

Deploying a Signed Android Application to the Enterprise using Oracle BI Mobile Security Toolkit

As of August 2018, Oracle Business Intelligence Mobile (Oracle BI Mobile) for Android supports AppConfig, a community focused on providing tools and best practices for native capabilities in mobile operating systems. AppConfig enables a more consistent, open, and simple way to configure and secure mobile apps to increase mobile adoption in business.

For details on AppConfig, see Oracle BI Mobile Security Toolkit Downloads.

- [Audience](#)
- [About the Security Toolkit for Oracle Business Intelligence Mobile](#)
- [How Are Updates to Oracle BI Mobile and the Oracle BI Mobile Security Toolkit Delivered?](#)
- [Overview of Creating an Application](#)
- [Re-Sign the Application](#)
- [Modify the Application](#)

Audience

The intended audience for these instructions is the developer or MDM (Mobile Device Management) expert who is familiar with Google's signing and deployment process and who is also familiar with the details of deploying an application with a selected MDM vendor.

About the Security Toolkit for Oracle Business Intelligence Mobile

If your enterprise is working with a Mobile Device Management (MDM) vendor or a Mobile Application Management (MAM) vendor, then use this document to prepare the Oracle BI Mobile application for enterprise deployment. This document shows you how to create a wrapped mobile app from Oracle BI Mobile.

The Oracle Business Intelligence Mobile Security Toolkit (Oracle BI Mobile Security Toolkit) provides the ability to generate a signed version of the Oracle BI Mobile for Android application. The toolkit includes the APK file and details for re-signing and repackaging the APK for “wrapping” with an appropriate MDM vendor.

How Are Updates to Oracle BI Mobile and the Oracle BI Mobile Security Toolkit Delivered?

You update your Oracle BI Mobile application through the Google Play Store or through the Oracle BI Mobile Security Toolkit.

The Oracle BI Mobile Security Toolkit is updated on a regular basis in order to synchronize with the Oracle BI Mobile application available on the Google Play Store. Oracle BI Mobile Security Toolkit updates are delivered in alignment with the releases of the Oracle BI Mobile application. As these updates are provided on an on-going basis, users must periodically update their Oracle BI Mobile applications—either through the Google Play Store or through the Oracle BI Mobile Security Toolkit.

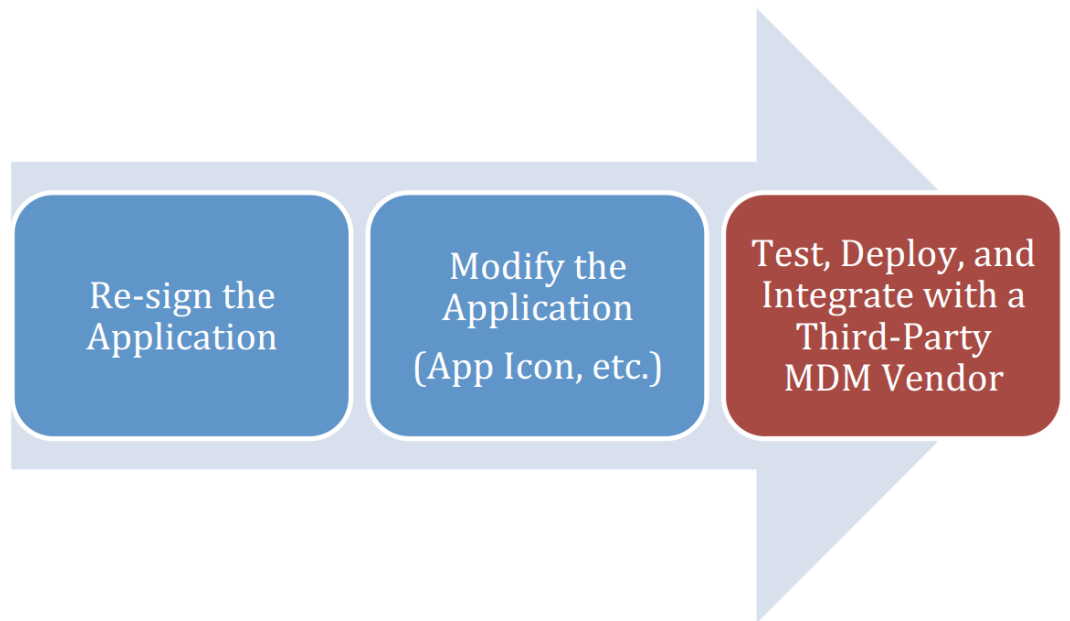
Note:

Whether you update your application through the Play Store or through the Oracle BI Mobile Security Toolkit, the ability to provide incremental updates is not supported. For updates accessed through Google Play Store, your installed application is replaced with the latest version available. For updates through the Oracle BI Mobile Security Toolkit, a completely new package of support files and libraries is provided.

Overview of Creating an Application

This topic describes the high-level process of creating an application for deployment in your organization's enterprise application store.

The first two steps in this process are documented in detail; the final step requires you to work with your IT department, the team in charge of your enterprise distribution, and your MDM vendor. This final step will vary from organization to organization.



Re-Sign the Application

You must re-sign the application with a proper certificate for your organization. If you do not re-sign the application, you run the risk of your toolkit-installed Oracle BI Mobile application being updated with a version from the Google Play Store.

When signing any Android application, first make sure you have a working knowledge of the Android signing process.

There are many techniques for re-signing an APK file. You should follow the technique recommended by your MDM vendor or a technique that is familiar to you.

Note:

Oracle does not provide any specific tools for re-signing.

Modify the Application

You can modify the application for things like application name or launch icon.

Use an APK tool provided by your Mobile Device Management (MDM) vendor or one that is familiar to you.

When making modifications to resources, you should be familiar with the requirements for that specific resource. For example, if you plan to change the launch icon, then you must be familiar with Android guidelines for icons.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Oracle® Fusion Middleware Deploying a Signed Android Application to the Enterprise using Oracle® Business Intelligence Mobile Security Toolkit, 12c Release 1
E92653-02

Copyright © 2015, 2018, Oracle and/or its affiliates. All rights reserved

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.