Using the MobileFirst Platform Operations Console

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

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 *demo/demo*.

Command-line

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

MobileFirst Studio

From MobileFirst in Eclipse, click on **Open MobileFirst 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 *demo/demo*.

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 TheAd
min --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 (../../client-side-development/using-cli-to-manage-mobilefirst-artifacts/) tutorial.

Navigating the console

Show the various pages in the console and what can be done in each of them

OLD CONTENT:

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 tutorial (../../authentication-security/application-authenticity/).

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.