

Application Authenticity

Overview

By issuing an HTTP request, any entity can access the HTTP services (APIs) that IBM MobileFirst Platform Foundation Server offers.

The out-of-the-box Application Authenticity security check ([../authentication-concepts/](#)) ensures that an application that tries to connect to a MobileFirst Server instance is the authentic one and was not tampered with or modified by a third-party attacker.

To enable Application Authenticity protection you can either follow the on-screen instructions in the MobileFirst Operations Console → [your-application] → Authenticity, or review the information below.

Availability

Application Authenticity is available in all supported platforms (iOS, Android, Windows 8.1 Universal, Windows 10 UWP) in both Cordova and Native applications.

Note: Application Authenticity is **not available** in the MobileFirst Development Server. To test, use a remote application server such as a QA, UAT or Production server.

Jump to:

- [Authenticity flow \(authenticity-flow\)](#)
- [Enabling authenticity \(enabling-application-authenticity\)](#)
- [Disabling authenticity \(disabling-application-authenticity\)](#)
- [Configuring authenticity \(configuring-application-authenticity\)](#)

Authenticity Flow

Application Authenticity is based on certificate keys that are used to sign the application bundles. Only the developer or the enterprise who have the original private key that was used to create the application are able to modify, repack, and re-sign the bundle.

Once an application has successfully registered with the MobileFirst Server, and passed the Authenticity challenge, an Authenticity token is granted. For as long as the token is valid, the Authenticity challenge will not occur again. See [Configuring authenticity \(configuring-authenticity\)](#) to learn how this can be customized.



The challenge token in the diagram is processed by compiled native code, so that third-party attackers cannot see the logic of this processing.

Enabling Application Authenticity

In order to enable Application Authenticity in your Cordova or Native application, the application's binary file needs to be signed using the MobileFirst-supplied command line tool. Eligible binary files are: `ipa` for iOS, `apk` for Android and `appx` for Windows 8.1 Universal & Windows 10 UWP.

1. Open a **Command-line** window and run the command: `java -jar path-to-mfp-server-authenticity-tool.jar path-to-binary-file`

For example:

```
java -jar /Users/idanadar/Desktop/mfp-server-authenticity-tool.jar /Users/idanadar/Desktop/MyBankApp.ipa
```

The result of the command above is a `.authenticity_data` file generated next to the `MyBankApp.ipa` file, called `MyBankApp.authenticity_data`.

2. Open the MobileFirst Operations Console in your browser of choice.
3. Select your application from the left-side pane and click on the Authenticity menu item.
4. Click on "Upload Authenticity File" to upload the `.authenticity_data` file.

Once the `.authenticity_data` file is uploaded, Application Authenticity is now enabled.

The screenshot shows the MobileFirst Operations Console interface. On the left, a sidebar contains a 'Back' link, the application name 'mfp', and a list of applications under 'Applications'. The main application 'com.worklight.MyBankApp' is selected, showing its platform as 'iOS' and version as '1.0'. The right pane displays the 'Application Authenticity' settings for 'com.worklight.MyBankApp iOS v 1.0'. The 'Authenticity' tab is active, showing a status of 'Disabled'. A message states: 'Activating Application Authenticity protection ensures that the only the authentic application binary is able to communicate with the MobileFirst Server.' Below this, a warning icon and text recommend enabling Application Authenticity. A button 'Upload Authenticity File' is visible. A section titled 'Follow these steps to set up Application Authenticity' lists three steps: 1. Download the Application Authenticity tool, 2. Create the Authenticity File, and 3. Upload the Authenticity File.

Disabling Application Authenticity

In order to disable Application Authenticity, click the "Delete Authenticity File" button.

This screenshot shows the same MobileFirst Operations Console interface as the previous one, but the 'Application Authenticity' status is now 'Enabled'. A green checkmark icon and a message 'Successfully uploaded the Authenticity File.' are displayed at the top of the settings pane. The 'Delete Authenticity File' button is now visible in the top right corner of the settings area. The 'Follow these steps to set up Application Authenticity' section remains the same.

Configuring Application Authenticity

The Application Authenticity out-of-the-box security check can be configured with the following property:

- `expirationInSec`: Defaults to 3600 seconds / 1 hour. Defines the duration until the Authenticity token expires.

Once an authenticity check has been performed, it will not be performed again until the token has expired based on the set value.

To configure the `expirationInSec` property:

1. Load the MobileFirst Operations Console and navigate to **[your application] → Security → Security Check Configurations** and click on **Create New**.
2. Search for the "appAuthenticity" scope element.

3. Set a new value in seconds.

