Using Direct Update to quickly update your application

Overview

With Direct Update, Cordova applications can be updated "over-the-air" with refreshed web resources.

Benefits of Direct Update:

- Using Direct Update, organizations can ensure that users always use the latest version of the application.
- Application versions are better controlled. Users are notified of pending updates or prevented from using obsolete versions.
- Updates that are deployed to the MobileFirst Server are automatically pushed to user devices.

Restrictions:

- Direct Update updates the app web resources only.
- To update native resources a new app version must be uploaded to the respective app store.
- Android: no restrictions.
- Windows 8 and Windows 10: no restrictions.
- iOS:
    - B2C: according to the terms of service of your company; usually at least bug fixes are allowed.
    - B2E: through the iOS Developer Enterprise Program.

Jump to:

- Under the hood
- How Direct Update works
- Deploying updated web resources to MobileFirst Server
- User experience
- Direct Update in the field
- Disabling old application versions
- Direct Update authenticity
- Differential Direct Update

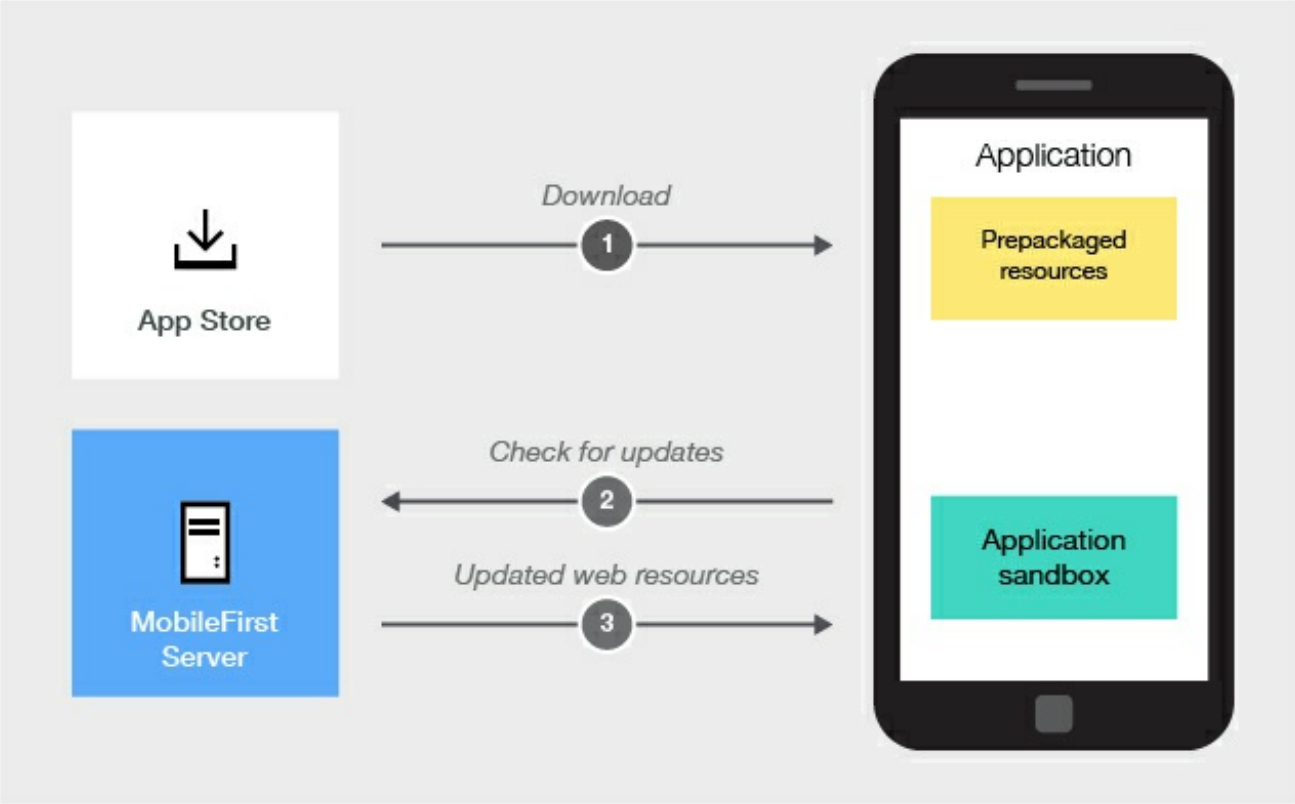
Under the Hood

TODO: update with information on direct update's security check.

How Direct Update works

The application web resources are initially packaged with the application to ensure first offline availability. Afterwards, the application checks for updates based on its configuration. The updated web resources are downloaded when necessary.

After a Direct Update, the application no longer uses the pre-packaged web resources. Instead it will use the web resources in the application's sandbox.

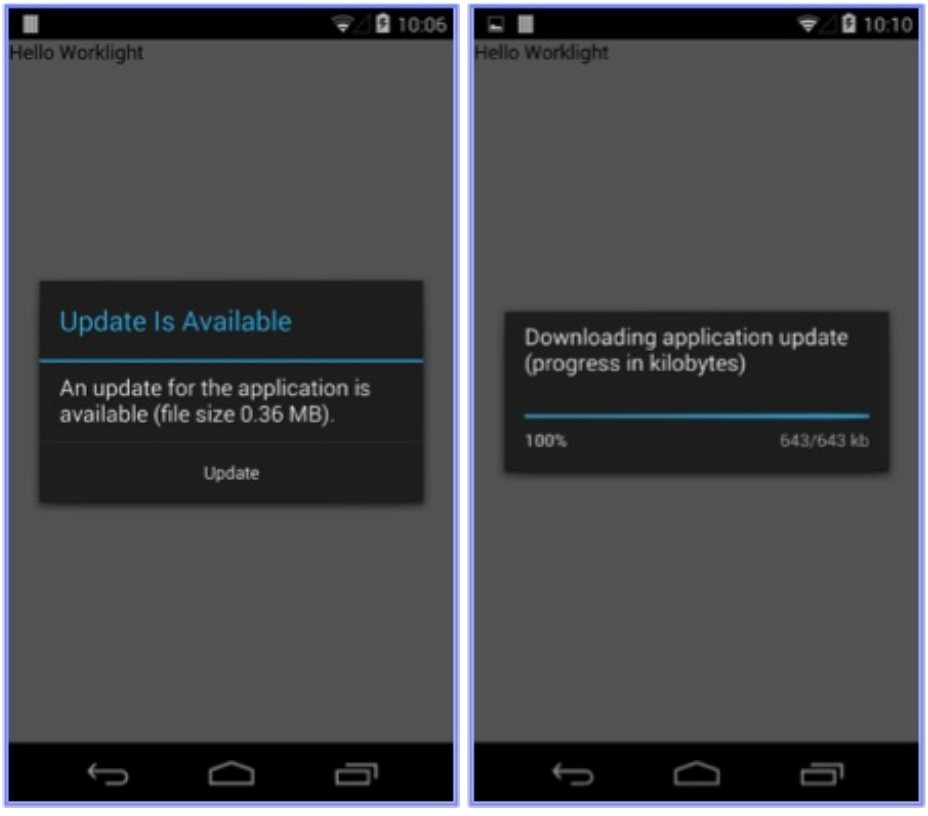


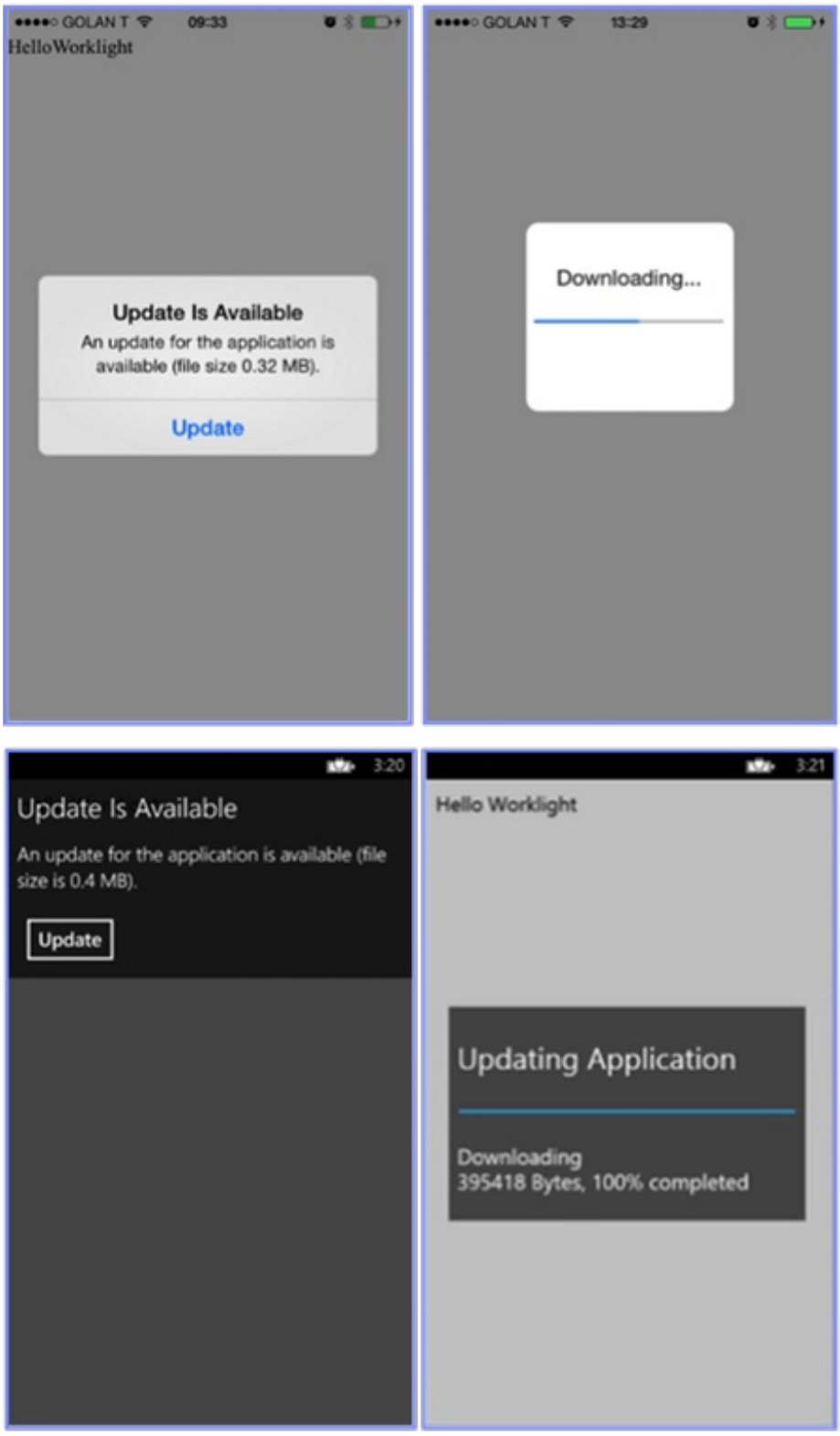
Deploying updated web resources to MobileFirst Server

TODO: how to create updated web resources and upload to the console

User Experience

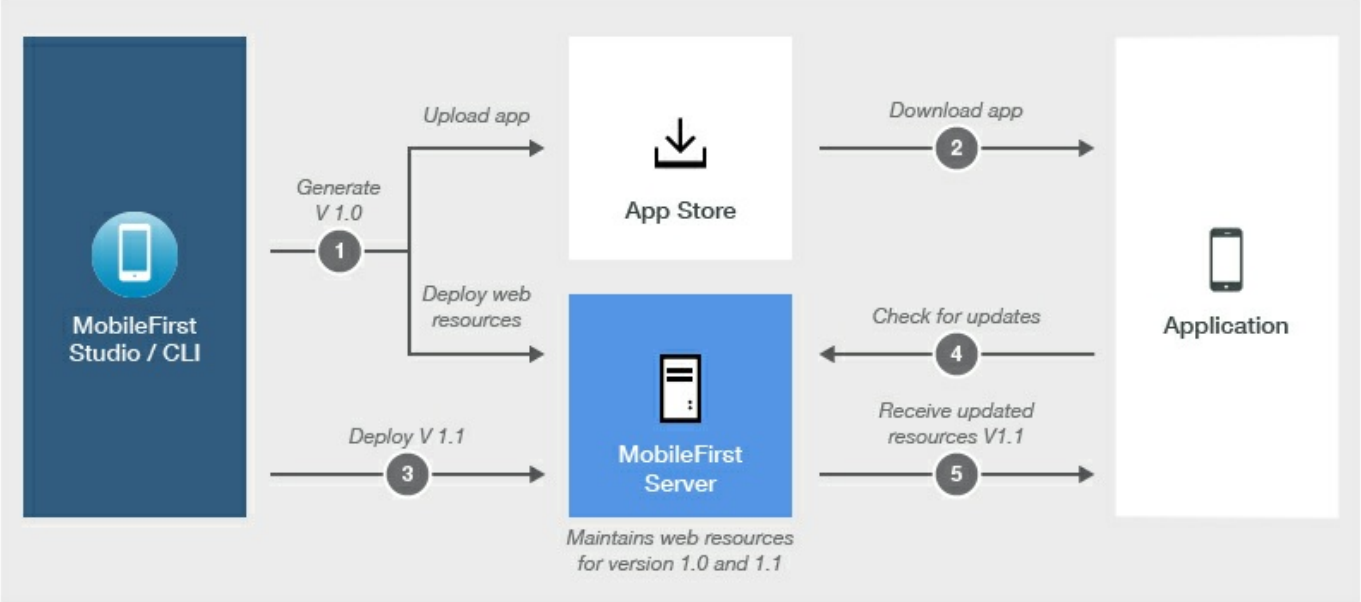
By default, after a Direct Update is received a dialog is displayed and the user is asked whether to begin the update process. After the user approves a progress bar dialog is displayed and the web resources are downloaded. The application is automatically reloaded after the update is complete.





Working with Direct Update in the field

The diagram below depicts the flow of updating an application's web resources using Direct Update once it has been submitted to the application stores and used by end-users.



Note: During development cycles, testers automatically get recent web resources through internal distribution mechanisms and not through application stores.

Disabling old application versions

From the MobileFirst Operations Console, it is possible to prevent users from using obsolete versions, and to notify users about available updates.

Clarification: The Remote Disable feature only prevents users from interacting with MobileFirst Server; that is, it prevents the app from connecting to the server. The application itself is still accessible. Any action in the application that requires server connectivity is blocked.

TODO: Show how to use remote disable in the console

Direct Update authenticity

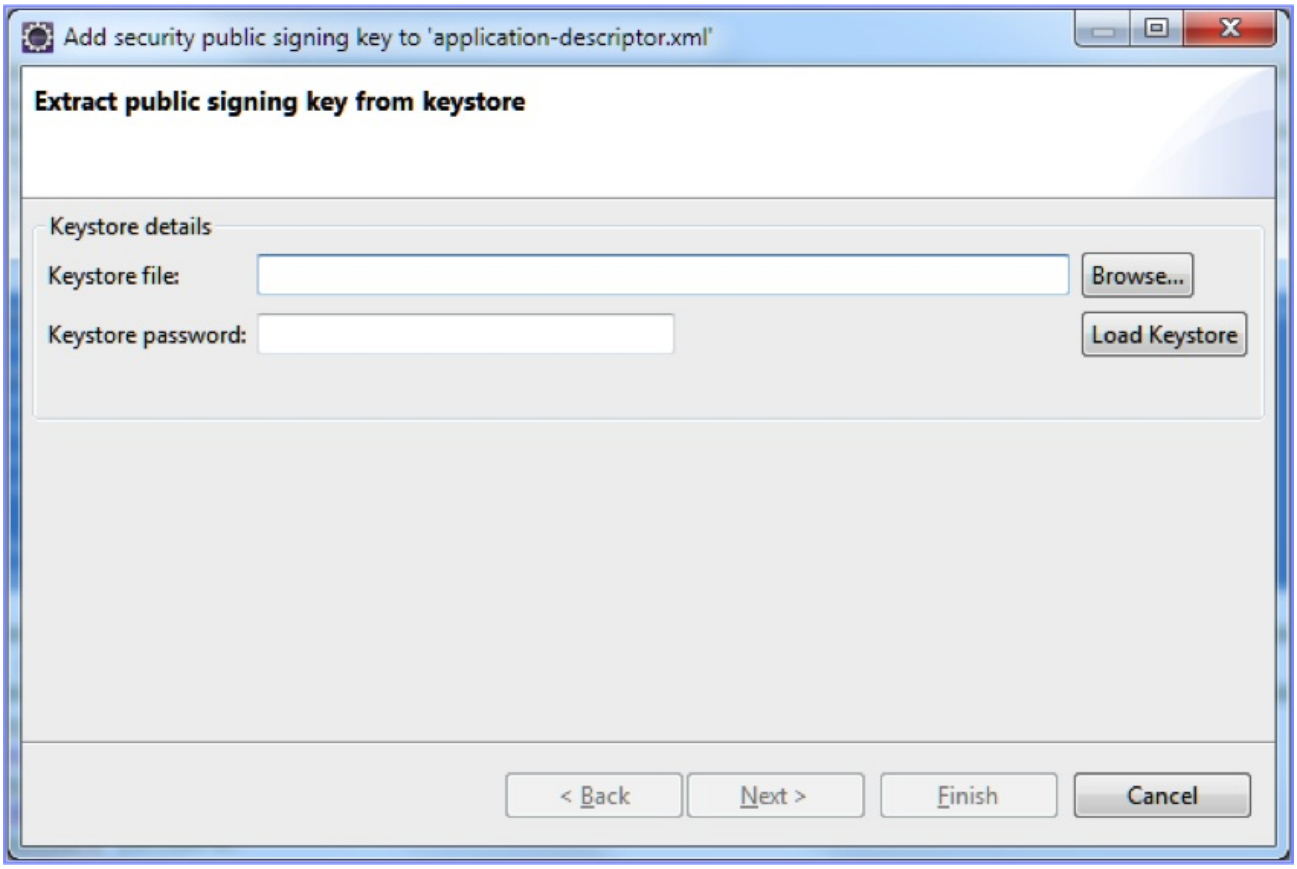
Enabling Direct Update authenticity prevents a 3rd-party attacker from altering the transmitted web resources from the server to the client application (that is, when it is cached in a content delivery network (CDN)).

To enable Direct Update authenticity:
TODO: write instructions how to enable it

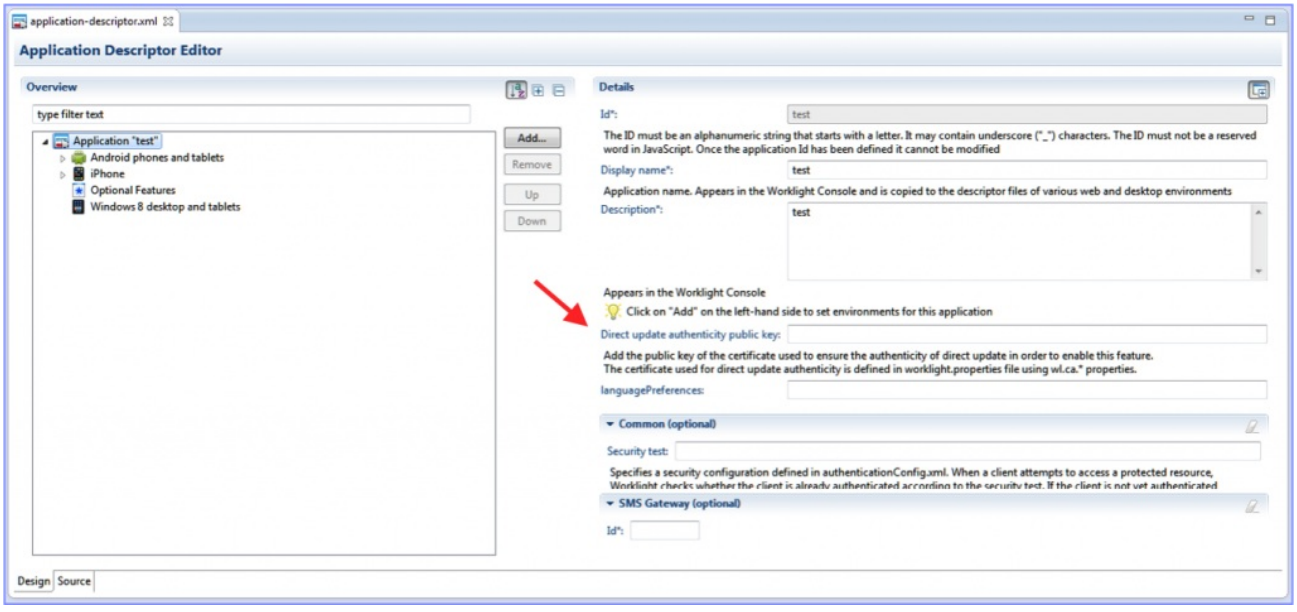
- Generate a certificate and place it in the MobileFirst project in the `server\conf` folder.
- Edit the MobileFirst Default Certificate section in `server\conf\worklight.properties` with the certificate keystore information, for example:

```
wl.ca.keystore.path=conf/myCert.jks
wl.ca.keystore.type=jks
wl.ca.keystore.password=myStrongPassword
wl.ca.key.alias=certAlias
wl.ca.key.alias.password=myCertPassword
```

- Add the certificate public key using the Application Descriptor Design view. To do so:
    - Right-click the application folder and select **Extract Public Signing Key**.
    - Follow the on-screen instructions.



The public key can then be found in the Application Descriptor Design view:



The public key can also be found in the Application Descriptor Editor view:

```
<application>
    …
    …
    …
    <directUpdateAuthenticityPublicKey>
        public keystore value
    </directUpdateAuthenticityPublicKey>
</application>
```

Notes:

- It is highly suggested to enable Secure Direct Update.
- Secure Direct Update does not work on already-deployed applications.
- Secure Direct Update works on applications published with the above configuration.

Differential Direct Update

Differential Direct Updates enables an application to download only the files that were changed since the last update instead of the entire web resources of the application. This reduces download time, conserves bandwidth, and improves overall user experience.

Important: A differential update is possible only if the client application's web resources are one version behind the application that is currently deployed on the server. Client applications that are more than one version behind the currently deployed application (meaning the application was deployed to the server at least twice since the client application was updated), receive a full update - meaning that the entire web resources are downloaded and updated.

There is no change in the behaviour of applications that were built with previous versions of IBM MobileFirst Platform Foundation.