Product Main Capabilities

Overview

With IBM MobileFirst Foundation, you can use capabilities such as development, testing, back-end connections, push notifications, offline mode, update, security, analytics, monitoring, and application publishing.

Development

IBM MobileFirst Foundation provides a framework that enables the development, optimization, integration, and management of secure mobile applications (apps). IBM MobileFirst Foundation does not introduce a proprietary programming language or model that users must learn.

You can develop apps by using HTML5, CSS3, and JavaScript. You can optionally write native code (Java or Objective-C). IBM MobileFirst Foundation provides an SDK that includes libraries that you can access from native code.

Back-end connections

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 the critical user-related functions. For example, customers can use a mobile application to shop anywhere, at any time, independent of the operating hours of the store. Their orders must still be processed by using the existing e-commerce platform of the store. To integrate a mobile application with enterprise services, you must use middleware such as a mobile gateway. IBM MobileFirst Foundation can act as this middleware solution and make communication with back-end services easier.

Push notifications

With push notifications, enterprise applications can send information to mobile devices, even when the application is not being used. IBM MobileFirst Foundation includes a unified notification framework which provides a consistent mechanism for such push notifications. With this unified notification framework, you can send push notifications without having to know the details of each targeted device or platform because each mobile platform has a different mechanism for push notification.

Offline mode

In terms of connectivity, mobile applications can operate offline, online, or in a mixed mode. IBM MobileFirst Foundation uses a client/server architecture that can detect whether a device has network connectivity, and the quality of the connection. Acting as a client, mobile applications periodically attempt to connect to the server and to assess the strength of the connection. An offline-enabled mobile application can be used when a mobile device lacks connectivity but some functions can be limited. When you create an offline-enabled mobile application, it is useful to store information about the mobile device that can help preserve its functionality in offline mode. This information typically comes from a back-end system, and you must consider data synchronization with the back end as part of the application architecture. IBM MobileFirst Foundation includes a feature that is called JSONStore for data exchange and storage. With this feature, you can create, read, update, and delete data records from a data source. Each operation is queued when operating offline. When a connection is available, the operation is transferred to the server and each operation is then performed against the source data.

Update

IBM MobileFirst Foundation simplifies version management and mobile application compatibility. Whenever a user starts a mobile application, the application communicates with a server. By using this server, IBM MobileFirst Foundation can determine whether a newer version of the application 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.

Security

Protecting confidential and private information is critical for all applications within an enterprise, including mobile applications. Mobile security applies at various levels, such as mobile application, mobile application services, or back-end service. You must ensure customer privacy and protect confidential data from being accessed by unauthorized users. Dealing with privately owned mobile devices means giving up control on certain lower levels of security, such as the mobile operating system.

IBM MobileFirst Foundation provides secure, end-to-end communication by positioning a server that oversees the flow of data between the mobile application and your back-end systems. With IBM MobileFirst Foundation, you can define custom security handlers for any access to this flow of data. Because any access to data of a mobile application has to go through this server instance, you can define different security handlers for mobile applications, web applications, and back-end access. With this kind of granular security, you can define separate levels of authentication for different functions of your mobile application. You can also prevent mobile applications from accessing sensitive information.

Analytics

The operational analytics feature enables searching across apps, services, devices, and other sources to collect data about usage, or to detect problems.

In addition to reports that summarize app activity, IBM MobileFirst Foundation 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.

Monitoring

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

Application publishing

IBM MobileFirst Foundation 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.

The concept of the Application Center is similar to the concept of the Apple public App Store or the Google Play store, except that it targets the development process.

The Application Center provides a repository for storing the mobile application files and a web-based

console for managing that repository. The Application Center also provides a mobile client application to allow users to browse the catalog of applications that are stored by the Application Center, install applications, leave feedback for the development team, and expose production applications to IBM® Endpoint Manager. Access to download and install applications from the Application Center is controlled by using access control lists (ACLs).