Managing Java CAPS Users

Part No: 821–2545
March 2011

ORACLE

Copyright © 2008, 2011, Oracle and/or its affiliates. All rights reserved.

License Restrictions Warranty/Consequential Damages Disclaimer

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

Warranty Disclaimer

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

Restricted Rights Notice

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, 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, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

Hazardous Applications Notice

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

Trademark Notice

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

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

Third Party Content, Products, and Services Disclaimer

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

120126@25097

Contents

Managing Java CAPS Users

The topics listed here provide information about how to manage users in Oracle Java Composite Application Platform Suite (Java CAPS).

Managing Repository Users

This category includes the following users:

- Users of Java CAPS Repository-based projects in the NetBeans IDE
- Users of the Java CAPS Uploader

The `admin` and `Administrator` users are responsible for creating these users and for assigning the appropriate roles. User management changes take effect immediately. You do not need to restart the Repository.

For information about how to use a Lightweight Directory Access Protocol (LDAP) server to manage Repository users, see *Using LDAP with Oracle Java CAPS*.

Repository User Names and Roles

The Repository includes the following default users. These users are created by default for testing and development purposes only. You should create new users for your production environment.

TABLE 1 Default Repository Users

User Name	Default Password
admin	adminadmin
Administrator	STC

User names can contain alphabetic, numeric, or underscore characters. User names must begin with an alphabetic character. Multibyte characters are not supported. User names are case sensitive. Roles enable you to organize users into groups. Each user name is associated with one or more predefined roles.

The following table describes the predefined roles for Repository users. The default Repository users have all of these roles. When you create a user, you can limit what the user can do by assigning only the appropriate roles. The `all` role is mandatory for each user.

TABLE 2 Predefined Roles (Repository)

Role	Tasks Allowed
all	A user name with this role can: ■ Work with Java CAPS Repository-based projects in the NetBeans IDE ■ Perform downloads in the Java CAPS Uploader
administration	A user name with this role has the privileges of the `all` role, plus the following privilege: ■ Perform uploads in the Java CAPS Uploader
management	This role has been deprecated.

If a user has more than one role, then the user's privileges are the combined privileges from all of the user's roles.

Note – The `admin` and `Administrator` users are the only users that can create other users.

Adding and Deleting Repository Users

You can add and delete Repository users from the NetBeans IDE.

▼ To Add a Repository User

1 In the NetBeans IDE, choose Tools > CAPS Repository > Maintain Users.

The User Management dialog box appears.

2. **Click Add.**

   The second User Management dialog box appears.

3. **In the User field, enter a name for the user.**

   User names can contain alphabetic, numeric, or underscore characters. User names must begin with an alphabetic character. Multibyte characters are not supported. User names are case sensitive.

4. **In the Password field, enter a password for the user.**

   Multibyte characters are not supported.

5. **In the Confirm Password field, enter the password again.**

Note – Each user is automatically assigned to the `all` role, which is required to connect to the Repository.

---

6. **Click OK.**

   The user name is added to the list in the initial User Management dialog box. This user can now log in with the assigned user name and password.

7. **Click Close.**

▼ To Delete a Repository User

1. **In the NetBeans IDE, choose Tools > CAPS Repository > Maintain Users.**

   The User Management dialog box appears.

2. **Select the user and click Delete.**

   The user is removed from the list.

3. **Click Close.**

Note – You cannot delete the `admin` user or the `Administrator` user.

Adding and Deleting Roles

You can add and delete roles for a Repository user. You perform these procedures in the NetBeans IDE.

Note – You cannot delete the `all` role for a user.

▼ To Add a Role for a Repository User

1. **In the NetBeans IDE, choose Tools > CAPS Repository > Maintain Users.**
   The User Management dialog box appears.
2. **Select the user and click Modify.**
   The second User Management dialog box appears.
3. **Click Add Role.**
   The Add Role dialog box appears.
4. **Select the desired role and click OK.**
   The new role appears in the list for the selected user.
5. **Click OK.**
6. **Click Close.**

▼ To Delete a Role for a Repository User

1. **In the NetBeans IDE, choose Tools > CAPS Repository > Maintain Users.**
   The User Management dialog box appears.
2. **Select the user and click Modify.**
   The second User Management dialog box appears.
3. **Select the role that you want to delete and click Delete Role.**
   The role disappears from the list.
4. **Click OK.**
5. **Click Close.**

Changing Passwords

The following procedure describes how users can change their password.

▼ To Change a Password

1. **In the NetBeans IDE, choose Tools > CAPS Repository > Maintain Users.**
   The User Management dialog box appears.
2. **Select the user and click Modify.**
   The second User Management dialog box appears.
3. **In the Password field, enter the new password for the user.**
   Multibyte characters are not supported.
4. **In the Confirm Password field, enter the password again.**
5. **Click OK.**
6. **Click Close.**

Creating Roles

You can create roles in addition to the predefined roles. This feature provides a means for organizing users into groups.

▼ To Create a Role for a Current User

1. **In the NetBeans IDE, choose Tools > CAPS Repository > Maintain Users.**
   The User Management dialog box appears.
2. **Select the user and click Modify.**
   The second User Management dialog box appears.
3. **Click Add Role.**
   The Add Role dialog box appears.
4. **Click Create Role.**
   The Role dialog box appears.
5. **In the Role field, type the name of the new role that you are creating.**
   Multibyte characters are not supported.
6. **Click OK.**
   The new role has been added to the list.

7 **Select the new role and click OK.**

The role is added for the selected user.

8 **Click OK.**

9 **Click Close.**

Managing Oracle Java CAPS JMS IQ Manager Users

This topic explains how to use a file-based realm to manage Oracle Java CAPS JMS IQ Manager users. A *realm* is a collection of users, groups, and roles that are used in enforcing security policies.

For information about how to use a Lightweight Directory Access Protocol (LDAP)-based realm to manage Oracle Java CAPS JMS IQ Manager users, see *Using LDAP with Oracle Java CAPS*.

Oracle Java CAPS JMS IQ Manager User Names and Roles

By default, Oracle Java CAPS JMS IQ Manager stores user information in the user store of the GlassFish Application Server. When you install Java CAPS, you create one default administrator user. The default name for this user is admin, but you must specify a password during installation.

Roles enable you to organize users into groups. Each user name is associated with one or more predefined roles. The following table describes the predefined roles for Oracle Java CAPS JMS IQ Manager users.

TABLE 3 Predefined Roles (Oracle Java CAPS JMS IQ Manager)

Role	Tasks Allowed
application	Enables clients to access the JMS IQ Manager.
asadmin	Enables use of the JMS control utility (`stcmsctrlutil`) or Enterprise Manager, and enables clients to access the JMS IQ Manager.

Disabling and Enabling the File-Based Realm

By default, Oracle Java CAPS JMS IQ Manager is configured to use a file-based realm for user management. You can disable and enable the file-based realm using the Configuration Agent.

To Log In to the Configuration Agent

1. **If the application server is not running, then start the application server.**
2. **In a browser, enter the following URL:**

   `http://hostname:portnumber/configagent`

   Set the hostname to the TCP/IP host name of the computer where the application server is installed. Set the port number to the administration port number of the application server. For example:

   `http://myserver.company.com:4848/configagent`

   The Configuration Agent Security Gateway appears.
3. **In the User ID field, enter an application server user name.**
4. **In the Password field, enter the corresponding password.**
5. **Click Login.**

   The Configuration Agent appears.

To Disable the File-Based Realm

1. **In the left pane of the Configuration Agent, click the JMS IQ Manager node (for example, `IQ_Manager_18007`).**
2. **Click the Access Control tab.**
3. **Clear the check box to the right of the Enable File Realm label.**
4. **Ensure that at least one other realm is selected, and that the Default Realm drop-down list is not set to the file-based realm.**
5. **Click Save.**

To Enable the File-Based Realm

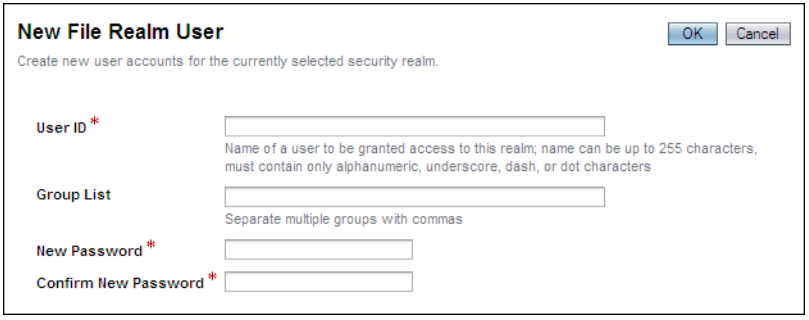
1. **In the left pane of the Configuration Agent, click the JMS IQ Manager node (for example, `IQ_Manager_18007`).**
2. **Click the Access Control tab.**
3. **Ensure that the check box to the right of the Require Authentication label is selected.**

4 Select the check box to the right of the Enable File Realm label.

5 Click Save.

Adding and Deleting Oracle Java CAPS JMS IQ Manager Users

If you are using the file-based realm to manage Oracle Java CAPS JMS IQ Manager users, then you add and delete users from the GlassFish Admin Console.



▼ To Add an Oracle Java CAPS JMS IQ Manager User

1 Log in to the Admin Console.

2 In the left pane, expand the Configuration node, the Security node, and the Realms node.

3 In the left pane, select the `admin-realm` node.

4 Click Manage Users.

5 Click New.

6 In the User ID field, enter a name for the user.

7 In the Group List field, enter one of the Java CAPS JMS IQ Manager roles: `asadmin` or `application`.

8 In the New Password and Confirm New Password fields, enter the password.

9 Click OK.

▼ To Delete an Oracle Java CAPS JMS IQ Manager User

1. **Log in to the Admin Console.**
2. **In the left pane, expand the Configuration node, the Security node, and the Realms node.**
3. **In the left pane, select the `admin-realm` node.**
4. **Click Manage Users.**
5. **Select the check box to the left of the user.**
6. **Click Delete.**

Managing Enterprise Manager Users

This category of user management refers to users who log in to Enterprise Manager to manage running Java CAPS applications.

For information about how to use a Lightweight Directory Access Protocol (LDAP) server to manage Enterprise Manager users, see *Using LDAP with Oracle Java CAPS*.

Enterprise Manager User Names and Roles

Enterprise Manager includes the following default users. These users are created by default for testing and development purposes only. You should create new users for your production environment.

TABLE 4 Default Enterprise Manager Users

User Name	Default Password
admin	adminadmin
Administrator	STC

Roles enable you to organize users into groups. Each user name is associated with one or more predefined roles. The following table describes the predefined roles for Enterprise Manager users. The default Enterprise Manager users have all of these roles. When you create a user, you can limit what the user can do by assigning only the appropriate roles.

TABLE 5 Predefined Roles (Enterprise Manager)

Role	Tasks Allowed
Deployment	Deploy and undeploy applications, manage servers, and monitor deployments.
User Management	Manage users of Enterprise Manager.
Read-Only Monitor	View information about Project components (not including Java Message Service components).
Controlling Monitor	Start, stop, and restart Project components (not including JMS components) and servers.
JMS Read-Only Monitor	View information about JMS components and messages.
JMS Read-Write Monitor	Create, edit, and delete JMS messages and destinations.
Manager	Manage the management applications and view application routing information.

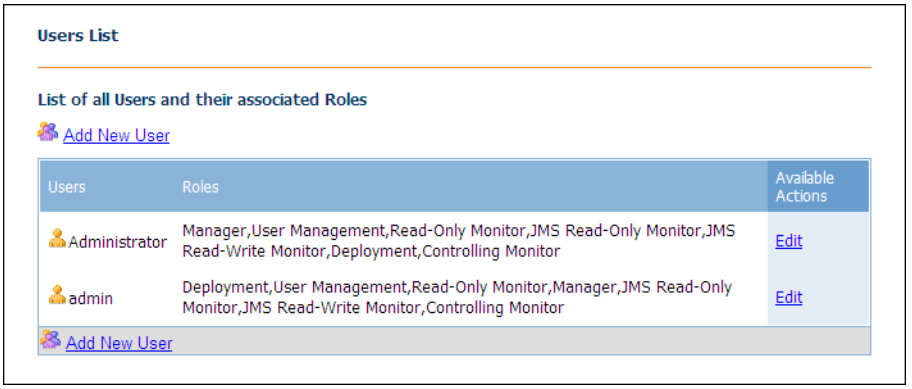
Security Gateway Overview

Enterprise Manager relies on a security gateway for centralized authentication. When a user tries to access Enterprise Manager, the gateway displays a login page. The user must enter a user name and password. If the user name and password are valid, then the home page of Enterprise Manager appears.

Enterprise Manager is composed of various management applications. All of the management applications rely on the security gateway for authentication. After a user is authenticated during the login procedure, the user can access each management application without needing to reenter the user name and password. This feature is called *single sign-on*. When a user exits Enterprise Manager and then attempts to log in at a later time, the gateway once again displays the login screen.

Adding and Deleting Enterprise Manager Users

You can add and delete Enterprise Manager users. To perform these tasks, you must have the `User Management` role. The following image shows the Users List page.



In order for the `JMS Read-Only Monitor` and `JMS Read-Write Monitor` roles to function correctly, the `Read-Only Monitor` role must be checked. If you select either role without checking the `Read-Only Monitor` role, then Enterprise Manager automatically checks the `Read-Only Monitor` role.

▼ To Add an Enterprise Manager User

1. **In the Explorer panel of Enterprise Manager, click User Management.**

   The Users List page appears.

2. **Click Add New User.**

   The Add/Edit User window appears.

3. **In the User Name field, enter a name for the user.**

   The user name is case sensitive.

4. **In the Password field, enter a password for the user.**

5. **In the Confirm Password field, enter the password again.**

6. **(Optional) In the Description field, enter a description for the user.**

7. **Select one or more predefined roles.**

8. **Click Submit.**

▼ To Delete an Enterprise Manager User

1. **In the Explorer panel of Enterprise Manager, click User Management.**
   The Users List page appears.
2. **In the Available Actions column, click Remove.**

Note – You cannot delete the `admin` user or the `Administrator` user.

Editing Enterprise Manager Users

You can edit Enterprise Manager users. For example, you can change the password of an existing user. To perform this task, you must have the `User Management` role.

▼ To Edit an Enterprise Manager User

1. **In the Explorer panel of Enterprise Manager, click User Management.**
   The Users List page appears.
2. **In the Available Actions column, click Edit.**
3. **Make one or more changes.**
4. **Click Submit.**
   If the user is currently logged in, then the changes become effective after the user logs out and logs in again.

Index

O

P

R

S

U