytime and from anywhere.

MaaS360 isolates and contains these resources to prevent data leaks while preserving the mobile experience on their devices, completely separating enterprise and personal data from each other. More importantly, it makes your employees more productive while maintaining data security. These capabilities can be enabled without requiring changes to your network, firewall security configuration or device VPN.

With the MaaS360 Advanced Mobile Management, IT administrators can manage and secure any personally (BYOD) or corporate-owned smartphone, tablet, and laptop, and ensure that they are in compliance with security policies before they are granted enterprise access. If devices are compromised (through jailbreaking or rooting), lost or stolen, corporate data, apps and profiles can be easily and automatically wiped.

MaaS360 Mobile Application Management simplifies the distribution, security, and lifecycle management of both private and public apps. Employees will have access to their own customized enterprise app catalogs with the apps they need to be productive.

Worklight and MaaS360 are very complementary in this area; both ensure a secure access to the back-end data of your enterprise. Worklight enables your back-end services to be used within the mobile applications and MaaS360 delivers secure access to critical information such as like email, contacts, calendar, documents, app data, and enterprise intranet.

Securing application with user authentication

MaaS360 provides an authentication system that will require users to authenticate before they access a mobile application. This authentication mechanism can be used on all types of applications, whether they are corporate applications that you are building within your enterprise or public applications that you want to make available to your employees. Thanks to the MaaS360 product, you can also connect this authentication system to the user directory (AD or LDAP) of your company so that users can provide their corporate credentials to access their mobile applications.

There are two ways to make this authentication system available. This authentication can be configured at time of application development by using the MaaS360 Mobile Application Security SDK, or can be enabled through application wrapping in the MaaS360 portal. Application wrapping is a simple process where the IT administrators clicks each of the application security policies needed, and MaaS360 seamlessly wraps the application without any coding by the developer.

If you are building a Worklight application, these two choices are available to you as well to protect the access to the application. IBM Worklight also has a security framework that you can use to control the access of the application with credentials. MaaS360 and Worklight are similar in this area, where the Worklight security framework can be configured to also use your corporate repository to access the application, but in the case of Worklight, this authentication can also be used to secure access to back-end services.

In general, you will secure the access to the application with the same realm as the access to the backend-data (the adapters). Another important element that you want to consider is that Worklight gives you much flexibility in the user experience during the login process, you can create the exact UI that you need and that fits your corporate identity. For these reasons, you might want to use the Worklight security framework to secure access to the application.

Single sign-on between apps

Both MaaS360 and IBM Worklight have single sign-on capabilities that allow users to enter credentials only once to allow access to several mobile applications on the device without having to sign into each application separately, however, they are very different in nature.

The MaaS360 single sign-on is a convenient way to protect the access to a group of applications with 4-digit PINs. You configure the PIN in the MaaS360 app on the device and this PIN will be requested to access to the MaaS360 application. This system is very different from the Worklight single sign-on system. In IBM Worklight the sign sign-on is a feature of the Worklight security framework.

Remote access control and wiping data

Worklight MAM features are providing a way to disable the access to an application for a particular user and a particular device from the Worklight Console, in order to cover the scenario of a stolen or lost device.
With MaaS360 the same scenario is re-enforced mainly because the device is managed by the MDM system. If a device is lost or stolen, an IT administrator can do much more than disabling access to an app. The device can be wiped, or applications can be removed from the device. Having the device managed by MaaS360 provides much more capabilities in this area.
With MaaS360 you can block access to an application with a feature called ‘Selective Wipe’. With this feature you can block the access to a particular application, for a particular user and device, and also to selectively wipe the data stored in the application. It is up to the developer to decide the data that needs to be wiped out. If you are building a Worklight application, then most likely you are using Worklight JSONStore as a way to store securely application data, you would then probably want to wipe the content of the JSONStore when receiving a ‘business wipe’ event from the MaaS360 backend.

Using the MaaS360 secured container to strengthen the application security

MaaS360 provides a secured container to strengthen the security of your application. This secured container can improve the security on the device, for example by restricting the access to the application if the device is jailbroken, and improve the security of the application data for example by disabling the copy paste operation so that no data can be pasted to an application that is not whitelisted.

MaaS360 provides two ways to enhance the security of an application. First through application wrapping, in this case the wrapping operation enforces a policy on the application by wrapping the existing application with the MaaS360 container. The second way is to use an SDK, that provides more flexibility in the way the app will react and enforce compliance.

If you are building a Worklight application, you can use both methods, but since you are building the application with Worklight, a more natural choice is to use the SDK and let the developer secure the app through the programming interface that is provided by the SDK.

To simplify this integration, the MaaS360 SDK contains all what is needed to use the MaaS360 in a Worklight application: The MaaS360 SDK is available packaged as a Worklight Application Component, a packaging that greatly simplifies the injection of the necessary libraries in your Worklight application. The SDK is available for native application and also for hybrid applications through a Cordova plugin, and an example of integration is provided.

IBM Worklight Application Center is an enterprise application store. With the Application Center, you can install, configure, and administer a repository of mobile applications for use by individuals and groups across your enterprise. You can control who in your organization can access the Application Center and upload applications to the Application Center repository, and who can download and install these applications onto a mobile device. You can also use the Application Center to collect feedback from users and access information about devices on which applications are installed.

MaaS360 also provides an enterprise application store, which serves the same goal as the Worklight application center. Through the MaaS360 app store you also create a repository of mobile applications for your employees, but MaaS360 is managing devices and applications, so the MaaS360 store has more control over the applications that are installed on the device when the employee device is managed. For example, MaaS360 can do the inventory of applications on the device, can push application and updates on a particular device, but these features are not possible when the device is not under control of MDM. So if you are using MaaS360, you will then rely on the MaaS360 app store for publishing applications to your employees.

The Worklight Application Center might still be useful in a development environment context. Development teams in your organization may setup a version of the Worklight application center for delivering applications before they are ready for publishing in the MaaS360 app store so that all the stakeholders can have an easy access to beta and pre-release versions.

Delivering application updates

The ability to deliver application updates for hybrid application (also known as “Direct Update”) is a key feature of Worklight. Whenever a user starts a mobile hybrid application (that is a mobile application with a portion of the logic and user interface by using web technologies : HTML5 CSS), the application communicates with a server. By using this server, IBM Worklight can determine whether a newer version of the application hybrid part (HTML, CSS, JavaScript) is available, and if so, give information to the user about it, or push an application update to the device. The server can also force an upgrade to the latest version of an application to prevent continued use of an outdated version. This ability is very useful to deliver updates of applications and also fix defect without any interaction from the user.

This system of Worklight is useful for an update of the hybrid part of the application, but when the native part of the application needs to be changed (for example a new OS version requires

to update and recompile the native application) Worklight cannot help you and you need to publish a new version in your enterprise app store.

If you are using MaaS360 and the device are managed by MaaS360 MDM, then you are able in this situation to push the new version of the application through the MaaS360 app store. You are then combining the best of both products: the ability to update easily and transparently the hybrid part of hybrid applications and also push new native applications to a device when needed.

Monitoring your environment

IBM Worklight includes a range of operational analytics and reporting mechanisms for collecting, viewing, and analyzing data from your IBM Worklight applications and servers, and for monitoring server health.

In addition to reports that summarize app activity, IBM Worklight includes a scalable operational analytics platform accessible in the Worklight Console. The analytics feature enables enterprises to search across logs and events that are collected from devices, apps, and servers for patterns, problems, and platform usage statistics. You can enable analytics, reports, or both, depending on your needs.

On the other hand, the cloud-based console of MaaS360 is really about monitoring the managed devices and their status again the policies that the IT administrator is enforcing.

The two administration tools are complementary to ensure that the device policy is enforced on devices and to monitor application activity and application health.

References

http://www.maas360.com/
http://www.ibm.com/developerworks/mobile/worklight/

Notices

property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan Ltd.

1623-14, Shimotsuruma, Yamato-shi

Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web

sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

Dept F6, Bldg 1

294 Route 100

Somers NY 10589-3216

USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Copyright

Trademarks

IBM, the IBM logo, ibm.com, and Worklight are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. MaaS360 is a trademark or registered trademark of Fiberlink, an IBM Company. Other product

and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Other company products or service names may be trademarks or service marks of others.