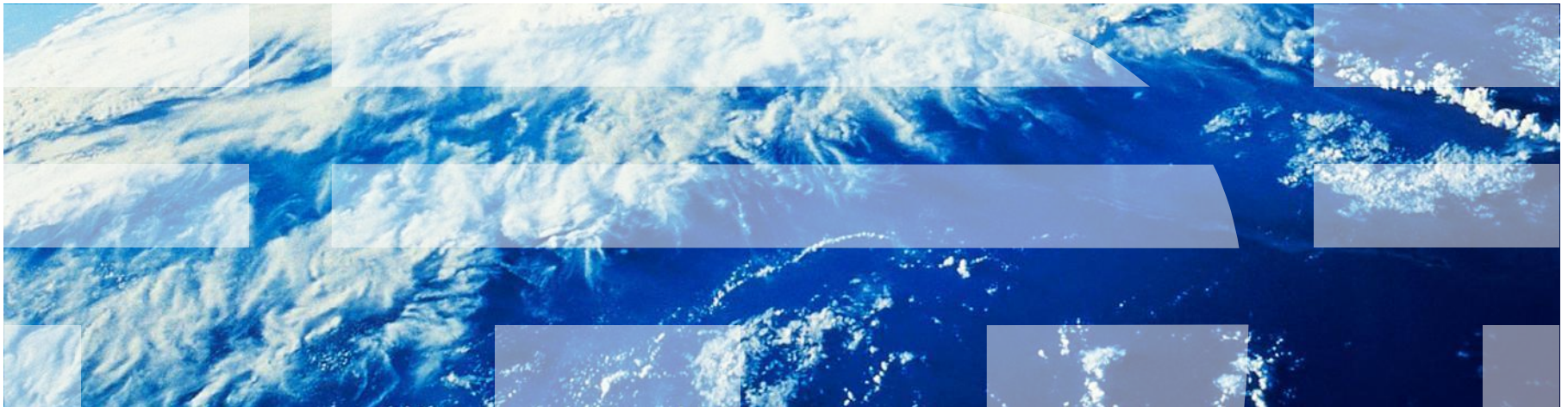


IBM Worklight Foundation V6.2.0 Getting Started

Custom authenticator and login module in iOS native applications



Trademarks

- IBM, the IBM logo, ibm.com, and Worklight are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. 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/>

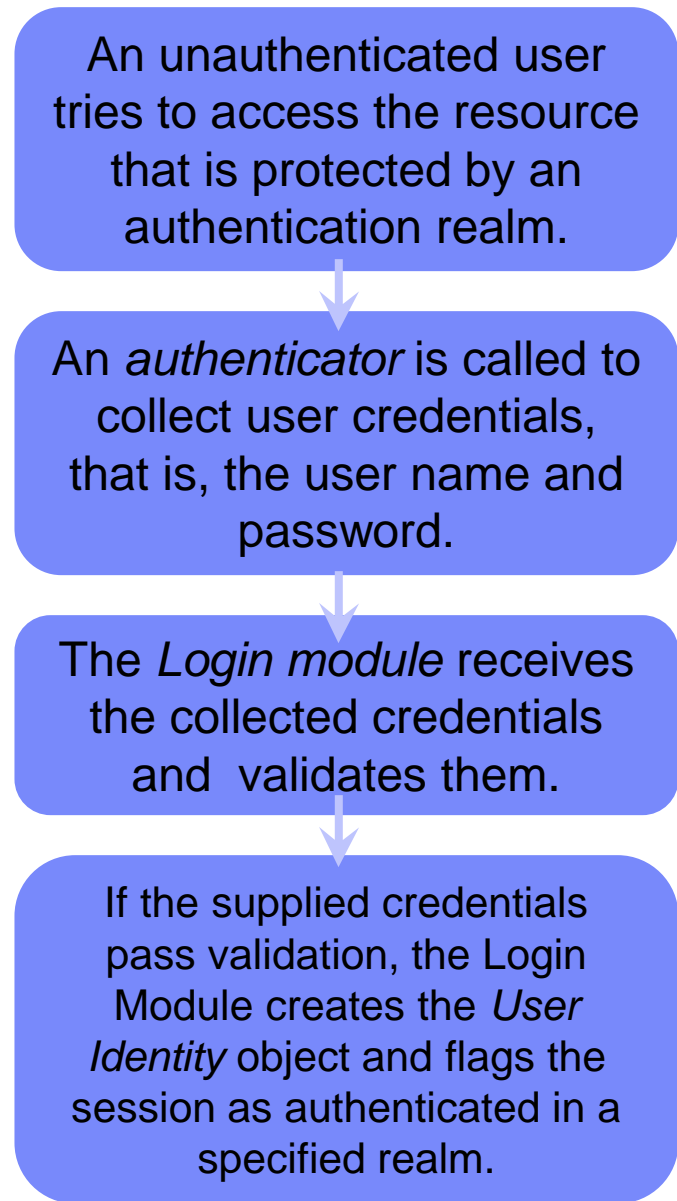
Agenda

- **Introduction to authentication**
- Configuring the authenticationConfig.xml file
- Creating a custom Java authenticator
- Creating a custom Java login module
- Creating client-side authentication components
- Examining the result

Introduction to authentication (1 of 3)



- The authentication process can be interactive:
 - For example, user name and password
- Or non-interactive:
 - For example, header-based authentication
- This process can involve a single step:
 - For example, a simple user name/password form)
- Or multiple steps:
 - For example, it might have to add a challenge after it issued the first password.
- The definition of the authentication realm includes the class name of an authenticator and a reference to a login module.
- An authenticator is an entity that collects user information.
 - For example, a login form
- A login module is a server entity that validates the retrieved user credentials and builds the user identity.
- You configure authentication settings such as realms, authenticators, and login modules, in the authenticationConfig.xml file that comes with Worklight Server.



Introduction to authentication (2 of 3)

- The authenticator, login module, and user identity instances are stored in a session scope. Therefore they exist while the session is alive.
- You can write custom login modules and authenticators when the default ones do not match your requirements.
- In previous modules:
 - You implemented a form-based authentication and used a non-validating login module.
 - You implemented an adapter-based authentication without having to add login modules, and validated credentials manually.
- In some cases, when credentials cannot be validated at adapter level and validation requires more complex code, you can implement an extra login module.
 - For example, when validation of credentials must be customized for a specific enterprise; or when more information must be retrieved from each client request, such as cookie, header, and user-agent.

Introduction to authentication (3 of 3)

- This module explains how to create a custom authenticator and a login module:
 - You learn how to implement a custom authenticator that collects the user name and password by using a request to a predefined URL.
 - You learn how to implement a custom login module that checks credentials that are received from the authenticator.
 - You learn how to define a realm that uses your custom authenticator and login module.
 - You learn how to use this realm to protect resources.
- For more information about authentication concepts, see IBM® Worklight ® Foundation user documentation.

Agenda

- Introduction to authentication
- **Configuring the authenticationConfig.xml file**
- Creating a custom Java authenticator
- Creating a custom Java login module
- Creating client-side authentication components
- Examining the result

Configuring authenticationConfig.xml (1 of 2)

- Add authentication information to the **authenticationConfig.xml** file.
- In the `<realms>` section, define a realm called **CustomAuthenticatorRealm**.
 - Make sure that it uses **CustomLoginModule**.
- Specify **MyCustomAuthenticator** as the class name. You implement it in subsequent slides.

```
<realm name="CustomAuthenticatorRealm" loginModule="CustomLoginModule">  
  <className>com.mypackage.MyCustomAuthenticator</className>  
</realm>  
<realm name="SampleAppRealm" loginModule="StrongDummy">
```

- In the `<loginModules>` section, add a **loginModule** called **CustomLoginModule**.

```
<loginModule name="CustomLoginModule">  
  <className>com.mypackage.MyCustomLoginModule</className>  
</loginModule>
```

- Specify **MyCustomLoginModule** as the class name. You implement it in subsequent slides.

Configuring authenticationConfig.xml (2 of 2)

- In the `<securityTests>` section, add a security test.
- Later, you use this security test to protect the adapter procedure. Therefore, use a `<customSecurityTest>` element.

```
<securityTests>
  <customSecurityTest name="CustomAuthSecurityTest">
    <test isInternalUserID="true" realm="CustomAuthenticatorRealm"/>
  </customSecurityTest>
</securityTests>
```

- Remember the security test name, because you use it in the next slides.

Agenda

- Introduction to authentication
- Configuring the authenticationConfig.xml file
- **Creating a custom Java authenticator**
- Creating a custom Java login module
- Creating client-side authentication components
- Examining the result

Creating a custom Java™ authenticator (1 of 21)

- The authenticator API includes the following methods:
 - `void init(Map<String, String> options)`
 - `AuthenticationResult processRequest(HttpServletRequest request, HttpServletResponse response, boolean isAccessToProtectedResource)`
 - `AuthenticationResult processAuthenticationFailure(HttpServletRequest request, HttpServletResponse response, String errorMessage)`
 - `AuthenticationResult processRequestAlreadyAuthenticated(HttpServletRequest request, HttpServletResponse response)`
 - `Map<String, Object> getAuthenticators(HttpServletRequest request)`
 - `Boolean changeResponseOnS(HttpServletRequest request, HttpServletResponse response)`
 - `WorkLightAuthenticator clone(WorkLightAuthenticator authenticator)`

The `init` method of the authenticator is called when the authenticator instance is created. It takes the parameters that are specified in the definition of the realm in the `authenticationConfig.xml` file.

Creating a custom Java authenticator (2 of 21)

- The authenticator API includes the following methods:
 - void **init**(Map<String, String> options)
 - AuthenticationResult **processRequest**(HttpServletRequest request, HttpServletResponse response, boolean isAccessToProtectedResource)
 - AuthenticationResult **processAuthenticationFailure**(HttpServletRequest request, HttpServletResponse response, String errorMessage)
 - AuthenticationResult **processRequestAlreadyAuthenticated**(HttpServletRequest request, HttpServletResponse response)
 - Map<String, Object> **getAuthenticators**(HttpServletRequest request)
 - Boolean **changeResponseOnS**(HttpServletRequest request, HttpServletResponse response)
 - WorkLightAuthenticator **cl**

The processRequest method is called for each request from an unauthenticated session.

Creating a custom Java authenticator (3 of 21)

- The authenticator API includes the following methods:
 - void **init**(Map<String, String> options)
 - AuthenticationResult **processRequest**(HttpServletRequest request, HttpServletResponse response, boolean isAccessToProtectedResource)
 - AuthenticationResult **processAuthenticationFailure**(HttpServletRequest request, HttpServletResponse response, String errorMessage)
 - AuthenticationResult **processRequestAlreadyAuthenticated**(HttpServletRequest request, HttpServletResponse response)
 - Map<String, Object> **getAuthenticators**(HttpServletRequest request)
 - Boolean **changeResponseOnSuccess**(HttpServletRequest request, HttpServletResponse response)
 - WorkLightAuthenticator **clone**(WorkLightAuthenticator authenticator)

The `processAuthenticationFailure` method is called if the login module returns a failure of credentials validation.

Creating a custom Java authenticator (4 of 21)

- The authenticator API includes the following methods:
 - void **init**(Map<String, String> options)
 - AuthenticationResult **processRequest**(HttpServletRequest request, HttpServletResponse response, boolean isAccessToProtectedResource)
 - AuthenticationResult **processAuthenticationFailure**(HttpServletRequest request, HttpServletResponse response, String errorMessage)
 - AuthenticationResult **processRequestAlreadyAuthenticated**(HttpServletRequest request, HttpServletResponse response)
 - Map<String, Object> **getAuthenticationData**()
 - request, HttpServletResponse
 - WorkLightAuthenticator

The `processRequestAlreadyAuthenticated` method is called for each request from an already authenticated session.

Creating a custom Java authenticator (5 of 21)

- The authenticator API includes the following methods:

- void **init**(Map<String, String> configuration)
- AuthenticationResult **process**(HttpServletRequest request, HttpServletResponse response, boolean isAccessToProtectedResource)
- AuthenticationResult **processAuthenticationFailure**(HttpServletRequest request, HttpServletResponse response)
- AuthenticationResult **processRequestAlreadyAuthenticated**(HttpServletRequest request, HttpServletResponse response)
- Map<String, Object> **getAuthenticationData**()
- Boolean **changeResponseOnSuccess**(HttpServletRequest request, HttpServletResponse response)
- WorkLightAuthenticator **clone**()

The `getAuthenticationData` method is used by a login module to get the credentials that are collected by an authenticator.

Creating a custom Java authenticator (7 of 21)

- The authenticator API includes the following methods:

- void **init**(Map<String, String> configuration)
- AuthenticationResult **process**(HttpServletRequest request, HttpServletResponse response, boolean isAccessToProtectedResource)
- AuthenticationResult **processAuthenticationFailure**(HttpServletRequest request, HttpServletResponse response)
- AuthenticationResult **processRequestAlreadyAuthenticated**(HttpServletRequest request, HttpServletResponse response)
- Map<String, Object> **getAuthenticationData**()
- Boolean **changeResponseOnSuccess**(HttpServletRequest request, HttpServletResponse response)
- WorkLightAuthenticator **clone**()

The `changeResponseOnSuccess` method is called after authentication success. It is used to add data to the response after the authentication is successful.

Creating a custom Java authenticator (8 of 21)

- The authenticator API includes the following methods:
 - void **init**(Map<String, String> configuration)
 - AuthenticationResult **process**(HttpServletRequest request, HttpServletResponse response, boolean isAccessToProtectedResource)
 - AuthenticationResult **processAuthenticationFailure**(HttpServletRequest request, HttpServletResponse response)
 - AuthenticationResult **processRequestAlreadyAuthenticated**(HttpServletRequest request, HttpServletResponse response)
 - Map<String, Object> **getAuthenticationData**()
 - Boolean **changeResponseOnSuccess**(HttpServletRequest request, HttpServletResponse response)
 - WorkLightAuthenticator **clone**()

The `clone` method is used to create a deep copy of class members.

Creating a custom Java authenticator (9 of 21)

- Create a **MyCustomAuthenticator** class in the **server\java** folder.
- Make sure that this class implements the **WorkLightAuthenticator** interface.

```
public class MyCustomAuthenticator implements WorkLightAuthenticator {
```

- Add the **authenticationData** map to your authenticator to hold the credentials information.
 - This object is retrieved and used by a login module.

```
private Map<String, Object> authenticationData = null;
```

Creating a custom Java authenticator (10 of 21)

- You must add a dependency on server runtime libraries to use server-related classes, for example, **HttpServletRequest**.
- Right-click your Worklight project and select **Properties**.
- Select **Java Build Path** → **Libraries** and click **Add Library**.
- Select **Server Runtime** and click **Next**.
- You see a list of server runtimes that are installed in your Eclipse.
- Select one and click **Finish**.
- Click **OK**.

Creating a custom Java authenticator (11 of 21)

- The `init` method is called when the authenticator is created.
- As its parameter, this method takes the map of options that is specified in a realm definition in the **authenticationConfig.xml** file.

```
@Override
public void init(Map<String, String> options) throws MissingConfigurationException {
    logger.info("init");
}
```

- The `clone` method of the authenticator creates a deep copy of the object members.

```
@Override
public WorkLightAuthenticator clone() throws CloneNotSupportedException {
    MyCustomAuthenticator otherAuthenticator = (MyCustomAuthenticator) super.clone();
    otherAuthenticator.authenticationData = new HashMap<String, Object>(authenticationData);
    return otherAuthenticator;
}
```

Creating a custom Java authenticator (12 of 21)

- The `processRequest` method is called for each unauthenticated request to collect credentials.

```
@Override
public AuthenticationResult processRequest(HttpServletRequest request, HttpServletResponse response, boolean isAccessToProtectedResource) {
    Logger.info("myCustomAuthenticator :: processRequest");
    if (request.getRequestURI().contains("my_custom_auth_request_url")){
        String username = request.getParameter("username");
        String password = request.getParameter("password");

        if (null != username && null != password) {
            authenticationData = new HashMap<String, String>();
            authenticationData.put("username", username);
            authenticationData.put("password", password);
            return AuthenticationResult.createFrom(authenticationData);
        } else {
            response.setContentType("application/json");
            response.setHeader("Cache-Control", "no-cache");
            response.getWriter().print("{\"authStatus\": \"failure\"}");
            return AuthenticationResult.createFrom(authenticationData);
        }
    }

    if (!isAccessToProtectedResource)
        return AuthenticationResult.createFrom(authenticationData);

    response.setContentType("application/json");
    response.setHeader("Cache-Control", "no-cache");
    response.getWriter().print("{\"authStatus\": \"failure\"}");
    return AuthenticationResult.createFrom(authenticationData);
}
```

The `processRequest()` method takes the request, response, and `isAccessToProtectedResource` arguments. The method might retrieve data from a request and write data to a response, and must return a specific `AuthenticationResult` status as described in subsequent slides. **Reminder:** the authenticator collects the credentials for a login module; it **does not** validate them.

Creating a custom Java authenticator (13 of 21)

- The `processRequest` method is called for each unauthenticated request to collect credentials.

```
@Override
public AuthenticationResult processRequest(HttpServletRequest request, HttpServletResponse response, boolean isAccessToProtectedResource) {
    logger.info("MyCustomAuthenticator :: processRequest");
    if (request.getRequestURI().contains("my_custom_auth_request_url")){
        String username = request.getParameter("username");
        String password = request.getParameter("password");

        if (null != username && null != password && username.length() > 0 && password.length() > 0){
            authenticationData = new HashMap<String, Object>();
            authenticationData.put("username", username);
            authenticationData.put("password", password);
            return AuthenticationResult.createFrom(AuthenticationStatus.SUCCESS, authenticationData);
        } else {
            response.setContentType("application/json; charset=UTF-8");
            response.setHeader("Cache-Control", "no-cache, must-revalidate");
            response.getWriter().print("{\"authStatus\":\"required\"}");
            return AuthenticationResult.createFrom(AuthenticationStatus.REQUIRED);
        }
    }

    if (!isAccessToProtectedResource)
        return AuthenticationResult.createFrom(AuthenticationStatus.SUCCESS);

    response.setContentType("application/json; charset=UTF-8");
    response.setHeader("Cache-Control", "no-cache, must-revalidate");
    response.getWriter().print("{\"authStatus\":\"required\"}");
    return AuthenticationResult.createFrom(AuthenticationStatus.REQUIRED);
}
```

The application sends an authentication request to a specific URL. This request URL contains a **my_custom_auth_request_url** component, which is used by the authenticator to make sure that this request is an authentication request. It is recommended to have a different URL component in every authenticator.

Creating a custom Java authenticator (14 of 21)

- The `processRequest` method is called for each unauthenticated request to collect credentials.

```
@Override
public AuthenticationResult processRequest(HttpServletRequest request, HttpServletResponse response, boolean isAccessToProtectedResource) {
    Logger.info("MyCustomAuthenticator :: processRequest");
    if (request.getRequestURL().contains("my_custom_auth_request_url")){
        String username = request.getParameter("username");
        String password = request.getParameter("password");

        if (null != username && null != password && username.length() > 0 && password.length() > 0){
            authenticationData = new HashMap<String, Object>();
            authenticationData.put("username", username);
            authenticationData.put("password", password);
            return AuthenticationResult.createFrom(AuthenticationStatus.SUCCESS);
        } else {
            response.setContentType("application/json; charset=UTF-8");
            response.setHeader("Cache-Control", "no-cache, must-revalidate");
            response.getWriter().print("{\"authStatus\":\"required\", \"password\":\"\"}");
            return AuthenticationResult.createFrom(AuthenticationStatus.REQUIRED);
        }
    }

    if (!isAccessToProtectedResource)
        return AuthenticationResult.createFrom(AuthenticationStatus.CLIENT_ERROR);

    response.setContentType("application/json; charset=UTF-8");
    response.setHeader("Cache-Control", "no-cache, must-revalidate");
    response.getWriter().print("{\"authStatus\":\"required\"}");
    return AuthenticationResult.createFrom(AuthenticationStatus.CLIENT_ERROR);
}
```

The authenticator retrieves the user name and password that are passed as request parameters.

Creating a custom Java authenticator (15 of 21)

- The `processRequest` method is called for each unauthenticated request to collect credentials.

```

@Override
public AuthenticationResult processRequest(HttpServletRequest request, HttpServletResponse response, boolean isAccessToProtectedResource) {
    Logger.info("MyCustomAuthenticator :: processRequest");
    if (request.getRequestURI().contains("my_custom_auth_request_url")){
        String username = request.getParameter("username");
        String password = request.getParameter("password");

        if (null != username && null != password && username.length() > 0 && password.length() > 0){
            authenticationData = new HashMap<String, Object>();
            authenticationData.put("username", username);
            authenticationData.put("password", password);
            return AuthenticationResult.createFrom(AuthenticationStatus.SUCCESS);
        } else {
            response.setContentType("application/json; charset=UTF-8");
            response.setHeader("Cache-Control", "no-cache, must-revalidate");
            response.getWriter().print("{\"authStatus\":\"required\"}");
            return AuthenticationResult.createFrom(AuthenticationStatus.REQUIRED);
        }
    }

    if (!isAccessToProtectedResource)
        return AuthenticationResult.createFrom(AuthenticationStatus.SUCCESS);

    response.setContentType("application/json; charset=UTF-8");
    response.setHeader("Cache-Control", "no-cache, must-revalidate");
    response.getWriter().print("{\"authStatus\":\"required\"}");
    return AuthenticationResult.createFrom(AuthenticationStatus.REQUIRED);
}

```

The authenticator checks the credentials for basic validity, creates an `authenticationData` object, and returns `SUCCESS`. `SUCCESS` means only that the credentials were successfully collected; after that, the login module is called to validate the credentials.

Creating a custom Java authenticator (16 of 21)

- The `processRequest` method is called for each unauthenticated request to collect credentials.

```
@Override
public AuthenticationResult processRequest(HttpServletRequest request) {
    logger.info("MyCustomAuthenticator :: processRequest");
    if (request.getRequestURI().contains("my_custom_auth_")) {
        String username = request.getParameter("username");
        String password = request.getParameter("password");

        if (null != username && null != password && username.length() > 0 && password.length() > 0) {
            authenticationData = new HashMap<String, Object>();
            authenticationData.put("username", username);
            authenticationData.put("password", password);
            return AuthenticationResult.createFrom(AuthenticationStatus.SUCCESS);
        } else {
            response.setContentType("application/json; charset=UTF-8");
            response.setHeader("Cache-Control", "no-cache, must-revalidate");
            response.getWriter().print("{\"authStatus\":\"required\", \"errorMessage\":\"Please enter username and password\"}");
            return AuthenticationResult.createFrom(AuthenticationStatus.CLIENT_INTERACTION_REQUIRED);
        }
    }

    if (!isAccessToProtectedResource) {
        return AuthenticationResult.createFrom(AuthenticationStatus.REQUEST_NOT_RECOGNIZED);
    }

    response.setContentType("application/json; charset=UTF-8");
    response.setHeader("Cache-Control", "no-cache, must-revalidate");
    response.getWriter().print("{\"authStatus\":\"required\"}");
    return AuthenticationResult.createFrom(AuthenticationStatus.CLIENT_INTERACTION_REQUIRED);
}
```

If a problem occurs with the received credentials, the authenticator adds an error message to the response and returns `CLIENT_INTERACTION_REQUIRED`. The client must still supply authentication data.

Creating a custom Java authenticator (17 of 21)

- The `processRequest` method is called for each unauthenticated request to collect credentials.

```
@Override
public AuthenticationResult processRequest(HttpServletRequest request) {
    Logger.info("MyCustomAuthenticator :: processRequest");
    if (request.getRequestURI().contains("my_custom_auth_request")) {
        String username = request.getParameter("username");
        String password = request.getParameter("password");

        if (null != username && null != password && username.length() > 0) {
            authenticationData = new HashMap<String, Object>();
            authenticationData.put("username", username);
            authenticationData.put("password", password);
            return AuthenticationResult.createFrom(AuthenticationStatus.REQUEST_NOT_RECOGNIZED);
        } else {
            response.setContentType("application/json; charset=UTF-8");
            response.setHeader("Cache-Control", "no-cache, must-revalidate");
            response.getWriter().print("{\"authStatus\":\"required\"}");
            return AuthenticationResult.createFrom(AuthenticationStatus.CLIENT_INTERACTION_REQUIRED);
        }
    }
}
```

```
if (!isAccessToProtectedResource)
    return AuthenticationResult.createFrom(AuthenticationStatus.REQUEST_NOT_RECOGNIZED);
```

```
response.setContentType("application/json; charset=UTF-8");
response.setHeader("Cache-Control", "no-cache, must-revalidate");
response.getWriter().print("{\"authStatus\":\"required\"}");
return AuthenticationResult.createFrom(AuthenticationStatus.CLIENT_INTERACTION_REQUIRED);
}
```

The `isAccessToProtectedResource` argument specifies whether an access attempt was made to a protected resource. If not, the method returns `REQUEST_NOT_RECOGNIZED`, which means that the authenticator treatment is not required, and can proceed with the request as is.

Creating a custom Java authenticator (18 of 21)

- The `processRequest()` method is called for each unauthenticated request to collect credentials.

```

@Override
public AuthenticationResult processRequest(HttpServletRequest request, HttpServletResponse response, boolean isAccessToProtectedResource) {
    Logger.info("MyCustomAuthenticator :: processRequest");
    if (request.getRequestURI().contains("my_custom_auth_request_url")){
        String username = request.getParameter("username");
        String password = request.getParameter("password");

        if (null != username && null != password && username.length() > 0 && password.length() > 0) {
            authenticationData = new HashMap<String, Object>();
            authenticationData.put("username", username);
            authenticationData.put("password", password);
            return AuthenticationResult.createFrom(AuthenticationStatus.CLIENT_INTERACTION_REQUIRED);
        } else {
            response.setContentType("application/json; charset=UTF-8");
            response.setHeader("Cache-Control", "no-cache, must-revalidate");
            response.getWriter().print("{\"authStatus\":\"required\"}");
            return AuthenticationResult.createFrom(AuthenticationStatus.CLIENT_INTERACTION_REQUIRED);
        }
    }

    if (!isAccessToProtectedResource)
        return AuthenticationResult.createFrom(AuthenticationStatus.CLIENT_INTERACTION_REQUIRED);

    response.setContentType("application/json; charset=UTF-8");
    response.setHeader("Cache-Control", "no-cache, must-revalidate");
    response.getWriter().print("{\"authStatus\":\"required\"}");
    return AuthenticationResult.createFrom(AuthenticationStatus.CLIENT_INTERACTION_REQUIRED);
}

```

If the request made to a protected resource does not contain authentication data, the authenticator adds an `authStatus:required` property to the response, and also returns a `CLIENT_INTERACTION_REQUIRED` status.

Creating a custom Java authenticator (19 of 21)

- The authenticator `getAuthenticationData` method is used by a login module to get collected credentials.

```
@Override
public Map<String, Object> getAuthenticationData() {
    logger.info("getAuthenticationData");
    return authenticationData;
}
```

- After the authenticated session is established, all requests are transported through the `changeResponseOnSuccess` and `processRequestAlreadyAuthenticated` methods.
- You can use these methods to retrieve data from requests and to update responses.

Creating a custom Java authenticator (20 of 21)

- The `changeResponseOnSuccess` method is called after credentials are successfully validated by the login module.
- You can use this method to modify the response before you return it to the client.
- This method must return `true` if the response was modified, or `false` otherwise.
- Use it to notify a client application about the authentication success.

```
@Override
public boolean changeResponseOnSuccess(HttpServletRequest request, HttpServletResponse response) throws IOException {
    logger.info("MyCustomAuthenticator :: changeResponseOnSuccess");
    if (request.getRequestURI().contains("my_custom_auth_request_url")){
        response.setContentType("application/json; charset=UTF-8");
        response.setHeader("Cache-Control", "no-cache, must-revalidate");
        response.getWriter().print("{\"authStatus\":\"complete\"}");
        return true;
    }
    return false;
}
```

Creating a custom Java authenticator (21 of 21)

- The `processRequestAlreadyAuthenticated` method returns `AuthenticationResult` objects for authenticated requests.

```
@Override
public AuthenticationResult processRequestAlreadyAuthenticated(HttpServletRequest request,
    logger.info("processRequestAlreadyAuthenticated");
    return AuthenticationResult.REQUEST_NOT_RECOGNIZED;
}
```

- If the login module returns an authentication failure, the `processAuthenticationFailure` method is called. This method writes an error message to a response body, and returns the `CLIENT_INTERACTION_REQUIRED` status.

```
@Override
public AuthenticationResult processAuthenticationFailure(HttpServletRequest request, HttpServletResponse response,
    String errorMessage) throws IOException, ServletException {

    logger.info("processAuthenticationFailure");
    response.setContentType("application/json; charset=UTF-8");
    response.setHeader("Cache-Control", "no-cache, must-revalidate");
    response.getWriter().print("{\"authRequired\":true, \"errorMessage\":\"" + errorMessage + "\"}");
    return AuthenticationResult.CLIENT_INTERACTION_REQUIRED;
}
```

Agenda

- Introduction to authentication
- Configuring the authenticationConfig.xml files
- Creating a custom Java authenticator
- **Creating a custom Java login module**
- Creating client-side authentication components
- Examining the result

Creating a custom Java login module (1 of 20)

- The login module API includes the following methods:
 - `void init(Map<String, String> options)`
 - `boolean login(Map<String, Object> authenticationData)`
 - `UserIdentity createIdentity(String loginModule)`
 - `void logout()`
 - `void abort()`
 - `WorkLightAuthLoginModule`

The `init` method of the login module is called when the login module instance is created. This method receives the options that are specified in the login module definition of the **authenticationConfig.xml** file.

Creating a custom Java login module (2 of 20)

- The login module API is:
 - void **init**(Map<String, String> options)
 - boolean **login**(Map<String, Object> authenticationData)
 - UserIdentity **createIdentity**(String loginModule)
 - void **logout**()
 - void **abort**()
 - WorkLightAuthLoginModule

The `login` method of the login module is used to validate the credentials that are collected by the authenticator.

Creating a custom Java login module (3 of 20)

- The login module API is:
 - void **init**(Map<String, String> options)
 - boolean **login**(Map<String, Object> authenticationData)
 - `UserIdentity` **createIdentity**(String loginModule)
 - void **logout**()
 - void **abort**()
 - WorkLightAuthLoginModule

The `createIdentity` method of the login module is used to create a `userIdentity` object after validation of the credentials succeeds.

Creating a custom Java login module (4 of 20)

- The login module API is:
 - void **init**(Map<String, String> options)
 - boolean **login**(Map<String, Object> authenticationData)
 - UserIdentity **createIdentity**(String loginModule)
 - void **logout**()
 - void **abort**()
 - WorkLightAuthLoginModule

The `logout` and `abort` methods are used to clean up cached data after a logout or authentication aborts.

Creating a custom Java login module (5 of 20)

- The login module API is:
 - void **init**(Map<String, String> configuration)
 - boolean **login**(Map<String, String> authenticationData)
 - UserIdentity **createIdentity**(String name, String password)
 - void **logout**()
 - void **abort**()
 - WorkLightLoginModule **clone**()

The `clone` method is used to create a deep copy of the class members.

Creating a custom Java login module (6 of 20)

- Create a **MyCustomLoginModule** class in the **server\java** folder.
- Make sure that this class implements the **WorkLightAuthLoginModule** interface.

```
public class MyCustomLoginModule implements WorkLightAuthLoginModule {
```

- Add two private class members, **USERNAME** and **PASSWORD**, to hold the user credentials

```
private String USERNAME;  
private String PASSWORD;
```

Creating a custom Java login module (7 of 20)

- The `init` method is called when the login module instance is created. As its parameter, it takes the map of options that are specified in a login module definition in the **authenticationConfig.xml** file.

```
@Override
public void init(Map<String, String> options) throws MissingConfigurationException {
    logger.info("init");
}
```

- The `clone` method of the login module creates a deep copy of the object members.

```
@Override
public MyCustomLoginModule clone() throws CloneNotSupportedException {
    return (MyCustomLoginModule) super.clone();
}
```

Creating a custom Java login module (8 of 20)

- The `login` method is called after the authenticator returns the `SUCCESS` status.

```
@Override
public boolean login(Map<String, Object> authenticationData) {
    logger.info("MyCustomLoginModule :: login");
    USERNAME = (String) authenticationData.get("username");
    PASSWORD = (String) authenticationData.get("password");

    if (USERNAME.equals("wuser") && PASSWORD.equals("12345"))
        return true;
    else
        throw new RuntimeException("Invalid credentials");
}
```

When called, the `login` method gets an `authenticationData` object from the authenticator.

Creating a custom Java login module (9 of 20)

- The `login` method is called after the authenticator returns the `SUCCESS` status.

```
@Override
public boolean login(Map<String, Object> authenticationData) {
    logger.info("MyCustomLoginModule :: login");
    USERNAME = (String) authenticationData.get("username");
    PASSWORD = (String) authenticationData.get("password");

    if (USERNAME.equals("wuser") && PASSWORD.equals("12345"))
        return true;
    else
        throw new RuntimeException("Invalid credentials");
}
```

The `login` method retrieves the user name and password that the authenticator previously stored.

Creating a custom Java login module (10 of 20)

- The `login` method is called after the authenticator returns the `SUCCESS` status.

```
@Override
public boolean login(Map<String, Object> authenticationData) {
    Logger.info("MyCustomLoginModule :: login");
    USERNAME = (String) authenticationData.get("username");
    PASSWORD = (String) authenticationData.get("password");

    if (USERNAME.equals("wuser") && PASSWORD.equals("12345"))
        return true;
    else
        throw new RuntimeException("Invalid credentials");
}
```

In this example, the login module validates the credentials against hardcoded values. You can implement your own validation rules. The `login` method returns `true` if the credentials are valid.

Creating a custom Java login module (11 of 20)

- The `login` method is called after the authenticator returns the `SUCCESS` status.

```
@Override
public boolean login(Map<String, Object> authenticationData) {
    logger.info("MyCustomLoginModule :: login");
    USERNAME = (String) authenticationData.get("username");
    PASSWORD = (String) authenticationData.get("password");

    if (USERNAME.equals("wuser") && PASSWORD.equals("12345"))
        return true;
    else
        throw new RuntimeException("Invalid credentials");
}
```

If the validation fails, the `login` method can either return `false` or throw a `RuntimeException`. The exception string is returned to the authenticator as an `errorMessage` parameter.

Creating a custom Java login module (12 of 20)

- The `createIdentity` method is called when the `login` method returns `true`. It is used to create an authenticated user identity object.

```
@Override
public UserIdentity createIdentity(String loginModule) {
    logger.info("MyCustomLoginModule :: createIdentity");

    HashMap<String, Object> customAttributes = new HashMap<String, Object>();
    customAttributes.put("AuthenticationDate", new Date());

    UserIdentity identity = new UserIdentity(loginModule, USERNAME, null, null, customAttributes, PASSWORD);
    return identity;
}
```

After the `login` method returns `true`, the `createIdentity` method is called. It is used to create a `UserIdentity` object. You can store your own custom attributes in it to use later in Java or adapter code.

Creating a custom Java login module (13 of 20)

- The `createIdentity` method is called when the `login` method returns `true`. It is used to create an authenticated user identity object.

```
@Override
public UserIdentity createIdentity(String loginModule) {
    logger.info("MyCustomLoginModule :: createIdentity");

    HashMap<String, Object> customAttributes = new HashMap<String, Object>();
    customAttributes.put("AuthenticationDate", new Date());

    UserIdentity identity = new UserIdentity(loginModule, USERNAME, null, null, customAttributes, PASSWORD);
    return identity;
}
```

The `UserIdentity` object contains user information. Its constructor is:

```
public
UserIdentity(String loginModule,
              String name,
              String displayName,
              Set<String> roles,
              Map<String, Object> attributes,
              Object credentials)
```

Creating a custom Java login module (14 of 20)

- The `createIdentity` method is called when the `login` method returns `true`. It is used to create an authenticated user identity object.

```
@Override
public UserIdentity createIdentity(String loginModule) {
    Logger.info("MyCustomLoginModule :: createIdentity");

    HashMap<String, Object> customAttributes = new HashMap<String, Object>();
    customAttributes.put("AuthenticationDate", new Date());

    UserIdentity identity = new UserIdentity(loginModule, USERNAME, null, null, customAttributes, PASSWORD);
    return identity;
}
```

Login module
name to set user
for

The `UserIdentity` object contains user

information. Its constructor is:

```
public
UserIdentity(String loginModule,
              String name,
              String displayName,
              Set<String> roles,
              Map<String, Object> attributes,
              Object credentials)
```

Creating a custom Java login module (15 of 20)

- The `createIdentity` method is called when the `login` method returns `true`. It is used to create an authenticated user identity object.

```
@Override
public UserIdentity createIdentity(String loginModule) {
    Logger.info("MyCustomLoginModule :: createIdentity");

    HashMap<String, Object> customAttributes = new HashMap<String, Object>();
    customAttributes.put("AuthenticationDate", new Date());

    UserIdentity identity = new UserIdentity(loginModule, USERNAME, null, null, customAttributes, PASSWORD);
    return identity;
}
```

A unique user identifier

The `UserIdentity` object contains user information. Its constructor is:

```
public
UserIdentity(String loginModule,
             String name,
             String displayName,
             Set<String> roles,
             Map<String, Object> attributes,
             Object credentials)
```

Creating a custom Java login module (16 of 20)

- The `createIdentity` method is called when the `login` method returns `true`. It is used to create an authenticated user identity object.

```
@Override
public UserIdentity createIdentity(String loginModule) {
    logger.info("MyCustomLoginModule :: createIdentity");

    HashMap<String, Object> customAttributes = new HashMap<String, Object>();
    customAttributes.put("AuthenticationDate", new Date());

    UserIdentity identity = new UserIdentity(loginModule, USERNAME, null, null, customAttributes, PASSWORD);
    return identity;
}
```

User display name

The `UserIdentity` object contains user information. Its constructor is:

```
public
UserIdentity(String loginModule,
             String name,
             String displayName,
             Set<String> roles,
             Map<String, Object> attributes,
             Object credentials)
```

Creating a custom Java login module (17 of 20)

- The `createIdentity` method is called when the `login` method returns `true`. It is used to create an authenticated user identity object.

```
@Override
public UserIdentity createIdentity(String loginModule) {
    logger.info("MyCustomLoginModule :: createIdentity");

    HashMap<String, Object> customAttributes = new HashMap<String, Object>();
    customAttributes.put("AuthenticationDate", new Date());

    UserIdentity identity = new UserIdentity(loginModule, USERNAME, null, null, customAttributes, PASSWORD);
    return identity;
}
```

User Java security roles

The `UserIdentity` object contains user information. Its constructor is:

```
public
UserIdentity(String loginModule,
             String name,
             String displayName,
             Set<String> roles,
             Map<String, Object> attributes,
             Object credentials)
```


Creating a custom Java login module (18 of 20)

- The `createIdentity` method is called when the `login` method returns `true`. It is used to create an authenticated user identity object.

```
@Override
public UserIdentity createIdentity(String loginModule) {
    logger.info("MyCustomLoginModule :: createIdentity");

    HashMap<String, Object> customAttributes = new HashMap<String, Object>();
    customAttributes.put("AuthenticationDate", new Date());

    UserIdentity identity = new UserIdentity(loginModule, USERNAME, null, null, customAttributes, PASSWORD);
    return identity;
}
```

Custom user attributes

The `UserIdentity` object contains user information. Its constructor is:

```
public
UserIdentity(String loginModule,
             String name,
             String displayName,
             Set<String> roles,
             Map<String, Object> attributes,
             Object credentials)
```

Creating a custom Java login module (19 of 20)

- The `createIdentity` method is called when the `login` method returns `true`. It is used to create an authenticated user identity object.

```
@Override
public UserIdentity createIdentity(String loginModule) {
    logger.info("MyCustomLoginModule :: createIdentity");

    HashMap<String, Object> customAttributes = new HashMap<String, Object>();
    customAttributes.put("AuthenticationDate", new Date());

    UserIdentity identity = new UserIdentity(loginModule, USERNAME, null, null, customAttributes, PASSWORD);
    return identity;
}
```

Sensitive user credentials that are not to be persisted.

The `UserIdentity` object contains user information. Its constructor is:

```
public
UserIdentity(String loginModule,
              String name,
              String displayName,
              Set<String> roles,
              Map<String, Object> attributes,
              Object credentials)
```

Creating a custom Java login module (20 of 20)

- The `logout` and `abort` methods are used to clean up class members after the user logs out or aborts the authentication flow.

```
@Override
public void logout() {
    logger.info("MyCustomLoginModule :: logout");
    USERNAME = null;
    PASSWORD = null;
}

@Override
public void abort() {
    logger.info("MyCustomLoginModule :: abort");
    USERNAME = null;
    PASSWORD = null;
}
```

Agenda

- Introduction to authentication
- Configuring the authenticationConfig.xml file
- Creating a custom Java authenticator
- Creating a custom Java login module
- **Creating client-side authentication components**
- Examining the result

Creating the client-side authentication components (1 of 5)

1. Create a native Android application and add the Worklight native APIs as explained in the documentation.
2. Add an Activity, `LoginCustomLoginModule`, which will handle and present the login form
 - *Remember to add this Activity to the `AndroidManifest.xml` file, too.*

3. Create a `MyChallengeHandler` class as a subclass of `ChallengeHandler`.

`MyChallengeHandler` must implement 2 main methods:

1. `isCustomResponse`
2. `handleChallenge`

Moreover, in the sample, the `submitLogin` method is added to present and handle the data that is received from the form.

Creating the client-side authentication components (2 of 5)

- The `isCustomResponse` method

```
public boolean isCustomResponse(WLResponse response) {  
    if (response == null || response.getResponseJSON() == null) {  
        return false;  
    }  
    if(response.toString().indexOf("authStatus") > -1){  
        return true;  
    }  
    else{  
        return false;  
    }  
}
```

- This method checks every custom response from Worklight Server to verify whether that is the expected challenge.

Creating the client-side authentication components (3 of 5)

- The `handleChallenge` method

```
public void handleChallenge(WLResponse response){
    try {
        if(response.getResponseJSON().getString("authStatus") == "complete"){
            submitSuccess(response);
        }
        else {
            cachedResponse = response;
            Intent login = new Intent(parentActivity,
LoginCustomLoginModule.class);
            parentActivity.startActivityForResult(login, 1);
        }
    } catch (JSONException e) {
        e.printStackTrace();
    }
}
```

- This method is called after the `isCustomResponse` method returns `true`. Here, this method is used to present the login form.

Creating the client-side authentication components (4 of 5)

- The `submitLogin` method

```
public void submitLogin(int resultCode, String userName, String password, boolean back){
    if (resultCode != Activity.RESULT_OK || back) {
        submitFailure(cachedResponse);
    } else {
        HashMap<String, String> params = new HashMap<String, String>();
        params.put("username", userName);
        params.put("password", password);
        submitLoginForm("/my_custom_auth_request_url", params, null, 0, "post");
    }
}
```

- If the user asks to abort this action, the `submitFailure` method is called. Otherwise, the information that is collected from the login form is sent to the custom authenticator by a call to the `submitLoginForm` method.

Creating the client-side authentication components (5 of 5)

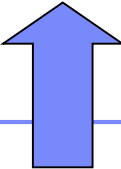
- In the Main Activity class connect to Worklight server, register your challengeHandler and invoke the protected adapter procedure.

```
final WLClient client = WLClient.createInstance(this);
client.connect(new MyConnectionListener());

challengeHandler = new AndroidChallengeHandler(this, realm);
client.registerChallengeHandler(challengeHandler);

invokeBtn = (Button) findViewById(R.id.invoke);
invokeBtn.setOnClickListener(new View.OnClickListener() {

    @Override
    public void onClick(View v) {
        WLProcedureInvocationData invocationData = new
        WLProcedureInvocationData("DummyAdapter", "getSecretData");
        WLRequestOptions options = new WLRequestOptions();
        options.setTimeout(30000);
        client.invokeProcedure(invocationData, new MyResponseListener(), options);
    }
});
```



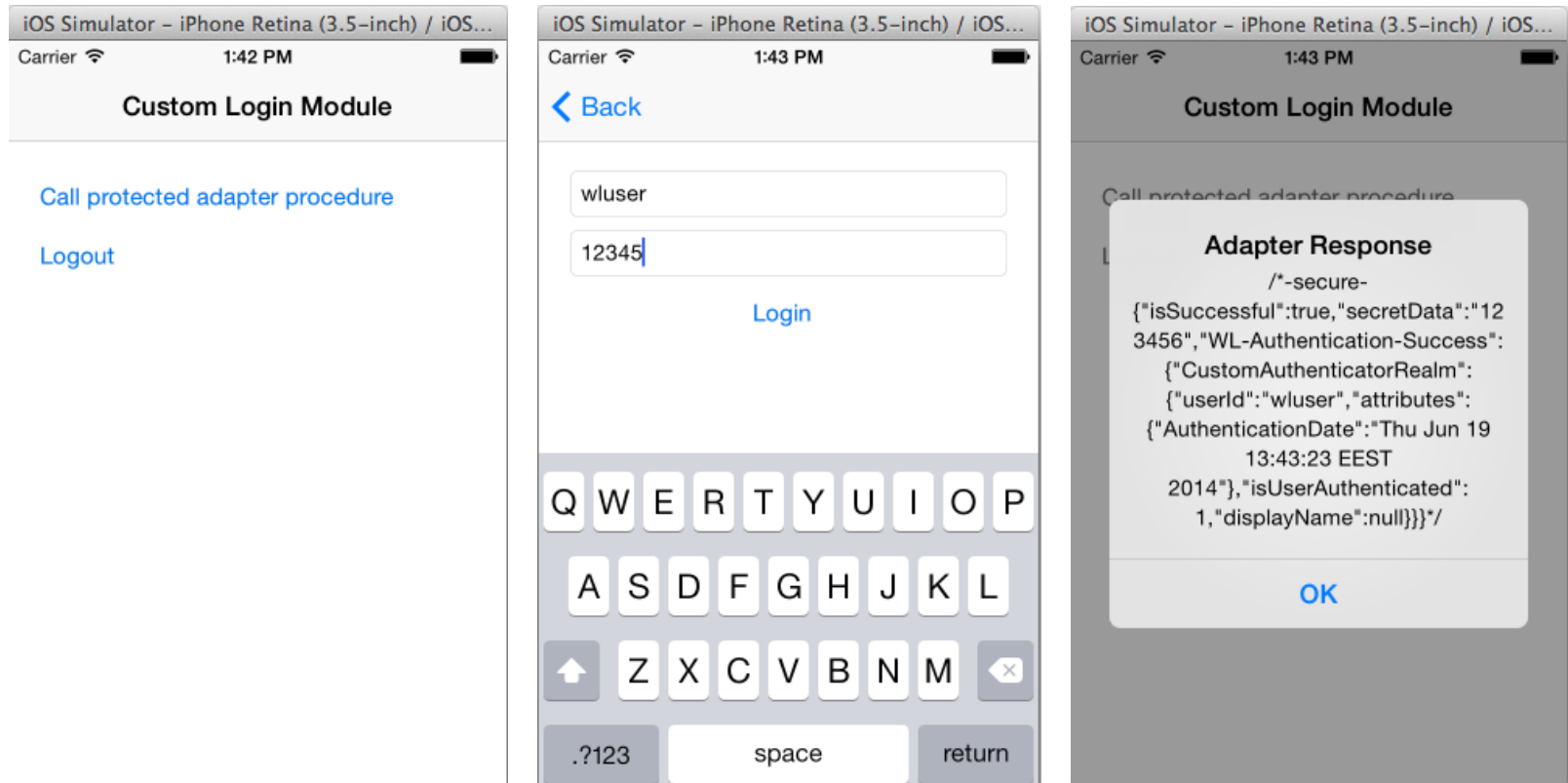
- The Procedure invocation triggers Worklight Server to send a challenge, which in turn triggers the custom challengeHandler object.

Agenda

- Introduction to authentication
- Configuring the authenticationConfig.xml file
- Creating a custom Java authenticator
- Creating a custom Java login module
- Creating client-side authentication components
- **Examining the result**

Examining the Result

- You can find the sample for this training module in the Getting Started page of the IBM Worklight Foundation documentation website at <http://www.ibm.com/mobile-docs>
- Enter *wluser* and *12345* as the user credentials



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 DriveArmonk, NY 10504-1785U.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-shiKanagawa 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 CorporationDept F6, Bldg 1
294 Route 100
Somers NY 10589-3216USA

- 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> 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> the sections entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at <http://www.ibm.com/software/info/product-privacy>.

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 Developer Edition support community at:
 - <https://www.ibm.com/developerworks/mobile/worklight/connect.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

