

# Using the MobileFirst Platform Operations Console

fork and edit tutorial (<https://github.ibm.com/MFPSamples/DevCenter/tree/master/tutorials/en/foundation/8.0/quick-start/console/index.md>)

| report issue (<https://github.ibm.com/MFPSamples/DevCenter/issues/new>)

## Overview

The MobileFirst Platform Operations Console is a web-based UI which enables simplified work flows for both the developer and the administrator to create, monitor, secure and administer applications & adapters.

Jump to:

- Accessing the console
- Navigating the console

## Accessing the console

The MobileFirst Operations Console can be accessed in the following ways:

### From a locally installed MobileFirst Server

#### Desktop Browser

From your browser of choice, load the URL `http://localhost:9080/mfpconsole` (`http://localhost:9080/mfpconsole`). The username/password are *admin/admin*.

#### Command-line

From a **Command-line** window, with the MobileFirst CLI installed, run the command: `mfpdev server console`.

### From a remotely installed MobileFirst Server

#### Desktop Browser

From your browser of choice, load the URL `http://the-server-host:server-port-number/mfpconsole`

The host server can be a customer-owner server, or running on a service such as Bluemix. The username/password are *admin/admin*.

#### Command-line

From a **Command-line** window, with the MobileFirst CLI installed,

1. Add a remote server definition:

##### *Interactive Mode*

Run the command: `mfpdev server add` and follow the on-screen instructions.

##### *Direct Mode*

Run the command with the following structure: `mfpdev server add [server-name] --URL [remote-server-URL] --login [admin-username] --password [admin-password] --contextroot [admin-service-name]`. For example:

```
mfpdev server add MyRemoteServer http://my-remote-host:9080/ --login TheAdmin --password ThePassword --contextroot mfpadmin
```

2. Run the command: `mfpdev server console MyRemoteServer`.

Learn more about the various CLI commands in the [Using CLI to manage MobileFirst artifacts \(../../using-the-mfpf-sdk/using-cli-to-manage-mobilefirst-artifacts/\)](#) tutorial.

## Navigating the console

### Dashboard

The Dashboard provides a glance view of the deployed projects.



### Runtime settings

Edit runtime properties such as Analytics server URL, global security variables, server keystore and confidential clients.



# Applications

## Creating applications

Provide basic application values and download Starter Code.

The screenshot shows the 'MobileFirst Operations Console' interface. On the left is a sidebar with navigation links: Dashboard, Runtimes, mfp (selected), Settings, Applications (with a 'Create new' button), Adapters (with a 'Create new' button), Devices, Client Logs, and Error Log. The main content area is titled 'Home > mfp > Register an Application'. It features a 'Register an Application' heading and a 'Choose Platform' section with radio buttons for Android, iOS (selected), Windows, and Windows Phone. Below this are input fields for 'Bundle ID \*', 'Application Identifier', and 'Version \*'. At the bottom is a 'Register application' button.

## Managing applications

Manage and configure registered applications by use of Direct Update ([../using-the-mfpf-sdk/direct-update/](#)), Remote Disable, Application Authenticity ([../authentication-and-security/application-authenticity/](#)), and setting security parameters ([../authentication-and-security/authentication-concepts/](#)).

The screenshot shows the 'MobileFirst Operations Console' interface for managing an application. The left sidebar shows a breadcrumb trail: < Back, mfp, Applications (with a 'Create new' button), and MyBankApp. Under 'MyBankApp', there is a 'Platform' section with a tree view showing 'iOS' (selected) and '1.0' (selected). The main content area is titled 'Home > mfp > MyBankApp > iOS 1.0' and includes a 'Delete version' button. It features a 'MyBankApp iOS v 1.0' heading and tabs for 'Management' (selected), 'Authenticity', 'Security', and 'Configuration Files'. Below the tabs, it shows 'Last modified: Jan 10, 2016, 8:03 AM'. The 'Application Access' section has a 'Status: \*' with radio buttons for 'Active' (selected), 'Active and Notifying', and 'Access Disabled'. The 'Direct Update' section includes a description: 'Update a Cordova cross-platform application by uploading a new web resource file.' and a box showing 'No Web Resources deployed' with an 'Upload File' button.

## Authentication and Security

Configure application security parameters.

MobileFirst Operations Console

Analytics ConsoleHello, demo

< Back

mfp

Applications

Create new

MyBankApp

Platform

^ iOS1

1.0

Push

Home > mfp > MyBankApp > iOS 1.0

Delete version

MyBankApp iOS v 1.0

ManagementAuthenticitySecurityConfiguration Files

Configurations

Maximum token expiration (seconds) \*

3600

Edit

Ipsum lorem

Map Scope Elements to Security Checks

Configure one or more authentications required for the client to get proper permissions for accessing a protected resource.

Create New

You didn't map scope elements to security checks yet

Get started by clicking "Create New"

Application Mandatory Scope

Configure one or more authentications required in order to get proper permissions for running the application. This can include out-of-the-box security checks or scope elements mapped to security checks.

Create New

## Notifications

Set-up push notifications ([../notifications/push-notifications-overview/](#)) and related parameters, such as tags, as well as sending notifications.

MobileFirst Operations Console

Analytics ConsoleHello, demo

< Back

mfp

Applications

Create new

MyBankApp

Platform

^ iOS1

1.0

Push

Home > mfp > MyBankApp > Push

Push

Send PushTagsPush Settings

Push Notification Settings

Configure your push notifications here. For detailed instructions, take a look at our [Push Notifications Guide](#)

Apple ProductionApple Sandbox

Apple Push Certificates for production

Learn more about how to generate and use APNS certificates here [Apple Push Certificates Guide](#)

Upload .p12 file \*

Password \*

Enter Password

Save

GCM Push Credentials

Learn more about how to set up Google Cloud Messaging here [Google Cloud Messaging Documentation](#)

## Adapters

### Creating adapters

Register an adapter and download Starter Code, as well as update an adapter on-the-fly by updating its properties without needing to re-build and re-deploy the adapter artifact.

MobileFirst Operations Console

Analytics ConsoleHello, demo

Dashboard

Runtimes

mfpmfp

Settings

Applications

Create new

No application deployed

Adapters

Create new

No adapter deployed

Devices

Client Logs

Error Log

Home > mfp > Create a new Adapter

Create a new Adapter

It seems like you don't have any adapters, lets get started

Deploy Adapter

Follow these steps to set up an adapter

Hide guide

1

Setting up your environment

Installing the command line interface (CLI)

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean euismod bibendum laoreet. Proin gravida dolor sit amet lacus accumsan et viverra justo commodo. Proin sodales pulvinar tempor.

Installing Maven

MVN Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean euismod bibendum laoreet. Proin gravida dolor sit amet lacus accumsan et viverra justo commodo. Proin sodales pulvinar tempor.

2

Start with a sample adapter

3

In your IDE of choice, edit the adapter code - REST end points and adapter descriptor

4

Build and package

5

Upload adapter

Adapter properties

After an adapter is deployed, it can be configured in the console.

MobileFirst Operations Console

Analytics ConsoleHello, demo

Dashboard

Runtimes

mfpmfp

Settings

Applications

Create new

com.ibm.hellocordova

old

Adapters

Create new

javaAdapter

Devices

Client Logs

Error Log

Home > mfp > javaAdapter

Delete

javaAdapter

ConfigurationsResourcesConfiguration Files

Resources

URL	Methods	Security
/users	GET	
/users/helloUserQuery	GET	
/users/newUsers	PUT	
/users/{first}/{middle}/{last}	POST	
/users/{username}	GET	

Devices

Administrators can search for devices that access the MobileFirst Server and can manage access rights. Devices can be searched for using either user ID or using a friendly name.

The user ID is the identifier that was used to log-in.

A friendly name is a name that is associated with the device to distinguish it from other devices that share the user ID. You can set the friendly name on the client by using the client-side JavaScript APIs:

`WL.Device.setFriendlyName` and `WL.Device.getFriendlyName`.

For more information, see the topic about device access management in the MobileFirst Operations Console in the user documentation.

replace with image showing logged devices



## Client logs

Administrators can use log profiles to adjust client logger configurations, such as log level and log package filters, for any combination of operating system, operating system version, application, application version, and device model.

When an administrator creates a configuration profile, the log configuration is concatenated with responses API calls such as `WLResourceRequest`, and is applied automatically.

For more information, see the topic about client-side log capture configuration from MobileFirst Operations Console in the user documentation.

replace with image showing client logs



## Error log

The Error log shows a list of the failed management operations that were initiated from the MobileFirst Operations Console, or from the command line, on the current runtime environment. Use the log to see the effect of the failure on the servers.

For more information, see the topic about error log of operations on runtime environments in the user documentation.



## License tracking

Accessible from the top Settings buttons.

License terms vary depending on which edition (Enterprise or Consumer) of MobileFirst Platform Foundation is being used. License tracking is enabled by default and tracks metrics relevant to the licensing policy, such as active client devices and installed applications. This information helps determine whether the current usage of MobileFirst Platform is within the license entitlement levels and can prevent potential license violations.

By tracking the usage of client devices and determining whether the devices are active, administrators can decommission devices that should no longer be accessing the service. This situation might arise if an employee has left the company, for example.

For more information, see the topic about license tracking in the user documentation.

replace with image showing license information

