

Oracle® Enterprise Repository

Container Managed Setup and Configuration Guide

10g Release 3 (10.3)

July 2009

Copyright © 2008, 2009, Oracle. All rights reserved.

Primary Author: Vimmika Dinesh

Contributing Author: Scott Spieker, Jeff Schieli, Sharon Fay

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

Oracle Enterprise Repository

Container Managed Setup and Configuration Guide

Table of Contents

- **Configure Oracle Enterprise Repository for use with Container Managed Authentication**
 - **Configure the Container to Support Realm Authentication**
 - **Configure Oracle Enterprise Repository for use with Container Managed Authentication**
 - **Modify the Oracle Enterprise Repository Web.xml File to Allow for Container Authentication**

Overview

The container is configured appropriately with a Realm or Authenticator back-end prior to enabling the values within the Oracle Enterprise Repository application.

Configure the Container to Support Realm Authentication

Please refer to your application server configuration documentation to define a security realm. A sample realm configuration for Tomcat is mentioned below:

An example realm configuration for Tomcat 5.5.x is mentioned below. This realm definition is included within the **\$CATALINA_HOME/conf/server.xml** file. NOTE: Only one realm can be active within the **\$CATALINA_HOME/conf/server.xml** file at a time.

```
<Realm className="org.apache.catalina.realm.JNDIRealm"
  debug="99"
  connectionURL="ldap://ldap1.example.com:389"
  alternateURL="ldap://ldap2.example.com:636"
  contextFactory="com.sun.jndi.ldap.LdapCtxFactory"
  authentication="simple"
  referrals="follow"
  userBase="OU=people,DC=example,DC=com"
  userSubtree="true"
  userSearch="(uid={0})"
  userRoleName="employeeType"
  roleBase="ou=groups,DC=example,DC=com"
  roleName="cn"
  roleSearch="(uniqueMember={0})"
  roleSubtree="true"/>
```

If you would want to use the `UserDatabaseRealm` defined within Tomcat, which is enabled by default, then you can set the contents of your **CATALINA_HOME/conf/tomcat-users.xml** file as follows:

```
<?xml version='1.0' encoding='utf-8'?>
<tomcat-users>
  <role rolename="user"/>
  <role rolename="systemAdministrator"/>
  <role rolename="bogus"/>
  <role rolename="aler_user"/>
  <role rolename="admin"/>

  <user username="user" password="user" roles="aler_user,user"/> <!-- Positive Test case -->
  <user username="u1" password="u1" roles="user"/> <!-- Negative Test Case -->
  <user username="container" password="container" roles="aler_user,user"/>
```

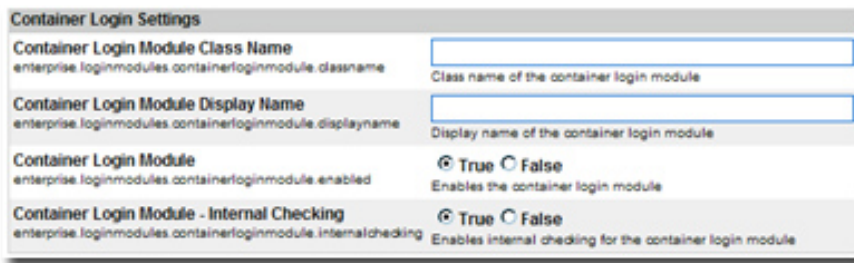
```
<user username="bogus" password="bogus" roles="bogus"/>
<user username="admin" password="admincontainer" roles="aler_user,user,admin"/>
</tomcat-users>
```

Configure Oracle Enterprise Repository for Container Managed Authentication

You can configure the Oracle Enterprise Repository for container managed authentication with the **Access Administrator** rights. This procedure is performed on the Oracle Enterprise Repository **Admin** screen.

1. Enter `container login module` in the System Settings **Search** text box.

The **Container Login Module** section opens in the **Enterprise Authentication** group of system settings.



2. Modify the following properties as indicated:

- **Container Login Module Class Name**
 - Enter `com.flashline.enterprise.authentication.server.loginmodule.ContainerLogin` in the text box.
- **Container Login Module Display Name**
 - Enter `Container Login Module` in the text box.
- **Container Login Module**
 - Set the property to **True**.
- **Enable the Container Managed Authentication Feature**
 - Set the `enterprise.authentication.container.enabled` to **True**.
- **Enable Role Synchronization from the User's Security Principle**
 - Set the `enterprise.authentication.container.synchroles.enabled` to **True**.
 - **NOTE:** When using Container Managed Authentication with BPM Harvester, the Exchange Utility, or any other REX operation, this property must be set to **false**. With this property set to false, user accounts will need to be created manually and have roles assigned to them by someone with at least **accessAdministrator** level permissions.

3. Click **Save**.

4. Enter `cookie login module` in the System Settings **Search** text box.

The **Cookie Login Settings** section opens in the **Enterprise Authentication** group of system settings.

5. Set the **Cookie Login Module** property to **False**.
6. Click **Save**.
7. Enter `plug-in login` in the System Settings **Search** text box.

The **Plugin Login Settings** section opens in the **Enterprise Authentication** group of system settings.

8. Enter `false` in the **Plug-in Login Module** text box.
9. Click **Save**.

Modify the Web Application's Web.xml File to Allow for Container Authentication

1. Stop the Oracle Enterprise Repository application or the application server that it runs within.
2. Modify the Oracle Enterprise Repository web.xml file:
 - o Add the following security constraint contents to the end of the file (NOTE: This configuration will need to be modified to fit your authentication requirements. This example uses BASIC authentication, which may not be appropriate for your environment).

```
<!-- Define a security constraint on this application -->
<security-constraint>
  <web-resource-collection>
    <web-resource-name>Entire Application</web-resource-name>
    <url-pattern>/* </url-pattern>
    <http-method>GET</http-method>
    <http-method>PUT</http-method>
    <http-method>POST</http-method>
    <http-method>DELETE</http-method>
  </web-resource-collection>
  <auth-constraint>
    <description>These roles have access to the Oracle Enterprise Repository</description>
    <role-name>user</role-name>
  </auth-constraint>
</security-constraint>
<security-constraint>
  <web-resource-collection>
    <web-resource-name>Secure Web Service</web-resource-name>
    <url-pattern>/services/FlashlineRegistry</url-pattern>
  </web-resource-collection>
</security-constraint>

<!-- Define the login configuration for this application -->
<login-config>
  <auth-method>BASIC</auth-method>
```

```
<realm-name>Oracle Enterprise Repository</realm-name>  
</login-config>
```

```
<security-role>  
  <role-name>user</role-name>  
  <role-name>admin</role-name>  
  <role-name>accessAdministrator</role-name>  
  <role-name>advancedSubmitter</role-name>  
  <role-name>businessAnalyst</role-name>  
  <role-name>projectAdministrator</role-name>  
  <role-name>projectArchitect</role-name>  
  <role-name>registrar</role-name>  
  <role-name>registrarAdministrator</role-name>  
  <role-name>systemAdministrator</role-name>  
</security-role>
```

3. Start / Restart the Oracle Enterprise Repository application.