Administrating applications through the MobileFirst Operations Console

Overview

You can administer MobileFirst applications through the MobileFirst Operations Console by locking apps or denying access, or by displaying notification messages.

You can start the console by entering one of the following URLs:

- Secure mode for production or test: `https://hostname:secure_port/mfpconsole`
- Development: `http://server_name:port/mfpconsole`

You must have a login and password that grant you authorization to access the MobileFirst Operations Console. For more information, see Configuring user authentication for MobileFirst Server administration (../../installation-configuration/production/server-configuration/#configuring-user-authentication-for-mobilefirst-server-administration).

You can use the MobileFirst Operations Console to manage your applications.

From the MobileFirst Operations Console, you can also access the Analytics console and control the collection of mobile data for analysis by the Analytics server. For more information, see Enabling or disabling data collection from the MobileFirst Operations Console (../../analytics/console/#enable-disable-analytics-support).

Jump to

Mobile-application management

The MobileFirst mobile-application-management capabilities provide MobileFirst Server operators and administrators with granular control over user and device access to their applications.

MobileFirst Server tracks all attempts to access your mobile infrastructure, and stores information about the application, the user, and the device on which the application is installed. The mapping between the application, the user, and the device, forms the basis for the server's mobile-application management capabilities.

Use IBM MobileFirst Operations Console to monitor and manage access to your resources:

- Search for a user by name, and view information about the devices and applications that they are using to access your resources.
- Search for a device by its display name, and view the users that are associated with the device, and the registered MobileFirst applications that are used on this device.
- Block access to your resources from all instances of your applications on a specific device. This is useful when a device is lost or stolen.
- Block access to your resources only for a specific application on a specific device. For example, if an employee changes departments, you can block the employee's access for an application of the previous department, but allow the employee access from other applications on the same device.
- Unregister a device, and delete all the registration and monitoring data that was gathered for the device.

Access-blocking has the following characteristics:

- The blocking operation is reversible. You can remove the block by changing the device or application status in MobileFirst Operations Console.
- The block applies only to protected resources. A blocked client can still use the application to access an unprotected resource. See Unprotected resources.
- Access to adapter resources on MobileFirst Server is blocked immediately when you select this operation. However, this might not be the case for resources on an external server because the application might still have a valid access token that has not expired.

Device status

MobileFirst Server maintains status information for every device that accesses the server. The possible status values are **Active**, **Lost**, **Stolen**, **Expired**, and **Disabled**.

The default device status is **Active**, which indicates that access from this device is not blocked. You can change the status to **Lost**, **Stolen**, or **Disabled** to block access to your application resources from the device. You can always restore the **Active** status to allow access again. See Managing device access in MobileFirst Operations Console.

The **Expired** status is a special status that is set by MobileFirst Server after a preconfigured inactivity duration elapses since the last time that the device connected to this server instance. This status is used for license tracking, and it does not affect the access rights of the device. When a device with an **Expired** status reconnects to the server, its status is restored to **Active**, and the device is granted access the server.

Device display name

MobileFirst Server identifies devices by a unique device ID, which is assigned by the MobileFirst client SDK. Setting a display name for a device allows you to search for the device by its display name. Application developers can use the setDeviceDisplayName method of the WLClient class to set the device display name. See the WLClient documentation in MobileFirst client-side API (http://www.ibm.com/support/knowledgecenter/SSHS8R_8.0.0/com.ibm.worklight.apiref.doc/apiref/r_ibm_worklight_client_side_api_.html). (The JavaScript class is **WL.Client.**) Java adapter developers (including security-check developers) can also set the device display name by using the setDeviceDisplayName method of the `com.ibm.mfp.server.registration.external.model` **MobileDeviceData** class. See MobileDeviceData (http://www.ibm.com/support/knowledgecenter/en/SSHS8R_8.0.0/com.ibm.worklight.apiref.doc/html/refobjc-worklight-ios/html/Classes/WLResourceRequest.html?view=kc).

Managing device access in MobileFirst Operations Console

To monitor and manage device access to your resources, select the Devices tab in the MobileFirst Operations Console dashboard.

Use the search field to search for a device by the user ID that is associated with the device, or by the display name of the device (if set). See Device display name. You can also search for part of the user ID or the device display name (at least three characters).

The search results display all the devices that match the specified user ID or device display name. For each device, you can see the device ID and display name, the device model, the operating system, and the list of users IDs that are associated with the device.

The Device Status column shows the status of the device. You can change the status of the device to **Lost**, **Stolen**, or **Disabled**, to block access from the device to protected resources. Changing the status back to **Active** restores the original access rights.

You can unregister a device by selecting **Unregister** in the **Actions** column. Unregistering a device deletes the registration data of all the MobileFirst applications that are installed on the device. In addition, the device display name, the lists of users that are associated with the device, and the public attributes that the application registered for this device are deleted.

Note: The **Unregister** action is not reversible. The next time that one of the MobileFirst applications on the device attempts to access the server, it will be registered again with a new device ID. When you select to register the device again, the device status is set to **Active**, and the device has access to protected resources, regardless of any previous blocks. Therefore, if you want to block a device, do not unregister it. Instead, change the device status to **Lost**, **Stolen**, or **Disabled**.

To view of all the applications that were accessed on a specific device, select the expand arrow icon next to the device ID in the devices table. Each row in the displayed applications table contains the name of the application, and the application's access status (whether access to protected resources is enabled for this application on this device). You can change the application's status to **Disabled** to block access from the application specifically on this device.

Jump to

Remotely disabling application access to protected resources

Use MobileFirst Operations Console (the console) to disable user access to a specific version of an application on a specific mobile operating system, and provide a custom message to the user.

1. Select your application version from the **Applications** section of the console's navigation sidebar, and then select the application **Management** tab.
2. Change the status to **Access Disabled**.
3. In the **URL of latest version** field, optionally provide a URL for a newer version of the application (usually in the appropriate public or private app store). For some environments, the Application Center provides a URL to access the Details view of an application version directly. See Application properties (../../appcenter/appcenter-console/#application-properties).
4. In the **Default notification message** field, add the custom notification message to display when the user attempts to access the application. The following sample message directs users to upgrade to the latest version:

```
This version is no longer supported. Please upgrade to the latest version.
```

5. In the **Supported locales** section, you can optionally provide the notification message in other languages.
6. Select **Save** to apply your changes.

When a user runs an application that was remotely disabled, a dialog window with your custom message is displayed. The message is displayed on any application interaction that requires access to a protected resource, or when the application tries to obtain an access token. If you provided a version-upgrade URL, the dialog has a **Get new version** button for upgrading to a newer version, in addition to the default **Close** button. If the user closes the dialog window without upgrading the version, they can continue to work with the parts of the application that do not require access to protected resources. However, any application interaction that requires access to a protected resource causes the dialog window to be displayed again, and the application is not granted access to the resource.

Displaying an administrator message

Follow the outlined procedure to configure the notification message. You can use this message to notify application users of temporary situations, such as a planned service downtime.

1. Select your application version from the **Applications** section of the MobileFirst Operations Console navigation sidebar, and then select the application Management tab.
2. Change the status to **Active and Notifying**.
3. Add a custom startup message. The following sample message informs the user of planned maintenance work for the application:

   ```
   The server will be unavailable on Saturday between 4 AM to 6 PM due to planned maintenance.
   ```

4. In the Supported locales section, you can optionally provide the notification message in other languages.
5. Select **Save** to apply your changes.

The message is displayed when the application first uses MobileFirst Server to access a protected resource, or obtain an access token. If the application acquires an access token when it starts, the message is displayed at this stage. Otherwise, the message is displayed on the first request from the application to access a protected resource or obtain an access token. The message is displayed only once, for the first interaction.

Defining administrator messages in multiple languages

Follow the outlined procedure to configure multiple languages for displaying the application administration messages that you defined through the console. The messages are sent based on the locale of the device, and must comply with the standards that the mobile operating system uses to specify locales.

1. Select your application version from the **Applications** section of the MobileFirst Operations Console navigation sidebar, and then select the application **Management** tab.
2. Select the status **Active and Notifying** or **Access Disabled**.
3. Select **Update Locales**. In the **Upload File** section of the displayed dialog window, select **Upload**, and browse to the location of a CSV file that defines the locales.

   Each line in the CSV file contains a pair of comma-separated strings. The first string is the locale code (such as fr-FR for French (France) or en for English), and the second string is the message text in the corresponding language. The specified locale codes must comply with the standards that the mobile operating system uses to specify locales, such as ISO 639-1, ISO 3166-2, and ISO 15924.

   > **Note:** To create the CSV file, you must use an editor that supports UTF-8 encoding, such as Notepad.

   Following is a sample CSV file that defines the same message for multiple locales:

   ```
   en,Your application is disabled
   en-US,Your application is disabled in US
   en-GB,Your application is disabled in GB
   fr,votre application est désactivée
   he,האפליקציה חסמומה
   ```

4. In the **Verify notification message** section, you can see a table of the locale codes and messages from your CSV file. Verify the messages, and select **OK**. You can select Edit, at any time, to replace the locales CSV file. You can also use this option to upload an empty CSV file to remove all locales.
5. Select **Save** to apply your changes.

The localized notification message is displayed on the user's mobile device, according to the locale of the device. If no message was configured for the device locale, the default message that you provided is displayed.

Application status and token licensing

You must manually restore the correct application status in MobileFirst Operations Console after Blocked status because of insufficient tokens.

If you use token licensing and you no longer have enough license tokens for an application, the application status of all versions of the application changes to **Blocked**. You are no longer able to change the status of any version of the application. The following message is displayed in MobileFirst Operations Console:

> The application got blocked because its license expired

If later enough tokens to run the application become free or your organization purchases more tokens, the following message is displayed in MobileFirst Operations Console:

> The application got blocked because its license expired but a license is available now

The display status is still **Blocked**. You must restore the correct current status manually from memory or your own records by editing the Status field. IBM MobileFirst Foundation does not manage the display of **Blocked** status in MobileFirst Operations Console of an application that was blocked because of insufficient license tokens. You are responsible for restoring such a blocked application to a real status that can be displayed through MobileFirst Operations Console.

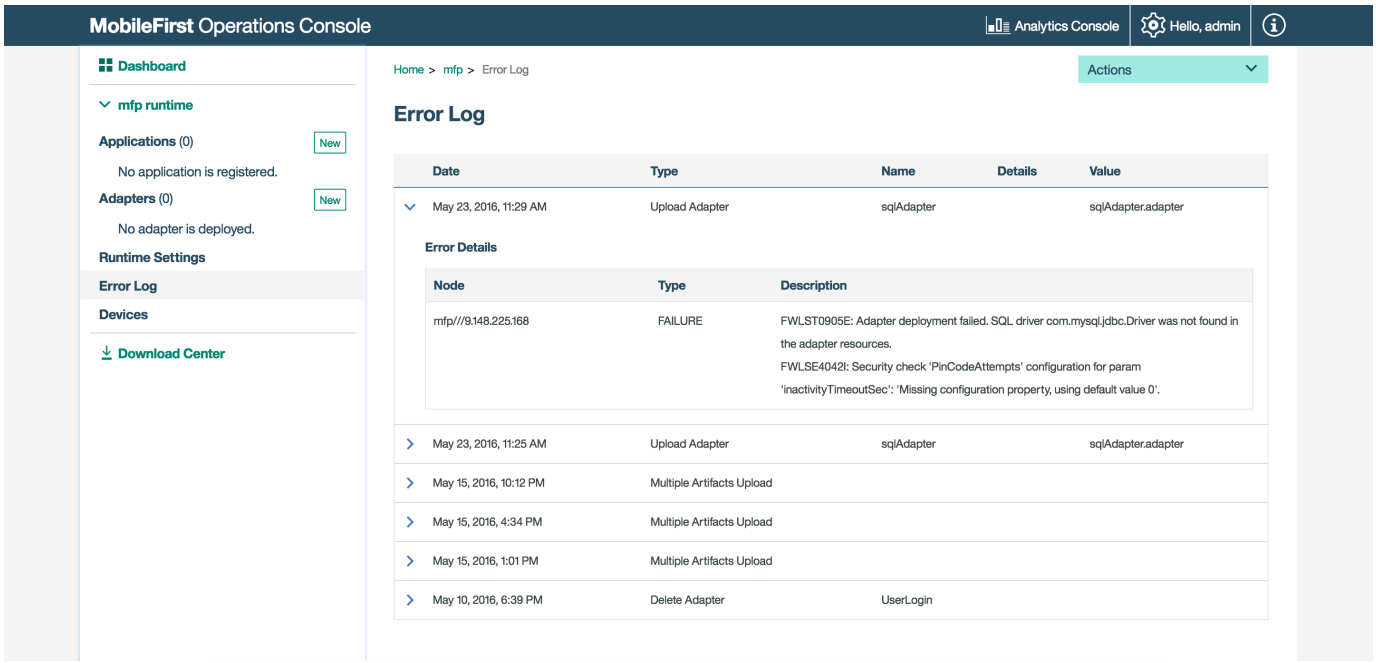
Error log of operations on runtime environments

Use the error log to access failed management operations initiated from MobileFirst Operations Console or the command line on the selected runtime environment, and to see the effect of the failure on the servers.

When a transaction fails, the status bar displays a notification of the error and shows a link to the error log. Use the error log to have more detail about the error, for example, the status of each server with a specific error message, or to have a history of errors. The error log shows the most recent operation first.

You access the error log by clicking **Error log** of a runtime environment in MobileFirst Operations Console.

Expand the row that refers to the failed operation to access more information about the current state of each server. To access the complete log, download the log by clicking **Download log**.



Audit log of administration operations

In the MobileFirst Operations Console, you can refer to an audit log of administration operations.

MobileFirst Operations Console provides access to an audit log for login, logout, and all administration operations, such as deploying apps or adapters or locking apps. The audit log can be disabled by setting the **mfp.admin.audit** Java Naming and Directory Interface (JNDI) property on the web application of the MobileFirst administration service to **false**.

To access the audit log, click the user name in the header bar and select **About**, click **Additional support information**, and then **Download audit log**.

Field name	Description
Timestamp	Date and time when the record was created.
Type	The type of operation. See list of operation types below for the possible values.
User	The **username** of the user who is signed in.
Outcome	The outcome of the operation; possible values are SUCCESS, ERROR, PENDING.
ErrorCode	If the outcome is ERROR, ErrorCode indicates what the error is.
Runtime	Name of the MobileFirst project that is associated with the operation.

The following list shows the possible values of Type of operation.

- Login
- Logout
- AdapterDeployment
- AdapterDeletion
- ApplicationDeployment
- ApplicationDeletion
- ApplicationLockChange
- ApplicationAuthenticityCheckRuleChange
- ApplicationAccessRuleChange
- ApplicationVersionDeletion
- add config profile
- DeviceStatusChange
- DeviceApplicationStatusChange
- DeviceDeletion
- unsubscribeSMS
- DeleteDevice
- DeleteSubscriptions
- SetPushEnabled
- SetGCMCredentials
- DeleteGCMCredentials
- sendMessage
- sendMessages
- setAPNSCredentials
- DeleteAPNSCredentials
- setMPNSCredentials
- deleteMPNSCredentials
- createTag
- updateTag
- deleteTag
- add runtime
- delete runtime

Last modified on