Protect

fork and edit tutorial (https://github.ibm.com/MFPSamples/DevCenter/tree/master/tutorials/en/product-integration/8.0/protect.html) | report issue (https://github.ibm.com/MFPSamples/DevCenter/issues/new)

MobileFirst Protect 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 MobileFirst Platform lets you build, run and manage HTML5, hybrid and native mobile apps.

If you are using MobileFirst Protect as the enterprise mobility management solution to enable your BYOD strategy and the MobileFirst 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.

Jump to:

- Introducing MobileFirst Platform and MobileFirst Protect
- Building mobile applications for your employees that connect to enterprise services
- Securing application with user authentication
- Single sign-on between apps
- Remote access control and wiping data
- Using the MobileFirst Protect secured container to strengthen the application security
- Application publishing
- Delivering application updates
- Monitoring your environment
- References

Introducing MobileFirst Platform and MobileFirst Protect

MobileFirst Protect 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 MobileFirst Protect 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. MobileFirst Protect 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 MobileFirst Protect are:

MobileFirst Protect Management Suite

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

- **MobileFirst Protect Devices**
  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.

- **MobileFirst Protect Applications**
  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
- **MobileFirst Protect Expenses**
  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
- **MobileFirst Protect Content**
  IBM MobileFirst Protect Content allows the administrator to add and distribute documents to supported devices. It includes MobileFirst Protect Doc Catalog, an on-device, password-protected container that provides a secure and simple way for users to access, view, and share documents. It includes seamless access to distributed content and repositories such as Microsoft SharePoint, Box, and Google Drive. Access to private Microsoft SharePoint and Microsoft Windows File Shares are available with the MobileFirst Protect Enterprise Gateway. Documents managed through MobileFirst Protect can be version controlled, audited, and secured through data loss prevention (DLP) policy options, such as require authentication, restrict copy-paste functionality, and block from being opened or shared in other applications.

MobileFirst Protect 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

- **MobileFirst Protect Secure Mail**
  An intuitive personal information management (PIM) app with email, calendar and contacts for iOS, Android and Windows Phone devices
- **MobileFirst Protect 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
- **MobileFirst Protect Mobile Application Security**
  Provides a mobile application container with full operational and security management to protect against data leaks for iOS and Android devices
- **MobileFirst Protect Content**
  IBM MobileFirst Protect Content allows the administrator to add and distribute documents to supported devices. It includes MobileFirst Protect Doc Catalog, an on-device, password-protected container that provides a secure and simple way for users to access, view, and share documents. It includes seamless access to distributed content and repositories such as Microsoft SharePoint, Box, and Google Drive. Access to private Microsoft SharePoint and Microsoft Windows File Shares are available with the MobileFirst Protect Enterprise Gateway. Documents managed through MobileFirst Protect can be version controlled, audited, and secured through data loss prevention (DLP) policy options, such as require authentication, restrict copy-paste functionality, and block from being opened or shared in other applications.

- **MobileFirst Protect Applications**
  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

MobileFirst Protect Content Suite

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.

- **MobileFirst Protect Content**
  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
- **MobileFirst Protect Document Editor**
  An office productivity app to create, edit, and save documents on iOS and Android devices and designed to prevent corporate data leaks
- **MobileFirst Protect Document Sync**
  Enables users to easily and securely synchronize content across managed iOS mobile devices

MobileFirst Protect Threat Management

IBM MobileFirst Protect Threat Management delivers a state-of-the-art system to protect against mobile malware on iOS and Android devices. You can gain visibility of these mobile risks and remediate the threats before they compromise your enterprise data. Through integration with IBM Security Trusteer®, leveraged by hundreds of millions of end users to protect organizations against fraud and data breaches, MobileFirst Protect provides a new layer of mobile security to Enterprise Mobility Management (EMM).

MobileFirst Protect Gateway Suite

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

- **MobileFirst Protect Gateway for Browser**
  Delivers access to enterprise intranet and internal websites without requiring a full device level VPN connection on iOS and Android devices
- **MobileFirst Protect Gateway for Documents**
  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
- **MobileFirst Protect Gateway for Applications**
  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: MobileFirst Protect Applications simplifies the distribution of applications to your employees and MobileFirst Protect Mobile Application Security enables secure containment of corporate data in your applications.

IBM MobileFirst Platform 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 MobileFirst Platform Foundation are:

MobileFirst Platform Studio

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

MobileFirst Platform Server

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

MobileFirst Platform 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.

MobileFirst Platform Operations Console

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

MobileFirst Platform 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 MobileFirst Platform will help you build mobile applications for your employees. With the MobileFirst Studio development tools, IBM MobileFirst Platform 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 crossplatform 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 MobileFirst Platform 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 MobileFirst Platform can act as this middleware solution and make communication with back-end services easier and seamless.

To achieve this integration MobileFirst Platform defines the notion of an adapter. Adapters are server-side code that is deployed on and serviced by the MobileFirst server component. An adapter connects the mobile application with the enterprise back-end service and performs any necessary application logic.

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

MobileFirst Protect Productivity Suite and MobileFirst Protect Content Suite , powered by MobileFirst Protect Gateway Suite 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.

MobileFirst Protect 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 MobileFirst Protect Management Suite, 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.

MobileFirst Protect Applications 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.

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

Securing application with user authentication

MobileFirst Protect 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 MobileFirst Protect 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 MobileFirst Protect Mobile Application Security SDK, or can be enabled through application wrapping in the MobileFirst Protect portal. Application wrapping is a simple process where the IT administrators clicks each of the application security policies needed, and MobileFirst Protect seamlessly wraps the application without any coding by the developer.

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

Single sign-on between apps

Both MobileFirst Protect and IBM MobileFirst Platform 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 MobileFirst Protect 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 MobileFirst Protect app on the device and this PIN will be requested to access to the MobileFirst Protect application. This system is very different from the MobileFirst single sign-on system. In IBM MobileFirst Platform the sign sign-on is a feature of the MobileFirst security framework.

Remote access control and wiping data

MobileFirst MAM features are providing a way to disable the access to an application for a particular user and a particular device from the MobileFirst Platform Operations Console, in order to cover the scenario of a stolen or lost device.

With MobileFirst Protect 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 MobileFirst Protect provides much more capabilities in this area. With MobileFirst Protect 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 MobileFirst Platform application, then most likely you are using 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 MobileFirst Protect backend.

Using the MobileFirst Protect secured container to strengthen the application security

MobileFirst Protect 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.

MobileFirst Protect 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 MobileFirst Protect 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 MobileFirst Platform application, you can use both methods, but since you are building the application with MobileFirst, 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 MobileFirst Protect SDK contains all what is needed to use the MobileFirst Protect in a MobileFirst Platform application: The MobileFirst Protect SDK is available packaged as a MobileFirst Application Component, a packaging that greatly simplifies the injection of the necessary

libraries in your MobileFirst Platform 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 MobileFirst Platform 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.

Application publishing

MobileFirst Protect also provides an enterprise application store, which serves the same goal as the MobileFirst Application Center. Through the MobileFirst Protect app store you also create a repository of mobile applications for your employees, but MobileFirst Protect is managing devices and applications, so the MobileFirst Protect store has more control over the applications that are installed on the device when the employee device is managed. For example, MobileFirst Protect 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 MobileFirst Protect, you will then rely on the MobileFirst Protect app store for publishing applications to your employees.

The MobileFirst Application Center might still be useful in a development environment context. Development teams in your organization may setup a version of the MobileFirst Application Center for delivering applications before they are ready for publishing in the MobileFirst Protect 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 MobileFirst Platform. 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 MobileFirst Platform 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 MobileFirst Platform 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) MobileFirst Platform cannot help you and you need to publish a new version in your enterprise app store.

If you are using MobileFirst Protect and the device are managed by MobileFirst Protect MDM, then you are able in this situation to push the new version of the application through the MobileFirst Protect 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 MobileFirst Platform includes a range of operational analytics and reporting mechanisms for collecting, viewing, and analyzing data from your IBM MobileFirst Platform applications and servers, and for monitoring server health.

In addition to reports that summarize app activity, IBM MobileFirst Platform includes a scalable operational analytics platform accessible in the MobileFirst Operations 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 MobileFirst Protect 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.mass360.com/)