Federal standards support in MobileFirst Foundation

Overview

IBM MobileFirst Foundation supports Federal Desktop Core Configuration (FDCC), and United States Government Configuration Baseline (USGCB) specifications. IBM MobileFirst Foundation also supports the Federal Information Processing Standards (FIPS) 140-2, which is a security standard that is used to accredit cryptographic modules.

Jump to

FDCC and USGCB support

The United States federal government mandates that federal agency desktops that run on Microsoft Windows platforms adopt Federal Desktop Core Configuration (FDCC) or the newer United States Government Configuration Baseline (USGCB) security settings.

IBM® Worklight® V5.0.6 was tested by using the USGCB and FDCC security settings via a self-certification process. Testing includes a reasonable level of testing to ensure that installation and core features function on this configuration.

References

For more information, see USGCB (http://usgcb.nist.gov/).

FIPS 140-2 support

Federal Information Processing Standards (FIPS) are standards and guidelines that are issued by the United States National Institute of Standards and Technology (NIST) for federal government computer systems. FIPS Publication 140-2 is a security standard that is used to accredit cryptographic modules. IBM MobileFirst Foundation provides FIPS 140-2 support for Android and iOS Cordova apps.

FIPS 140-2 on the MobileFirst Server, and SSL communications with the MobileFirst Server

The IBM MobileFirst Foundation server runs in an application server, such as the WebSphere® Application Server. The WebSphere Application Server can be configured to enforce the use of FIPS 140-2 validated cryptographic modules for inbound and outbound Secure Socket Layer (SSL) connections. The cryptographic modules are also used for the cryptographic operations that are performed by the applications by using the Java Cryptography Extension (JCE). Since the MobileFirst Server is an application that runs on the application server, it uses the FIPS 140-2 validated cryptographic modules for the inbound and outbound SSL connections.

When an IBM MobileFirst Foundation client transacts a Secure Socket Layer (SSL) connection to a MobileFirst Server, which is running on an application server that is using the FIPS 140-2 mode, the results are the successful use of the FIPS 140-2 approved cipher suite. If the client platform does not

support one of the FIPS 140-2 approved cipher suites, the SSL transaction fails and the client is not able to establish an SSL connection to the server. If successful, the client uses a FIPS 140-2 approved cipher suite.

> **Note:** The cryptographic module instances that are used on the client are not necessarily FIPS 140-2 validated. For options to use FIPS 140-2 validated libraries on client devices, see below.

Specifically, the client and server are using the same cipher suite (SSL*RSA*WITH*AES*128*CBC*SHA for example), but the client side cryptographic module perhaps did not go through the FIPS 140-2 validation process, whereas the server side is using FIPS 140-2 certified modules.

FIPS 140-2 on the MobileFirst client device for protection of data at rest in JSONStore and data in motion when using HTTPS communications

Protection of data at rest on the client device is provided by the JSONStore feature of IBM MobileFirst Foundation. Protection of data in motion is provided by the use of HTTPS communication between the MobileFirst client and the MobileFirst Server.

On iOS devices, the FIPS 140-2 support is enabled by default for both data at rest and data in motion.

Android devices use non-FIPS 140-2 validated libraries by default. There is an option to use FIPS 140-2 validated libraries for the protection (encryption and decryption) of the local data that is stored by JSONStore and for the HTTPS communication to the MobileFirst Server. This support is achieved by using an OpenSSL library that achieved FIPS 140-2 validation (Certificate #1747). To enable this option in a MobileFirst client project, add the optional Android FIPS 140-2 plug-in.

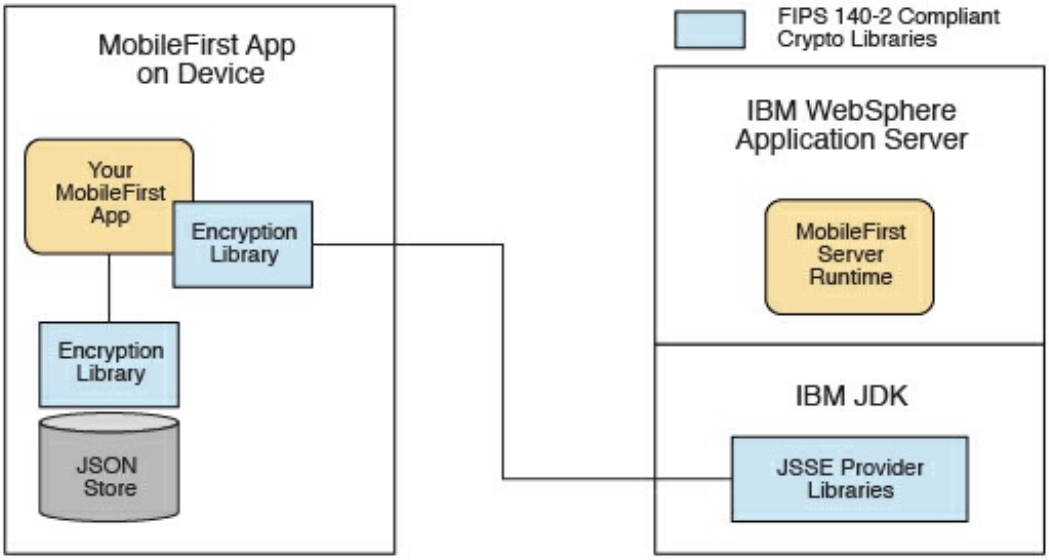
Note: There are some restrictions to be aware of:

- This FIPS 140-2 validated mode applies only to the protection (encryption) of local data that is stored by the JSONStore feature and protection of HTTPS communications between the MobileFirst client and the MobileFirst Server.
- This feature is only supported on the iOS and Android platforms.
    - On Android, this feature is only supported on devices or simulators that use the x86 or armeabi architectures. It is not supported on Android using armv5 or armv6 architectures. The reason is because the OpenSSL library used did not obtain FIPS 140-2 validation for armv5 or armv6 on Android. FIPS 140-2 is not supported on 64-bit architecture even though the MobileFirst library does support 64-bit architecture. FIPS 140-2 can be run on 64-bit devices if the project includes only 32-bit native NDK libraries.
    - On iOS, it is supported on i386, x86_64, armv7, armv7s, and arm64 architectures.
- This feature works with hybrid applications only (not with native applications).
- For native iOS, FIPS is enabled through the iOS FIPS libraries and is enabled by default. No action is required to enable FIPS 140-2.
- For HTTPS communications:
    - For Android devices, only the communications between the MobileFirst client and the MobileFirst Server use the FIPS 140-2 libraries on the client. Direct connections to other servers or services do not use the FIPS 140-2 libraries.
    - The MobileFirst client can only communicate with a MobileFirst Server that runs in supported environments, which are listed in the System Requirements (http://www-01.ibm.com/support/docview.wss?uid=swg27024838). If the MobileFirst Server runs in a non-supported environment, the HTTPS connection might fail with a key size too small error. This

error does not occur with HTTP communications.

- IBM MobileFirst Platform Application Center client does not support the FIPS 140-2 feature.

If you previously made the changes that are described in the tutorial, you must first save any other environment-specific changes that you made, and then delete and re-create your Android or iOS environments.



> For more information about JSONStore, see JSONStore overview (../../application-development/jsonstore).

References

For information about how to enable FIPS 140-2 mode in WebSphere Application Server, see Federal Information Processing Standard support (http://ibm.biz/knowctr#SSAW57_8.5.5/com.ibm.websphere.nd.multiplatform.doc/ae/rovr_fips.html).

For the WebSphere Application Server Liberty profile, no option is available in the administrative console to enable FIPS 140-2 mode. But you can enable FIPS 140-2 by configuring the Java™ runtime environment to use the FIPS 140-2 validated modules. For more information, see Java Secure Socket Extension (JSSE) IBMJSSE2 Provider Reference Guide.

Enabling FIPS 140-2

On iOS devices, the FIPS 140-2 support is enabled by default for both data at rest and data in motion. For Android devices, add the `cordova-plugin-mfp-fips` Corodva plugin.

Once added, the feature applies both to HTTPS and JSONStore data encryption.

Notes:

- FIPS 140-2 is only supported on Android and iOS. The iOS architectures that support FIPS 140-2 are i386, armv7, armv7s, x86_64, and arm64. The Android architectures that support FIPS 140-2 are x86 and armeambi.
- On Android, FIPS 140-2 is not supported on 64-bit architecture even though the MobileFirst library does support 64-bit architecture. When you use FIPS 140-2 on a 64-bit device, you might see the following error:

```
java.lang.UnsatisfiedLinkError: dlopen failed: "..." is 32-bit instead of 64-bit
```

This error means that you have 64-bit native libraries in your Android project, and FIPS 140-2 does not currently work when you use these libraries. To confirm, go to src/main/libs or src/main/jniLibs under your Android project, and check whether you have the x86_64 or arm64-v8a folders. If you do, delete these folders, and FIPS 140-2 can work again.

Configure FIPS 140-2 mode for HTTPS and JSONStore encryption

For iOS apps, FIPS 140-2 is enabled through the iOS FIPS libraries. It is enabled by default, so no action is required to enable or configure it.

The following code snippet is populated into a new IBM MobileFirst Foundation application in the initOptions object in the index.js for the Android operating system for configuring FIPS 140-2:

```
var wlInitOptions = {
  ...
  // # Enable FIPS 140-2 for data-in-motion (network) and data-at-rest (JSONStore) on Android.
  //   Requires the FIPS 140-2 optional feature to be enabled also.
  // enableFIPS : false
  ...
};
```

The default value of **enableFIPS** is `false` for the Android operating system. To enable FIPS 140-2 for both HTTPS and JSONStore data encryption, uncomment and set the option to `true`. After you set the value of **enableFIPS** to `true`, you should listen for the FIPS ready JavaScript event by creating a listening event similar to the following sample:

```
document.addEventListener('WL/FIPS/READY',
   this.onFipsReady, false);

onFipsReady: function() {
  // FIPS SDK is loaded and ready
}
```

After you set the value of the **enableFIPS** property, re-build the Android platform.

**Note:* You must install the FIPS Cordova plugin before you set the enableFIPS property value to true. Otherwise, a warning message is logged that states the initOption value is set, but the optional feature was not found. The FIPS 140-2 and JSONStore features are both optional on the Android operating system. FIPS 140-2 affects JSONStore data encryption only if the JSONStore optional feature is also enabled. If JSONStore is not enabled, then FIPS 140-2 does not affect JSONStore. In iOS, the FIPS 140-2 optional feature is not required for JSONStore FIPS 140-2 (data at rest) or HTTPS encryption (data in motion) because they are both handled by iOS. In Android, you must enable the FIPS 140-2 optional feature if you want to use JSONStore FIPS 140-2 or HTTPS encryption.

```
[WARN] FIPSHttp feature not found, but initOptions enables it on startup
```

Configuring FIPS 140-2 for existing applications

The FIPS 140-2 optional feature is not enabled by default on apps created for any versions of the Android operating system and on iOS apps in versions of IBM MobileFirst Foundation before version 8.0. To

enable the FIPS 140-2 optional feature for the Android operating system, see Enabling FIPS 140-2. After the optional feature is enabled, you can configure FIPS 140-2.

After you completed the steps that are described in Enabling FIPS 140-2, you must configure FIPS 140-2 by modifying the initOptions object in the index.js file to add the FIPS configuration property.

Note: The FIPS 140-2 feature, combined with the JSONStore feature, enables FIPS 140-2 support for JSONStore. This combination supersedes what was indicated in tutorial JSONStore - Encrypting sensitive data with FIPS 140-2 that was available for IBM® Worklight® V6.0 or earlier. If you previously modified an application by following the instructions in this tutorial, delete and re-create its iPhone, iPad, and Android environments. Because any environment-specific changes that you previously made are lost when you delete an environment, make sure to back up any such changes before you delete any environment. After the environment is re-created, you can reapply those changes to the new environment.

Add the following property to the initOptions object found in the index.js file.

```
enableFIPS : true
```

Re-build the Android platform.