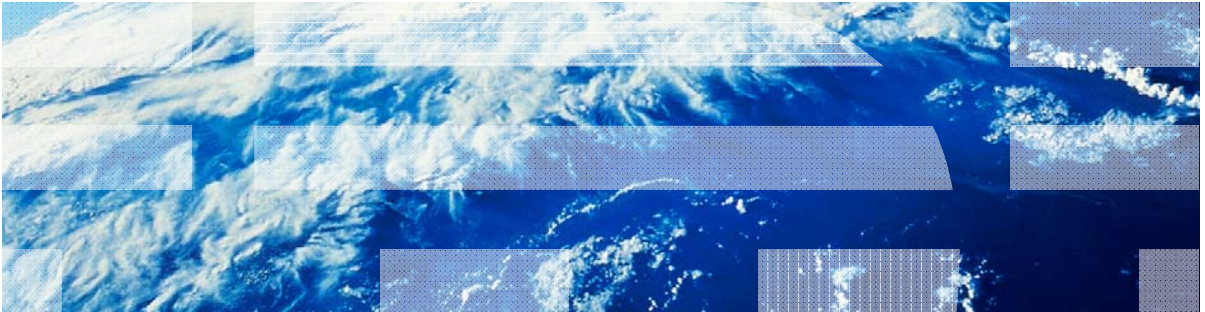


IBM Worklight V5.0.6 Getting Started

WebSphere LTPA based authentication



Trademarks

- IBM, the IBM logo, ibm.com, and WebSphere are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Worklight is a trademark or registered trademark of Worklight, an IBM Company. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “[Copyright and trademark information](#)” at www.ibm.com/legal/copytrade.shtml.
- Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.
- Other company products or service names may be trademarks or service marks of others.
- This document may not be reproduced in whole or in part without the prior written permission of IBM.

About IBM

- See <http://www.ibm.com/ibm/us/en/>

Using this module

- This module is intended for use with either the IBM® Worklight® Consumer Edition or the IBM Worklight Enterprise Edition.
 - The functionality that this module demonstrates is not available in the free IBM Worklight Developer Edition.
 - To use this module, Worklight Server must be installed on WebSphere® Application Server Full Profile, or on WebSphere Application Server Liberty Profile.

Agenda

- WebSphere LTPA-based authentication introduction
- Understanding server-side authentication options
- Configuring Worklight server for LTPA authentication
 - Configurations for WebSphere Application Server
 - Additional steps required for Option 1
 - Optional steps for protecting Worklight Console
- Creating client-side authentication components
- Examining the result
- Exercise

WebSphere LTPA-based authentication introduction

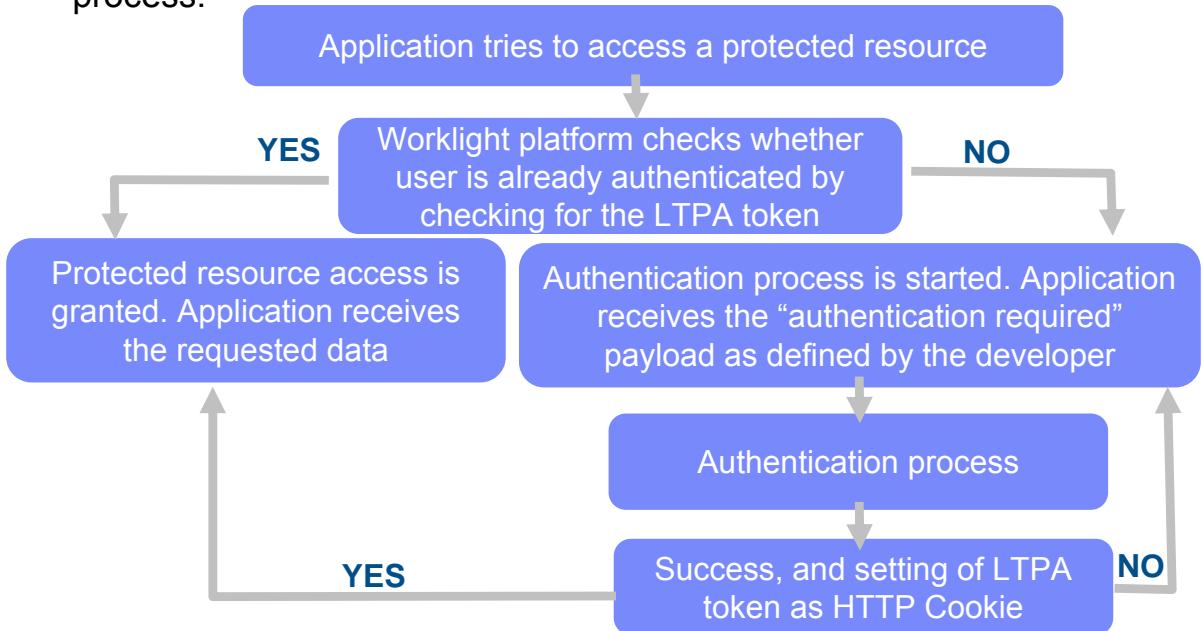
- WebSphere Application Server uses a secure token in a Lightweight Third-Party Authentication (LTPA) cookie to verify authenticated users, and to use this mechanism to trust users across a secure WebSphere Application server domain.
- When you run IBM Worklight on WebSphere Application server, you can use the **WebSphereFormBasedAuthenticator** and the **WebSphereLoginModule** to authenticate to the Worklight app by using an LTPA token.
- There are two options in support of WebSphere LTPA-based authentication for Worklight apps, referred to as **Option 1** and **Option 2**.

Agenda

- WebSphere LTPA-based authentication introduction
- **Understanding server-side authentication options**
- Configuring Worklight server for LTPA authentication
 - Configurations for WebSphere Application Server
 - Additional steps required for Option 1
 - Optional steps for protecting Worklight Console
- Creating client-side authentication components
- Examining the result
- Exercise

Understanding server-side authentication options

- This diagram illustrates the WebSphere LTPA-based authentication process.



Understanding server-side authentication options

Option 1

- If the enterprise policy requires WAR files to be protected on secured WebSphere Application Servers, then Option 1 can be used to handle this situation.
- Secure the web resources in the Worklight project WAR file by specifying the resource and the user role.
 - The authenticator and loginmodule that are defined as part of this configuration will authenticate the user (based on the provided credential) by using the underlying WebSphere Application Server Security API. Hence if the user provides user name and password on initial login, then this data is used to authenticate the user against the underlying registry that the WebSphere Application Server is configured against. Otherwise, if a valid LTPA token is provided on subsequent access, then this LTPA credential is used.

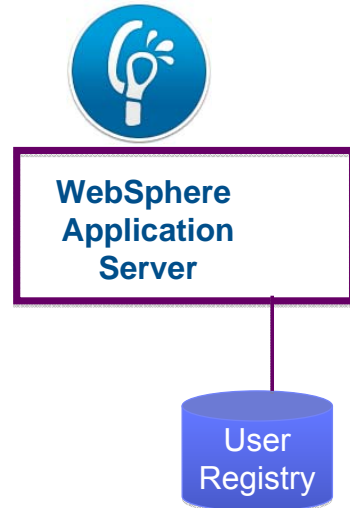
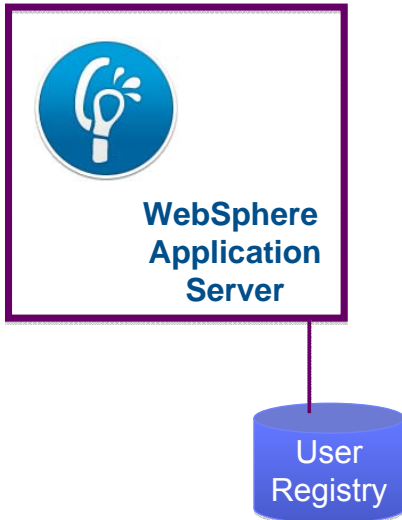
Understanding server-side authentication options

Option 2

- Option 2 is for the IBM Worklight security configuration to handle user authentication at the Worklight platform level, by using the security configuration of the underlying WebSphere Application Server.
 - The Worklight project that is deployed as a WAR file on the WebSphere Application Server is not secured. Hence the web.xml file of this WAR file does not reference any security constraints that protect the web resources.
 - The authenticator and loginmodule that are defined as part of this configuration will authenticate the user (based on the provided credential) by using the underlying WebSphere Application Server Security API. Hence if the user provides user name and password on initial login, then this data is used to authenticate the user against the underlying registry that WebSphere Application Server is configured against. Otherwise, if a valid LTPA token is provided on subsequent access, then this LTPA credential is used.

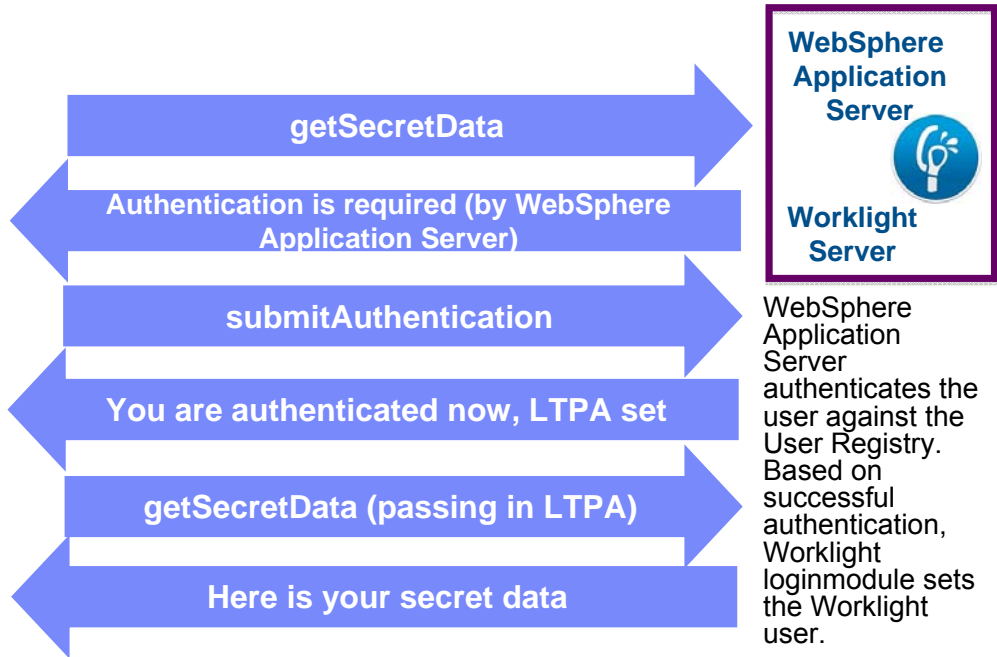
Understanding server-side authentication options

- Option 1: Authentication is enforced by WebSphere Application Server
- Option 2: Worklight Server enforces the authentication by relying on WebSphere Application Server configuration



Understanding server-side authentication options

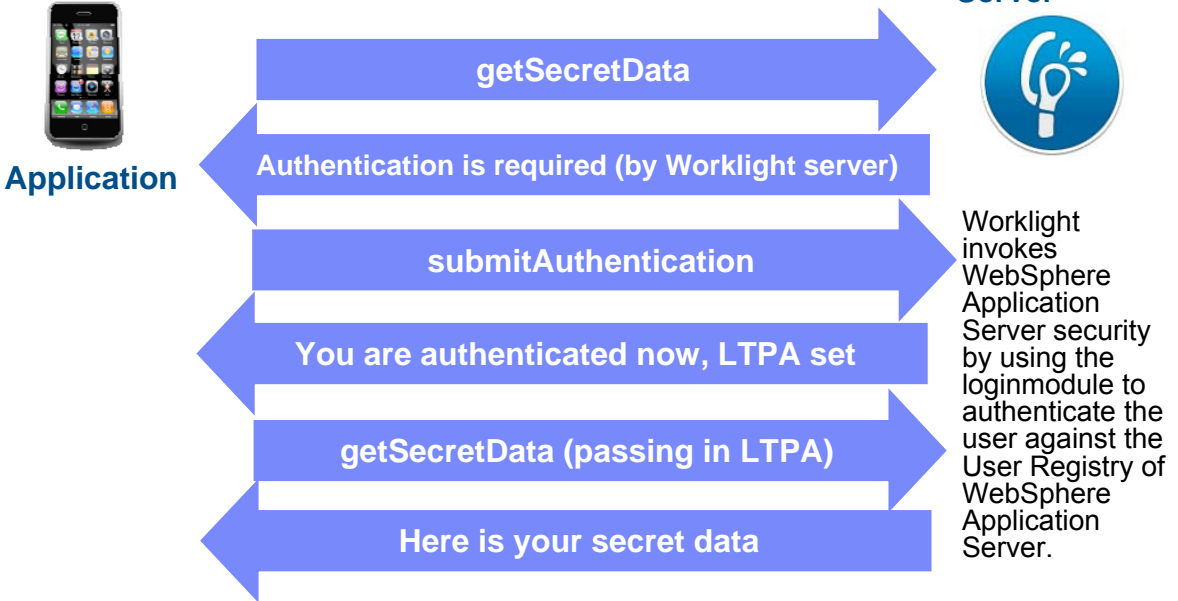
- Option 1



WebSphere Application Server authenticates the user against the User Registry. Based on successful authentication, Worklight loginmodule sets the Worklight user.

Understanding server-side authentication options

- Option 2



Understanding server-side authentication options

- Option 1 and Option 2 both present benefits and have different usages:

	Option 1	Option 2
Benefits	<p>This option uses the traditional WebSphere Application Server authentication and trust model.</p> <p>The container enforces all security, hence can reuse existing investments in securing the Java Enterprise Edition (Java EE) container by using third-party SSO products.</p>	<p>This option uses the traditional WebSphere Application Server authentication and trust model without the impact of modifying the IBM Worklight project WAR file.</p> <p>The container enforces all security, hence can reuse existing investments in securing the Java™ Enterprise Edition (Java EE) container by using third-party SSO product.</p> <p>The layered authentication of device, application, application instance, and user works as intended.</p> <p>Flexibility in configuring specific security settings that are IBM Worklight runtime specific without being hindered by the underlying container security.</p>
Usage	<p>This option is suitable for scenarios where the devices can be trusted and access for rogue applications is restricted.</p>	<p>This option is suitable for scenarios where the devices or the apps on the devices cannot be trusted.</p> <p>The multi-step authenticity checking that is built into IBM Worklight platform ensures denial of services to jail-broken devices, rogue applications, and unauthorized users.</p>

- Based on the above benefits, if your business needs do not require the use of Option 1, then Option 2 is recommended

Agenda

- WebSphere LTPA-based authentication introduction
- Understanding server-side authentication options
- **Configuring Worklight server for LTPA authentication**
 - **Configurations for WebSphere Application Server**
 - Additional steps required for Option 1
 - Optional steps for protecting Worklight Console
- Creating client-side authentication components
- Examining the result
- Exercise

Configurations for WebSphere Application Server

Step 1: Enable WebSphere Application Server security

- To compare the two options, you must first define the following settings on WebSphere Application Server:

For option 1:

- Enable administrative security
- Enable application security

For option 2:

- Enable administrative security

The screenshot displays the WebSphere Administration Console interface. On the left is a navigation tree with categories like 'Global security', 'Administrative security', and 'Application security'. The main content area shows the 'Global security' configuration page. Under the 'Administrative security' heading, the checkbox for 'Enable administrative security' is checked and highlighted with an orange box. Below it are links for 'Administrative user roles', 'Administrative group roles', and 'Administrative authentication'. Under the 'Application security' heading, the checkbox for 'Enable application security' is checked and highlighted with an orange box. The 'Java 2 security' section has the checkbox for 'Use java 2 security to restrict application access to local resources' unchecked. The 'User account repository' section is partially visible at the bottom.

Configurations for WebSphere Application Server

Step 2: Configuring authenticationConfig.xml realm and authenticator

- Uncomment the realm under the “For websphere” comment in the authenticationConfig.xml found in {WAS_HOME}/profiles/{your profile}/installedApps/{your node}/{worklight EAR}/{worklight WAR}/WEB-INF/classes/conf, so as to obtain the following text:

```
<!-- For websphere -->
<realm name="WASLTPARealm" loginModule="WASLTPAModule">
  <className>com.worklight.core.auth.ext.WebSphereFormBasedAuthenticator</className>
  <parameter name="login-page" value="/login.html"/>
  <parameter name="error-page" value="/loginError.html"/>
</realm>
```

- Optionally, you can include the parameters cookie-domain, cookie-name, and httponly-cookie. For more information, see the section about the LTPA authenticator in the product documentation
- Uncomment the loginModule under the “For websphere” comment:

```
<!-- For websphere -->
<loginModule name="WASLTPAModule">
  <className>com.worklight.core.auth.ext.WebSphereLoginModule</className>
</loginModule>
```

- Note: The above lines may already be uncommented

Configurations for WebSphere Application Server

Step 3: Configuring authenticationConfig.xml security tests

- Add security tests to authenticationConfig.xml for desired environments:
 - Add webSecurityTest if you plan to develop for web environments
 - Add mobileSecurityTest if you plan to develop for mobile environments

```
<securityTests>
  <webSecurityTest name="wasWebSecurity">
    <testUser realm="WASLTPARealm"/>
  </webSecurityTest>
  <mobileSecurityTest name="wasMobileSecurity">
    <testAppAuthenticity/>
    <testDeviceId provisioningType="none" />
    <testUser realm="WASLTPARealm" />
  </mobileSecurityTest>
</securityTests>
```

Agenda

- WebSphere LTPA-based authentication introduction
- Understanding server-side authentication options
- **Configuring Worklight server for LTPA authentication**
 - Configurations for WebSphere Application Server
 - **Additional steps required for Option 1**
 - Optional steps for protecting Worklight Console
- Creating client-side authentication components
- Examining the result
- Exercise

Additional steps required for Option 1

Step 1: Creating login.html

- Create a new file named login.html and save it to the root of your WAR file: {WAS_HOME}/profiles/{your profile}/installedApps/{your node}/{worklight EAR}/{worklight WAR}
- Set its content as follows:

```
<html>
  <head></head>
  <body>
    <form action="j_security_check" method="post">
      Username: <input type="text" name="j_username" size="20"><br>
      Password: <input type="password" name="j_password" size="20"><br>
      <input type="submit" value="Login">
    </form>
  </body>
</html>
```

Additional steps required for Option 1

Step 2: Creating loginError.html

- Create the loginError.html error page and place it in the root of your WAR file: {WAS_HOME}/profiles/{your profile}/installedApps/{your node}/{worklight EAR}/{worklight WAR}. This page is used when login fails.
- Set its content as follows:

```
<html>
<head></head>
<body>
    Login invalid.
</body>
</html>
```

Additional steps required for Option 1

Step 3: Configuring web.xml

- Locate the web.xml file:
 {WAS_HOME}/profiles/{your profile}/installedApps/{your node}/{worklight EAR}/{worklight WAR}/WEB-INF/web.xml
- Add the following tag inside the root tag (copy and paste the text on the right, if preferred)
- This will let WebSphere Application Server know what configuration the WAR expects

```

    • <security-constraint id="SecurityConstraint_1">
    •   <web-resource-collection id="WebResourceCollection_1">
    •     <web-resource-name>Snoop Servlet</web-resource-name>
    •     <description>Protection area for Snoop Servlet.</description>
    •     <url-pattern>/*</url-pattern>
    •     <http-method>GET</http-method>
    •     <http-method>POST</http-method>
    •   </web-resource-collection>
    •   <auth-constraint id="AuthConstraint_1">
    •     <description>Snoop Servlet Security::All Authenticated users
    •       for Snoop Servlet.</description>
    •     <role-name>Role 3</role-name>
    •   </auth-constraint>
    •   <user-data-constraint id="UserDataConstraint_1">
    •     <transport-guarantee>NONE</transport-guarantee>
    •   </user-data-constraint>
    • </security-constraint>
    • <security-role id="SecurityRole_1">
    •   <description>All Authenticated Users Role.</description>
    •   <role-name>Role 3</role-name>
    • </security-role>
    • <login-config>
    •   <auth-method>FORM</auth-method>
    •   <form-login-config>
    •     <form-login-page>/login.html</form-login-page>
    •     <form-error-page>/loginError.html</form-error-page>
    •   </form-login-config>
    • </login-config>
  
```

Agenda

- WebSphere LTPA-based authentication introduction
- Understanding server-side authentication options
- **Configuring Worklight server for LTPA authentication**
 - Configurations for WebSphere Application Server
 - Additional steps required for Option 1
 - **Optional steps for protecting Worklight Console**
- Creating client-side authentication components
- Examining the result
- Exercise

Optional: Protecting the Worklight Console

- To protect the Worklight Console with WebSphere Application Server authentication credentials, modify authenticationConfig.xml as follows:
- Uncomment the <staticResources> element to enable protection of static resources:

```
<!-- Uncomment the next element to protect the worklight console and the first section in securityTests below. -->  
<staticResources>  
  <resource id="worklightConsole" securityTest="WorklightConsole">  
    <urlPatterns>/console*/</urlPatterns>  
  </resource>  
</staticResources>
```

- Add a <customSecurityTest> element to your existing security tests:

```
<securityTests>  
  <customSecurityTest name="WorklightConsole">  
    <test realm="WASLTPARealm" isInternalUserID="true"/>  
  </customSecurityTest>  
</securityTests>
```

Agenda

- WebSphere LTPA-based authentication introduction
- Understanding server-side authentication options
- Configuring Worklight server for LTPA authentication
 - Configurations for WebSphere Application Server
 - Additional steps required for Option 1
 - Optional steps for protecting Worklight Console
- **Creating client-side authentication components**
- Examining the result
- Exercise

Creating client-side authentication components

- Use an existing Worklight application that is from one of the Authentication modules.
- To implement security for an app, follow the same methods as for any other type of realm, and then configure the challenge handler to use your realm:

```
var sampleAppRealmChallengeHandler = WL.Client.createChallengeHandler("WASLTPARealm");
```

- In the `applicationDescriptor.xml` file, specify the security test that your app must use for the appropriate environments.

– For example:

```
<common securityTest="WAS-securityTest" />
<android version="1.0" securityTest="WAS-securityTest" >
  <pushSender key="keyTest" senderId="senderIdTest" />
</android>
```

- Deploy and test the application by using Option 2. The authentication requires a valid user name and password from the underlying user registry that the WebSphere Application Server is configured against. When the authentication is successful, the Worklight app is authenticated.

Agenda

- WebSphere LTPA-based authentication introduction
- Understanding server-side authentication options
- Configuring Worklight server for LTPA authentication
 - Configurations for WebSphere Application Server
 - Additional steps required for Option 1
 - Optional steps for protecting Worklight Console
- Creating client-side authentication components
- Examining the result
- Exercise

Examining the result

The diagram illustrates the state of a web application during form-based authentication. It consists of three overlapping gray rectangular panels:

- Left Panel:** A login form with labels "Username:" and "Password:" above two input fields, and a "Login" button below them.
- Middle Panel:** A panel titled "Form based authentication" with a blue header. Below the header, it says "You're currently in the AppBody" and contains two buttons: "Call protected adapter proc" and "Logout".
- Bottom-Right Panel:** A box containing a JSON response from a callback function:

```
getSecretData_Callback response :: {"status":  
200,"invocationContext":null,"invocationResult":  
{"responseID":"2","isSuccessful":true,"secretData":"123  
456"}}
```

Agenda

- WebSphere LTPA-based authentication introduction
- Understanding server-side authentication options
- Configuring Worklight server for LTPA authentication
 - Configurations for WebSphere Application Server
 - Additional steps required for Option 1
 - Optional steps for protecting Worklight Console
- Creating client-side authentication components
- Examining the result
- Exercise

Exercise

- Examine the Authentication sample that is used for Option 2
- Implement Option 1 by securing the Worklight project WAR as shown in the Option 1 steps:
 - Update the web.xml file of the WAR file
 - Repackage the WAR file and redeploy it to the WebSphere Application Server
- The user experience should be identical

Notices

- Permission for the use of these publications is granted subject to these terms and conditions.
- This information was developed for products and services offered in the U.S.A.
- IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.
- IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
 - IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.
- For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:
 - Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan
- **The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.**
- This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.
- Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.
- IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.
- Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:
 - IBM Corporation
Dept F6, Bldg 1
294 Route 100
Somers NY 10589-3216
USA

- Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.
- The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.
- Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

COPYRIGHT LICENSE:

- This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.
- Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:
 - © (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

Privacy Policy Considerations

- IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.
- Depending upon the configurations deployed, this Software Offering may use session cookies that collect session information (generated by the application server). These cookies contain no personally identifiable information and are required for session management. Additionally, persistent cookies may be randomly generated to recognize and manage anonymous users. These cookies also contain no personally identifiable information and are required.
- If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent. For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at <http://www.ibm.com/privacy>; and IBM's Online Privacy Statement at <http://www.ibm.com/privacy/details/en/usa> sections entitled "Cookies, Web Beacons and Other Technologies" and "Software Products and Software-as-a-Service".

Support and comments

- For the entire IBM Worklight documentation set, training material and online forums where you can post questions, see the IBM website at:
 - <http://www.ibm.com/mobile-docs>
- **Support**
 - Software Subscription and Support (also referred to as Software Maintenance) is included with licenses purchased through Passport Advantage and Passport Advantage Express. For additional information about the International Passport Advantage Agreement and the IBM International Passport Advantage Express Agreement, visit the Passport Advantage website at:
 - <http://www.ibm.com/software/passportadvantage>
 - If you have a Software Subscription and Support in effect, IBM provides you assistance for your routine, short duration installation and usage (how-to) questions, and code-related questions. For additional details, consult your IBM Software Support Handbook at:
 - <http://www.ibm.com/support/handbook>
- **Comments**
 - We appreciate your comments about this publication. Please comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this document. The comments you send should pertain to only the information in this manual or product and the way in which the information is presented.
 - For technical questions and information about products and prices, please contact your IBM branch office, your IBM business partner, or your authorized remarketer.
 - When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you. IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you state.
 - Thank you for your support.
 - Submit your comments in the IBM Worklight forums at:
 - <https://www.ibm.com/developerworks/mobile/mobileforum.html>
 - If you would like a response from IBM, please provide the following information:
 - Name
 - Address
 - Company or Organization
 - Phone No.
 - Email address

Thank You

