



Managing Java CAPS Users



Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 820-3401-10
June 2008

Copyright 2008 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more U.S. patents or pending patent applications in the U.S. and in other countries.

U.S. Government Rights – Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

This distribution may include materials developed by third parties.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, the Solaris logo, the Java Coffee Cup logo, docs.sun.com, Java, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. or its subsidiaries in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and SunTM Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

Products covered by and information contained in this publication are controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical or biological weapons or nuclear maritime end uses or end users, whether direct or indirect, are strictly prohibited. Export or reexport to countries subject to U.S. embargo or to entities identified on U.S. export exclusion lists, including, but not limited to, the denied persons and specially designated nationals lists is strictly prohibited.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Contents

1	Managing Java CAPS Users	5
	Managing Repository Users	5
	Repository User Names and Roles	5
	Adding and Deleting Repository Users	6
	Adding and Deleting Roles	8
	Changing Passwords	9
	Creating Roles	9
	Managing Sun JMS IQ Manager Users	10
	Sun JMS IQ Manager User Names and Roles	10
	Disabling and Enabling the File-Based Realm	11
	Adding and Deleting Sun JMS IQ Manager Users	12
	Managing Enterprise Manager Users	13
	Enterprise Manager User Names and Roles	13
	Security Gateway Overview	14
	Adding and Deleting Enterprise Manager Users	15
	Editing Enterprise Manager Users	16
	Index	17

Managing Java CAPS Users

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

If you have any questions or problems, see the Java CAPS web site at <http://goldstar.stc.com/support>.

- “Managing Repository Users” on page 5
- “Managing Sun JMS IQ Manager Users” on page 10
- “Managing Enterprise Manager Users” on page 13

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 Java CAPS*.

Repository User Names and Roles

The Repository includes the following default users.

TABLE 1-1 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 1-2 Predefined Roles (Repository)

Role	Tasks Allowed
all	A user name with this role can: <ul style="list-style-type: none">■ 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 <code>all</code> role, plus the following privilege: <ul style="list-style-type: none">■ 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 Sun JMS IQ Manager Users

This topic explains how to use a file-based realm to manage Sun 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 Sun JMS IQ Manager users, see *Using LDAP with Java CAPS*.

Sun JMS IQ Manager User Names and Roles

By default, Sun JMS IQ Manager stores user information in the user store of Sun Java™ System Application Server.

The application server includes the following default user. Java CAPS allows you to change the user name and password during installation.

TABLE 1-3 Default Application Server User

User Name	Default Password
admin	adminadmin

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 Sun JMS IQ Manager users.

TABLE 1-4 Predefined Roles (Sun JMS IQ Manager)

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

Disabling and Enabling the File-Based Realm

By default, Sun JMS IQ Manager is configured to use a file-based realm for user management.

You can disable and enable the file-based realm by 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 Sun JMS IQ Manager Users

If you are using the file-based realm to manage Sun JMS IQ Manager users, then you add and delete users from the Sun Java System Application Server Admin Console.

New File Realm User OK Cancel

Create new user accounts for the currently selected security realm.

User ID *
Name of a user to be granted access to this realm; name can be up to 255 characters, must contain only alphanumeric, underscore, dash, or dot characters

Group List
Separate multiple groups with commas

New Password *

Confirm New Password *

▼ To Add a Sun 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 Sun 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 a Sun 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 Java CAPS*.

Enterprise Manager User Names and Roles

Enterprise Manager includes the following default users.

TABLE 1-5 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 1-6 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 screen capture shows the Users List page.

Users	Roles	Available Actions
Administrator	Manager, User Management, Read-Only Monitor, JMS Read-Only Monitor, JMS Read-Write Monitor, Deployment, Controlling Monitor	Edit
admin	Deployment, User Management, Read-Only Monitor, Manager, JMS Read-Only Monitor, JMS Read-Write Monitor, Controlling Monitor	Edit

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

A

adding

- Enterprise Manager users, 15-16
- Repository users, 7
- roles, 8
- Sun JMS IQ Manager users, 12-13

admin user

- Enterprise Manager, 14
- Repository, 6
- Sun JMS IQ Manager, 10

administration role, 6

Administrator user

- Enterprise Manager, 14
- Repository, 6

all role, 6

application role, 11

asadmin role, 11

C

case sensitivity, user names, 6

Configuration Agent, logging in, 11

Controlling Monitor role, 14

creating, roles, 9-10

D

deleting

- Enterprise Manager users, 16
- Repository users, 7-8

deleting (*Continued*)

- roles, 8
- Sun JMS IQ Manager users, 12-13
- Deployment role, 14

E

Enterprise Manager user management, 13-16

F

file realm, 10

G

gateway, 14-15

J

JMS Read-Only Monitor role, 14

JMS Read-Write Monitor role, 14

M

management role, 6

Manager role, 14

multibyte characters, not supported, 6

P

passwords

- Enterprise Manager users, 16
- Repository users, 7, 9

R

Read-Only Monitor role, 14

realm

- defined, 10
- disabling, 11-12
- enabling, 11-12

Repository user management, 5-10

roles

- adding, 8
- creating, 9-10
- deleting, 8
- predefined, 6, 10, 14

S

security gateway, 14-15

single sign-on, 14-15

Sun JMS IQ Manager user management, 10-13

U

Uploader, users of, 5

user management

- Enterprise Manager, 13-16
- Repository, 5-10
- Sun JMS IQ Manager, 10-13

User Management role, 14

users

- admin, 6, 10, 14
- Administrator, 6, 14