Introduction to MobileFirst Platform Operations Console

Overview

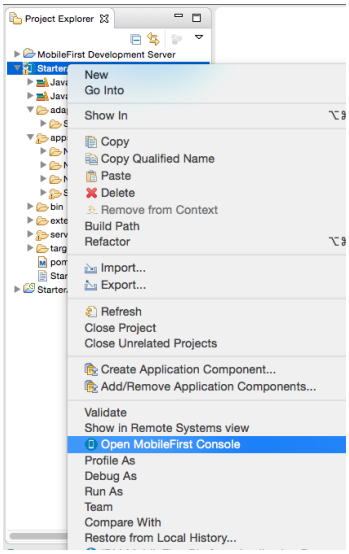
The MobileFirst Platform Operations Console is a web-based UI dedicated to the ongoing monitoring and administration of the deployed applications, adapters, and push notifications. The console also provides access to server logs (audit and error), Operational Analytics, device profiling, and more.

Agenda

- Accessing the console
- Navigating the console
- Console actions

Accessing the console

You can access the console in three ways.



1. ### From MobileFirst Studio

   To view the MobileFirst Operations Console, right-click the project name and select **Open MobileFirst Operations Console**.
   To view the MobileFirst Operations Console in an external browser window, from the top menu bar in Eclipse go to **Window > Preferences > General > Web Browser** and select **Use external web browser**.

2. ### From the command-line interface (CLI)

   `mfp console` – Opens the MobileFirst Operations Console in your default web browser.
   Learn more from Using CLI to create, build, and manage MobileFirst project artifacts (../../advanced-client-side-development/using-cli-to-create-build-and-manage-mobilefirst-project-artifacts/).

3. ### From a URL

   The console can also be accessed directly via its URL:
   `http://hostname:port/worklightconsole`

   If required, the default username and password for the console are `admin/admin`.

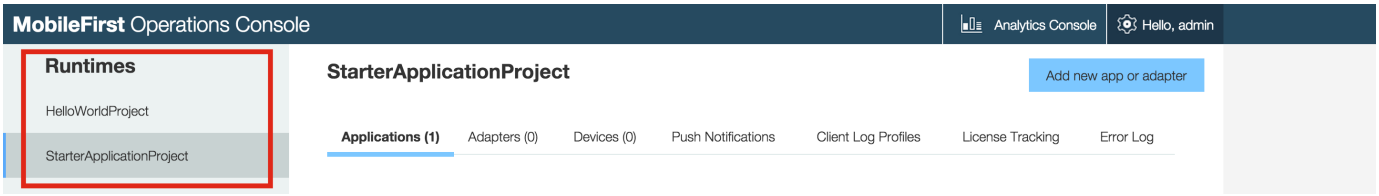
Navigating the console

Empty console

Before any project is deployed.

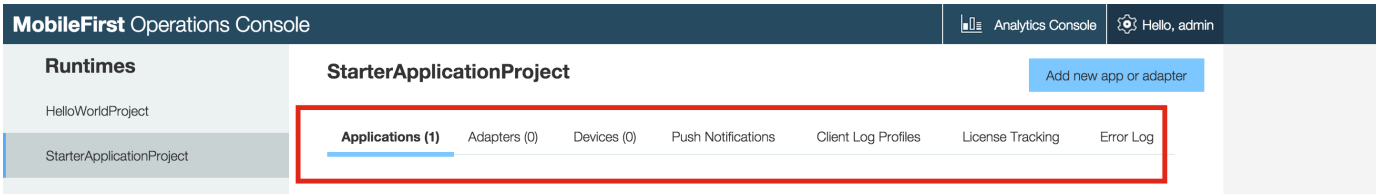
Multiple projects

All the projects currently deployed on the server appear in the console.



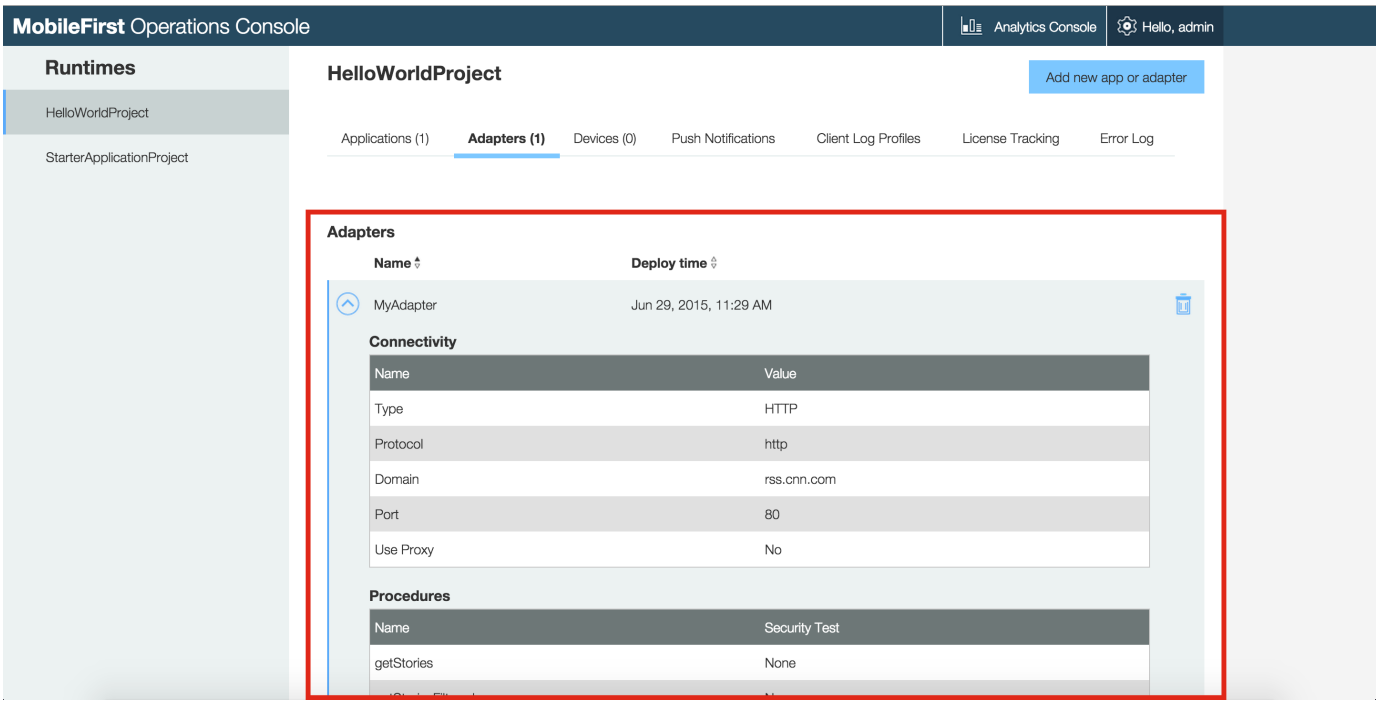
Project actions

When a project is selected, the different information views/available actions are shown.
See Console actions for more information.



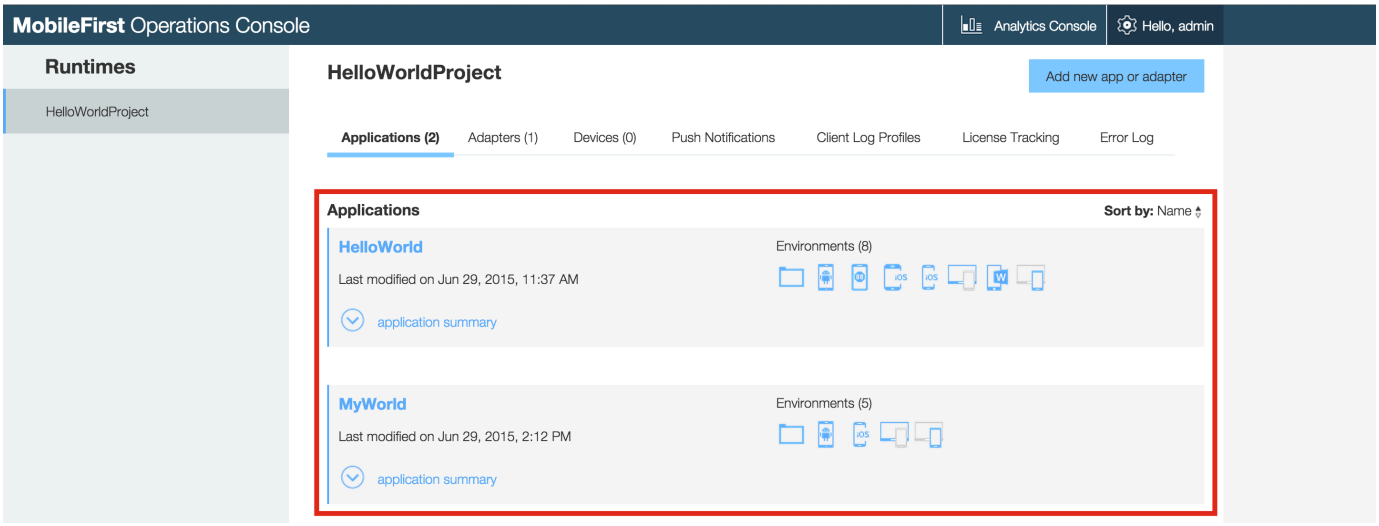
Adapters

Learn more about adapters from Server-side development (../../server-side-development/).



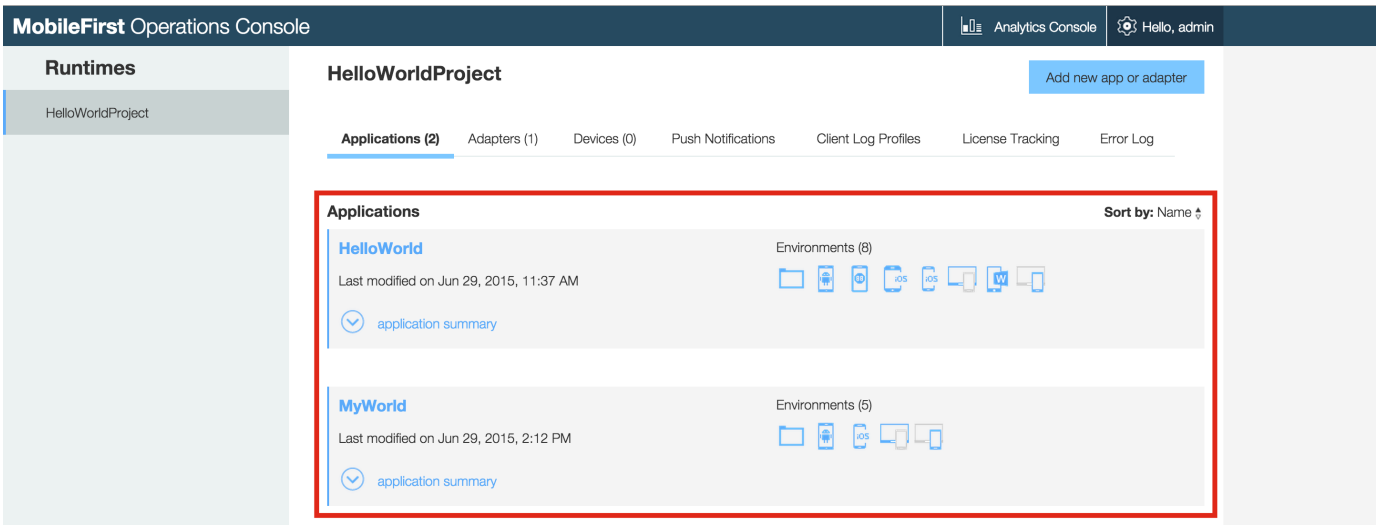
Applications

A project can contain several applications, sharing server-side components such as adapters.



Application details and environments

Click the name of an application to see more details about the application, including the list of environments. **Common Resources** allows you to preview the common resources of a hybrid application in the browser.



Environment details

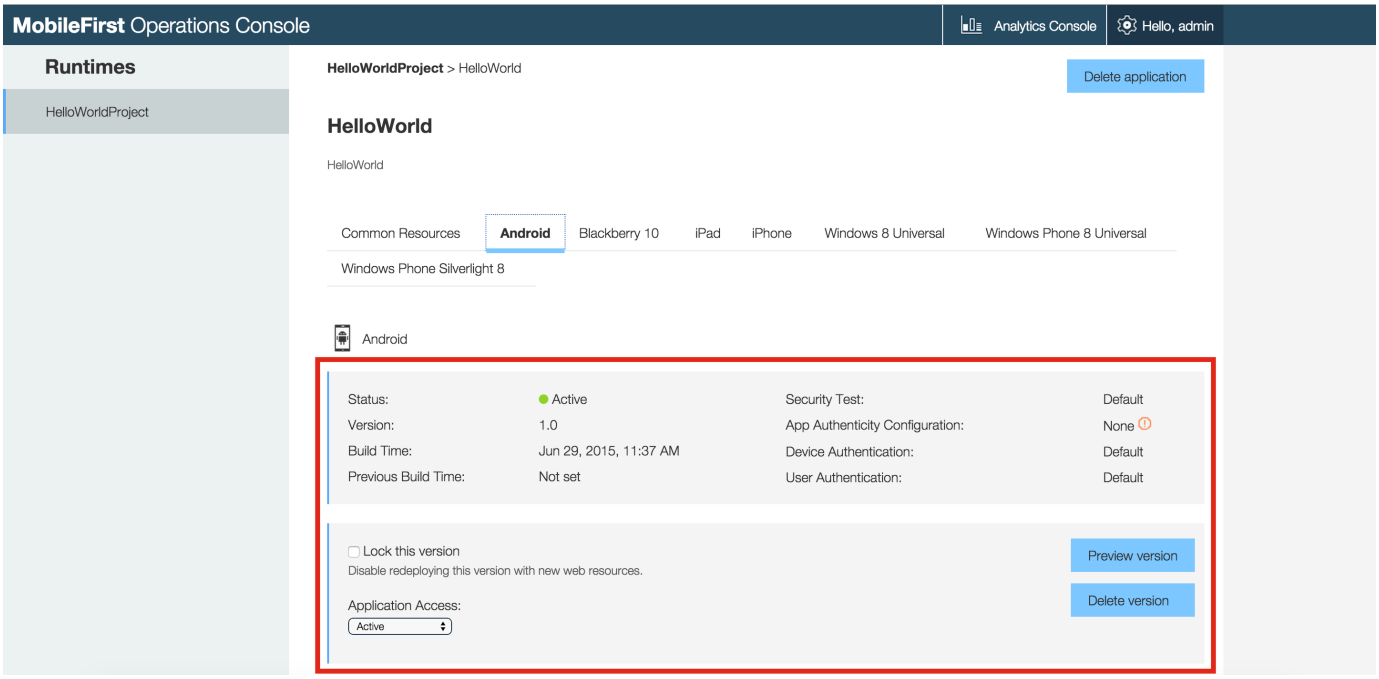
Expand an environment to see more details. Click the button to preview this specific environment.

Application access

By using the Remote Disable feature, an administrator can deny a user access to a certain application version, due to phase-out policy or due to security issues encountered in the application.

Authenticity

Learn more about application authenticity in the Application Authenticity Protection tutorial (../../authentication-security/application-authenticity-protection/).



Console actions

License tracking

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.

Devices

Administrators can search for devices that access the MobileFirst Server and can manage access rights.

You can search for devices on the user ID or on a friendly name.

- The user ID is the identifier that was used to log in to the authentication realm.
- 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.getFriendlyName` and `WL.Device.setFriendlyName`.

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

Client log profiles

Related tutorial: Remote controlled client-side log collection (../../advanced-client-side-development/remote-controlled-client-side-log-collection/)

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 to explicit WLClient `connect` and `invokeProcedure`/`WLResourceRequest` API calls, and is applied automatically.

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

Errors log

The Errors 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.

Audit log

The audit log provides information on administration operations such as login, logout, deploying apps or adapters, or locking apps. You can disable the audit log by setting the `ibm.worklight.admin.audit` JNDI property on the web application of the MobileFirst Administration Service (`worklightadmin.war`) to `false`.

> For more information, see the topic about audit log of administration operations, in the user documentation.