One Design
One Server
One User Experience

Managing an Encyclopedia Volume

Information in this document is subject to change without notice. Examples provided are fictitious. No part of this document may be reproduced or transmitted in any form, or by any means, electronic or mechanical, for any purpose, in whole or in part, without the express written permission of Actuate Corporation.

© 1995 - 2011 by Actuate Corporation. All rights reserved. Printed in the United States of America.

Contains information proprietary to:
Actuate Corporation, 2207 Bridgepointe Parkway, San Mateo, CA 94404

www.actuate.com
www.birt-exchange.com

The software described in this manual is provided by Actuate Corporation under an Actuate License agreement. The software may be used only in accordance with the terms of the agreement. Actuate software products are protected by U.S. and International patents and patents pending. For a current list of patents, please see http://www.actuate.com/patents.

Actuate Corporation trademarks and registered trademarks include:
Actuate, ActuateOne, the Actuate logo, Archived Data Analytics, BIRT, Collaborative Reporting Architecture, e.Analysis, e.Report, e.Reporting, e.Spreadsheet, Encyclopedia, Interactive Viewing, OnPerformance, Performancesoft, Performancesoft Track, Performancesoft Views, Report Encyclopedia, Reportlet, The people behind BIRT, X2BIRT, and XML reports.

Actuate products may contain third-party products or technologies. Third-party trademarks or registered trademarks of their respective owners, companies, or organizations include:

Adobe Systems Incorporated: Flash Player. Apache Software Foundation (www.apache.org): Axis, Axis2, Batik, Batik SVG library, Commons Command Line Interface (CLI), Commons Codec, Derby, Shindig, Struts, Tomcat, Xerces, Xerces2 Java Parser, and Xerces-C++ XML Parser. Bits Per Second, Ltd. and Graphics Server Technologies, L.P.: Graphics Server. Bruno Lowagie and Paulo Soares: iText, licensed under the Mozilla Public License (MPL). Castor (www.castor.org), ExoLab Project (www.exolab.org), and Intalio, Inc. (www.intalio.org): Castor. Codejock Software: Xtreme Toolkit Pro. DataDirect Technologies Corporation: DataDirect JDBC, DataDirect ODBC. Eclipse Foundation, Inc. (www.eclipse.org): Babel, Data Tools Platform (DTP) ODA, Eclipse SDK, Graphics Editor Framework (GEF), Eclipse Modeling Framework (EMF), and Eclipse Web Tools Platform (WTP), licensed under the Eclipse Public License (EPL). Jason Hsueth and Kenton Varda (code.google.com): Protocole Buffer. ImageMagick Studio LLC.: ImageMagick. InfoSoft Global (P) Ltd.: FusionCharts, FusionMaps, FusionWidgets, PowerCharts. Mark Adler and Jean-loup Gailly (www.zlib.net): zLib. Matt Ingenthron, Eric D. Lambert, and Dustin Sallings (code.google.com): Spymemcached, licensed under the MIT OSI License. International Components for Unicode (ICU): ICU library. KL Group, Inc.: XRT Graph, licensed under XRT for Motif Binary License Agreement. LEAD Technologies, Inc.: LEADTOOLS. Microsoft Corporation (Microsoft Developer Network): CompoundDocument Library. Mozilla: Mozilla XML Parser, licensed under the Mozilla Public License (MPL). MySQL Americas, Inc.: MySQL Connector. Netscape Communications Corporation, Inc.: Rhino, licensed under the Netscape Public License (NPL). Oracle Corporation: Berkeley DB. PostgreSQL Global Development Group: pgAdmin, PostgreSQL, PostgreSQL JDBC driver. Rogue Wave Software, Inc.: Rogue Wave Library SourcePro Core, tools.h++. Sam Stephenson (prototype.conio.net): prototype.js, licensed under the MIT license. Sencha Inc.: Ext JS. Sun Microsystems, Inc.: JAXB, JDK, Jstl. ThimbleWare, Inc.: JMemcached, licensed under the Apache Public License (APL). World Wide Web Consortium (W3C)(MIT, ERCIM, Keio): Flute, JTidy, Simple API for CSS. XFree86 Project, Inc.: (www.xfree86.org): xvfb. Yuri Kanivets (code.google.com): Android Wheel gadget, licensed under the Apache Public License (APL). ZXing authors (code.google.com): ZXing, licensed under the Apache Public License (APL).

All other brand or product names are trademarks or registered trademarks of their respective owners, companies, or organizations.

Document No. 110812-2-530304 July 8, 2011

Contents

About *Managing an Encyclopedia Volume*. vii

Chapter 1
Understanding Encyclopedia volume management 1
About Encyclopedia volume management 2
Logging in to Management Console 2
Navigating in Files and Folders 5
About designs 6
Running a design 6
About user types 9
Setting display options 11
Filtering Encyclopedia volume data 13
Performing a search 16

Chapter 2
Managing users 19
About user accounts 20
Creating a user account 21
About job priority 21
Modifying user properties 28
Modifying user properties for multiple accounts 31
Cloning a user 36
Deleting a user 37

Chapter 3
Working with security roles 39
About security roles 40
About hierarchical security roles 40
About system-defined security roles 41
About Information Console functionality levels 42
Managing security roles 43

Chapter 4
Managing files and folders 53
About files and folders 54
Understanding file and folder properties 55
About General properties 56
About file and folder privileges 58
About folder privileges 58

About file privileges 58
Setting privileges on a folder or file 59
About dependencies 62
About autoarchiving 63
Using the File Type list 65
About the default or inherited archiving policy 67
Viewing the existing archive policy 67
Selecting not to delete automatically 68
Selecting to delete by specifying a time or date 68
Adding files and folders to the Encyclopedia volume 71
Creating a folder 71
Uploading a file 73
Deleting, copying, moving, and downloading a file or folder 78
Deleting a file or folder 78
Copying or moving a file or folder 79
Managing Actuate queries 83
Creating a query 83
Editing a query 84
Running and scheduling a query 85
Caching information objects 86
Activating a cache object 86
Understanding the status of a cache object 87
Populating the cache table 88

Chapter 5
Scheduling, running, and managing designs 89
Understanding how to run a design 90
Running a design 91
Scheduling a job 93
Specifying scheduling properties 94
About scheduling a job 96
About job priority and resource groups 98
About retrying a failed job 100
Setting the Encyclopedia volume job retry policy 101
Specifying parameters 101
Saving parameter values for reuse 102
Specifying output settings 103
Bundling an ROI file 105
Specifying a headline 106
About the file format of a document 106
Setting privileges for an output document 113
About Datamart Security 114
Setting channel options 115

Notifying users about a job 115
Printing a document 117
Understanding service requirements 119
Troubleshooting problems 119
Solving a dependency problem 120
Solving a privilege problem 121
Bursting a document 121
Using a date-and-time expression in a document or version name 122
About the locale maps 122
About predefined date-and-time formats 122
About a file name in an expression 123
Creating a custom date format 123
Creating a custom time format 125
Monitoring job status 127
Setting job completion notice properties 128
Getting detailed information about a job 131
Editing a scheduled job 134
Cancelling a scheduled job 135
Deleting a job or job completion notice 135

Chapter 6
Managing channels and notification groups 137
About channels 138
Managing channels 138
Subscribing to channels 138
About the personal channel 138
Creating and managing channels 139
Viewing a document 147
Working with notification groups 147

Chapter 7
Working with file types 155
About file types and volume management 156
Working with Actuate Query 156
About the information object ODA driver 157
About the Actuate Query template file 157
About the Actuate Query template report design 157
Using a customized Actuate Query template 158
Managing Actuate Analytics files 158
About Analytics file types 159
About Analytics data source support 159
About the Analytics default data source 159
About connection information in an external file 160

Accessing a Microsoft Analysis Services data cube 160
Managing spreadsheet designs 162
Understanding how iServer handles spreadsheet files 162
Specifying spreadsheet design connection properties 163
Setting parameters for spreadsheet designs 163

Chapter 8
Managing volume-level operations 167
Working at the volume level 168
Archiving files and removing empty folders 170
Using autoarchiving applications 171
Setting the volume's autoarchiving and purging rules 172
Scheduling and initiating an autoarchiving cycle 173
Setting web browser defaults 174
Setting volume privileges 175
Setting volume-level printer options 175

Chapter 9
Managing Encyclopedia volume security 179
About Encyclopedia volume security 180
About the types of privileges 180
About Page-Level Security and SmartSheet options 181
About accessing files and folders 181
Planning how to assign privileges 182
Setting privileges to access an information object 184
Using page-level security 185
Viewing reports using page-level security 185
Enabling page-level security 185
Using information object pass-through security 185
About Open Security 188
About RSSE 188
Open Security levels 190
About external user authentication 191
About external user properties 191
About external user registration 192
About externally defined security roles 193
About the All security role and external registration 193
About the anonymous user and external registration 193
About the Administrator security role and external registration 193
About the administrator user and external registration 193
About the Operator security role and external authentication 194
About channels and external authentication 194
Using Management Console with Open Security 194

About home folder privileges 194
About printer properties 194
About externally-defined properties 195
About searching when using an RSSE application 195
Using RSSE with page-level or SmartSheet security 195

Index 197

About *Managing an Encyclopedia Volume*

Managing an Encyclopedia Volume discusses how to administer an Actuate iServer System Encyclopedia volume. The chapters in this guide are:

- *About Managing an Encyclopedia Volume.* This chapter provides an overview of this guide.
- *Chapter 1. Understanding Encyclopedia volume management.* This chapter discusses how to connect to an Encyclopedia volume and how to use the Management Console.
- *Chapter 2. Managing users.* This chapter discusses how to create and maintain user accounts.
- *Chapter 3. Working with security roles.* This chapter discusses how to create and use security roles, which apply a set of privileges to a group of users.
- *Chapter 4. Managing files and folders.* This chapter discusses the management of files and folders, including creating folders and uploading files.
- *Chapter 5. Scheduling, running, and managing designs.* This chapter discusses how to set up and run Actuate iServer System jobs.
- *Chapter 6. Managing channels and notification groups.* This chapter discusses how to manage channels and notification groups.
- *Chapter 7. Working with file types.* This chapter discusses the Encyclopedia volume file types, working with Actuate Query, administering Actuate Analytics files, and administering spreadsheet reports.
- *Chapter 8. Managing volume-level operations.* This chapter discusses volume-level management tasks, such as archiving files, backing up an Encyclopedia volume, setting system-wide printer options, and connecting to an external cache for running information objects.

- *Chapter 9. Managing Encyclopedia volume security.* This chapter discusses Encyclopedia security features, provides details about privileges, and discusses Open Security.

Chapter

1

Understanding Encyclopedia volume management

This chapter contains the following topics:

- About Encyclopedia volume management
- Filtering Encyclopedia volume data
- Performing a search

About Encyclopedia volume management

BIRT iServer is a document server that generates, manages and securely delivers Actuate Basic, BIRT, and BIRT spreadsheet documents stored in an Encyclopedia volume. An Encyclopedia volume is a disk-based repository containing designs, documents, information objects, shared libraries, and user information.

iServer extracts data from common data sources, such as relational databases and other data sources. iServer consists of the following components, which are accessible using a standard browser:

- Management Console
  Use this console to manage Encyclopedia volume user accounts, assign privileges, schedule designs, and distribute documents.
- Configuration Console
  Use this console to configure iServer and change system parameters, such as diagnostic logging and e-mail notification settings, and update your license.
- Information Console
  Use this console to run designs, view, and interact with documents. Figure 1-1 shows a typical reporting environment in which iServer generates documents, manages an Encyclopedia volume, and connects to multiple data sources.

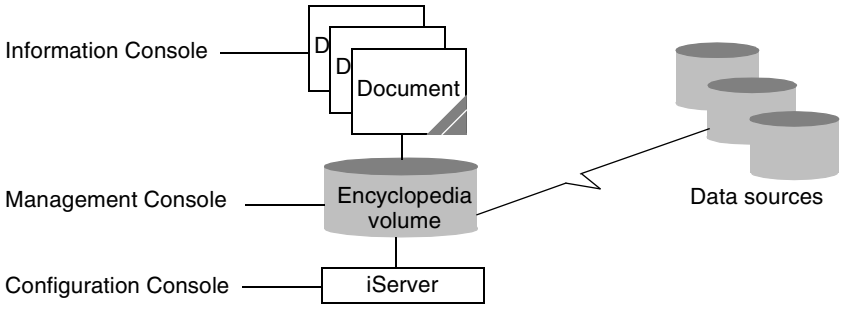

Figure 1-1 iServer reporting environment

Logging in to Management Console

To administer an Encyclopedia volume, you log in to Management Console. To log in to Management Console, the Actuate BIRT iServer service must be running.

By default, the service starts automatically when your system starts. If you do not choose to have the service start automatically during installation, you must start it manually or reconfigure the service to start when the system boots.

How to configure Actuate BIRT iServer startup properties

In Windows, to configure Actuate BIRT iServer service properties, perform the following tasks:

1 Choose Start➤Settings➤Control Panel➤Administrative Tools➤Services.

2 In Services, select Actuate BIRT iServer Enterprise service properties, as shown in Figure 1-2.

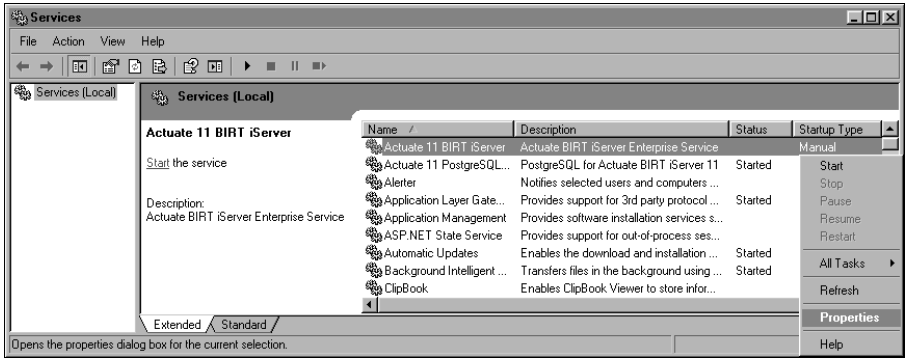

Figure 1-2 Choosing Actuate BIRT iServer service Properties

3 In Properties—General, set Startup type to Automatic, as shown in Figure 1-3.

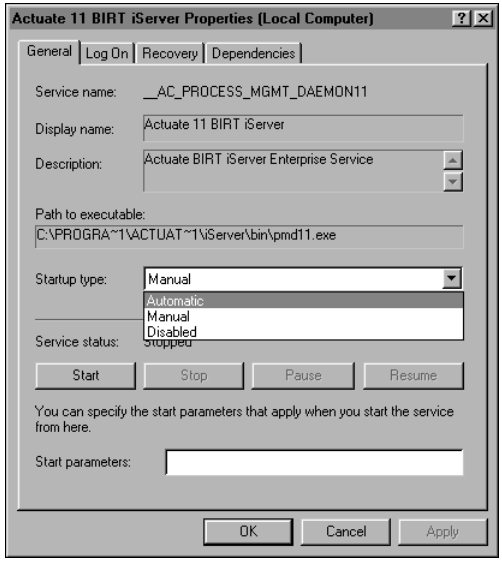

Figure 1-3 Configuring Startup type for Actuate BIRT iServer service

To run the service in your current session, you must start the service manually or reboot the system. To start the service manually, in Services, select Actuate BIRT iServer service Start, as shown in Figure 1-4.

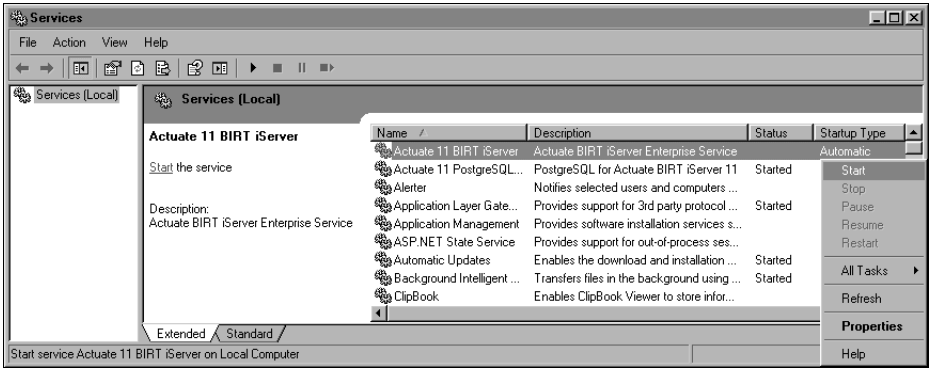

Figure 1-4 Choosing to start iServer service

In Linux, to configure Actuate BIRT iServer service properties, perform the following tasks:

1. To start Actuate BIRT iServer service automatically when your machine boots, log in as root, and type:

   ```
   ./AcServer/bin/update_rclocal.sh
   ```

2. To start Actuate BIRT iServer service manually, perform the following steps:

   1. Go to the iServer bin directory. For example:

      ```
      cd /opt/actuate/AcServer/bin
      ```

   2. Type:

      ```
      ./start_srvr.sh
      ```

You can launch Management Console locally or remotely to manage the Encyclopedia volume.

How to launch Management Console

1. Choose one of the following ways to launch Management Console:

   - In Windows, from the Start menu, choose:

     Start➤Programs➤Actuate 11➤BIRT iServer Management Console

     Or, type the following URL in a browser:

     http://localhost:8900/acadmin/login.jsp

   - In Linux, Open a browser and type the following URL:

     http://localhost:8900/acadmin/login.jsp

2 To log in to Management Console as Administrator, perform the following steps:

1 Accept or specify Administrator as the user name.

2 If you are logging in to Management Console for the first time, leave Password blank.

3 Accept the default Language and Time zone, or choose the locale for your region.

Figure 1-5 shows the login page for Management Console.

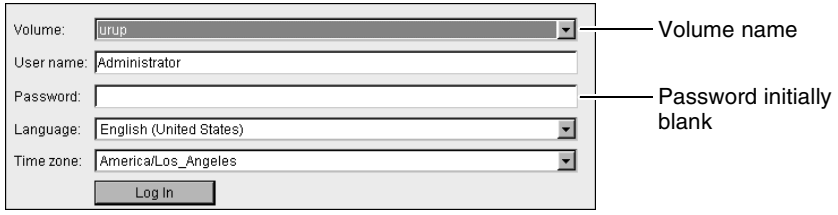

Figure 1-5 Logging in to Management Console

Choose Log In.

Navigating in Files and Folders

When you log in, Management Console displays the list of files and folders in the administrator home folder. The list consists of a number of sample BIRT design files and the BIRT Examples Read Me file, which contains a brief description of each sample BIRT design. The path to the current folder appears above Filter. To navigate to another folder, choose a folder in the path, such as the root folder, which is the Encyclopedia volume name, as shown in Figure 1-6.

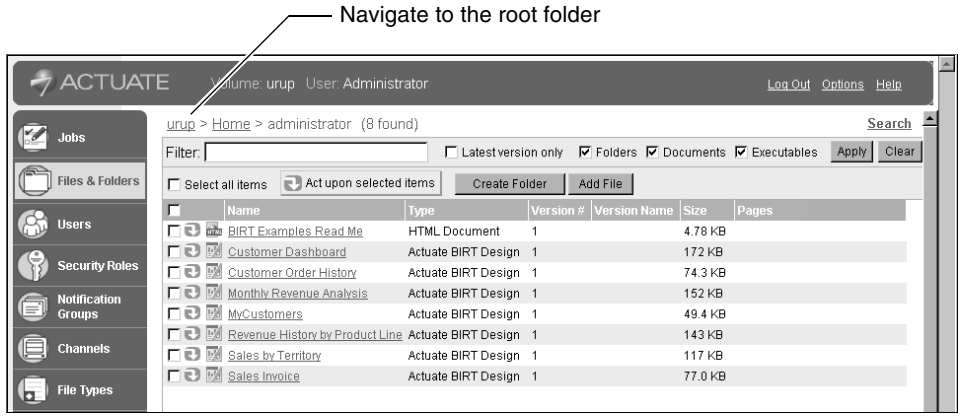

Figure 1-6 Viewing Files and Folders

Users typically have access to multiple levels of folders. From the root folder, choose the Public folder. The folder name is added to the path. Choose BIRT and BIRT Studio Examples and the path appears, as shown in Figure 1-7.

Figure 1-7 Viewing the path to the current folder

Each folder name in the path is a link to that folder. Choosing a folder name in the path displays the contents of that folder.

About designs

A design is an executable file that, when run, generates a document. Designs include the following file types:

Actuate BIRT Design (.rptdesign).

Actuate BIRT Spreadsheet Design (.sox).

Actuate Report Executable (.rox)

Figure 1-8 shows two types of designs, an Actuate BIRT Design and an Actuate BIRT Spreadsheet Executable.

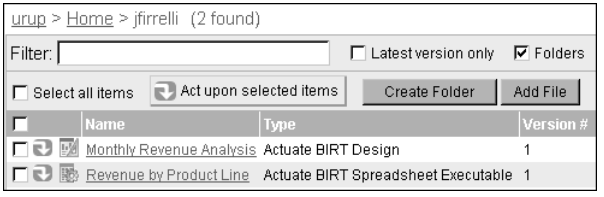

Figure 1-8 Two design files

Running a design

In addition to the sample designs in the administrator's home folder, shown in Figure 1-6, the following folders in the root directory also contain sample designs:

- Dashboard
  Contains a folder named Contents, containing a BIRT Dashboard file and a BIRT Gadget design.
- Public
  - BIRT and BIRT Studio Examples
    Contains a readme file and sample BIRT designs.

- Information Objects Based Examples
  Contains a readme file, a sample project folder, a BIRT design, and a BIRT Spreadsheet design.
- JSAPI Examples
  Contains examples of designs that call the Actuate JSAPI. View the documents these designs create in Information Console.
- Spreadsheet Examples
  Contains a readme file and sample BIRT Spreadsheet designs.

- Resources
  Contains three BIRT library (.rptlibrary) files:
  - BIRTSamples
  - themes
  - ThemesReportItems

  These are XML files that contain reusable and shareable design elements. A design developer uses a designer such as BIRT Designer Professional to create a .rptlibrary file. View these documents in Information Console.

Figure 1-9 shows the folders containing sample designs and design libraries in the root directory.

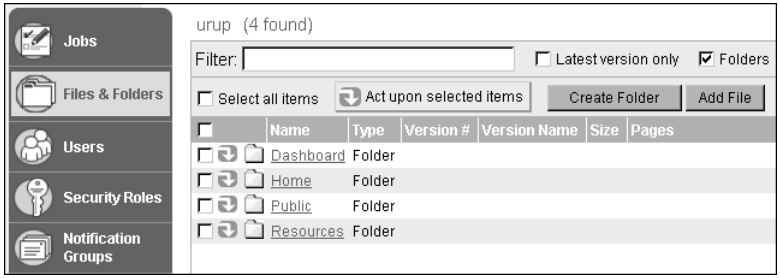

Figure 1-9 Accessing sample designs and design libraries

How to run a design

To run a BIRT example, perform the following tasks:

1. Choose the Public folder.
2. Choose the BIRT and BIRT Studio Examples subfolder.
3. Choose to run a design. For example, point to the arrow next to Product Sales by State and choose Run, as shown in Figure 1-10.

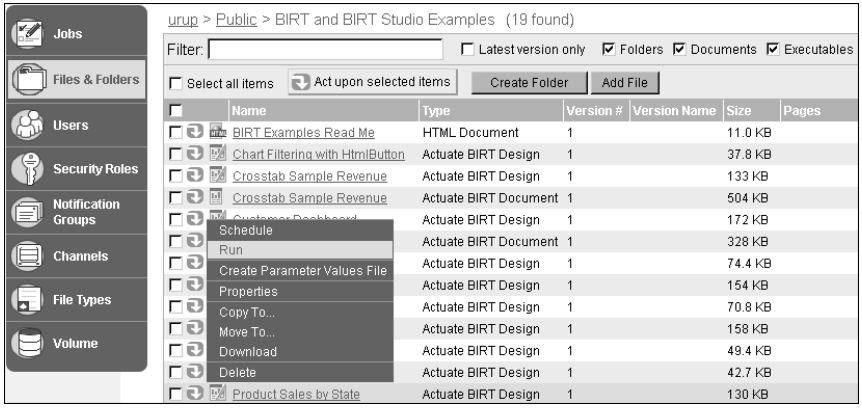

Figure 1-10 Choosing to run Product Sales by State

Run appears, as shown in Figure 1-11. Accept the default parameter in Please specify the product code. Choose OK.

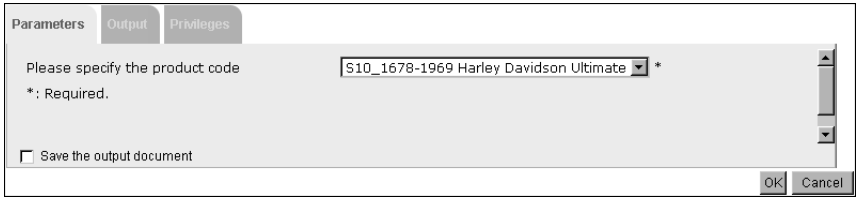

Figure 1-11 Running a design

iServer displays the document in the viewer, as shown in Figure 1-12.

Figure 1-12 Document displayed in the viewer

About user types

When an administrator logs in to Management Console, the side menu contains the options available to an administrator, as shown in Figure 1-13.

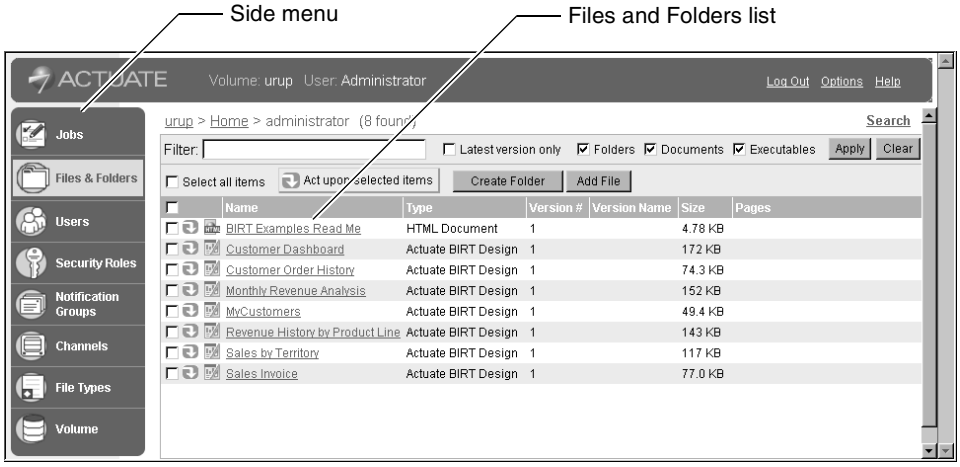

Figure 1-13 Viewing Adminstrator's list of files and folders

Management Console supports the following types of users and security roles:

- Administrator

  A user and a security role. A user with Administrator role privileges functions as the Administrator user. The Administrator has privileges to perform all tasks in BIRT iServer System.

- Operator

  A security role. A user with Operator role privileges performs tasks such as scheduling jobs, administering files and folders, performing online backup and auto archive operations, and printing.

- User

  A user with appropriate privileges can schedule jobs, view documents, administer files and folders, subscribe to channels, and configure personal settings in the user account.

Depending on the type of user or role, Management Console displays a different set of menu options, as shown in Figure 1-14.

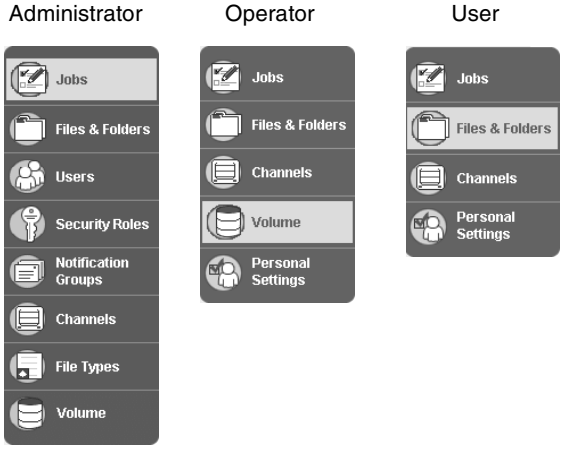

Figure 1-14 Menu options available to different types of users and roles

Table 1-1 describes the menu options available to each type of user and role.

Table 1-1 Management Console menu options

Icon	Description	Admin	Operator	User
Jobs	Displays lists of jobs created by the user, or all jobs, if logged in as the administrator, grouped according to status. Job status categories include scheduled, waiting for event, pending, running, and completed.	x	x	x
Files and Folders	Displays the list of files and folders accessible to the user, or all files and folders if logged in as the administrator.	x	x	x
Users	Displays the list of users who have access to the Encyclopedia volume.	x		
Security Roles	Displays the list of security roles.	x		
Notification Groups	Displays the list of user groups to notify about the status of documents.	x		
Channels	Displays the list of channels subscribed to by the user, or all channels if logged in as the administrator.	x	x	x
File Types	Displays the list of file types that the Encyclopedia volume can store.	x		

Table 1-1 Management Console menu options

Icon	Description	Admin	Operator	User
Volume	Allows the administrator and operator to configure volume properties, and perform online backup and auto archive operations.	x	x	
Personal Settings	Displays user settings, such as password, e-mail address, job notifications, roles, groups, channel subscriptions, privilege template, and printing options.		x	x

Setting display options

For each tabular list appearing in a menu choice, Options contains a corresponding list of available and selected columns which control the display. In Options, choose a category, such as Jobs Scheduled, Files and Folders, or Channels, and select the columns to appear in the tabular list.

Figure 1-15 shows the available and selected columns for Options—Users.

Figure 1-15 Selecting Options—Users

How to modify a tabular list

To modify the tabular list for Users, customizing:Management Console perform the following tasks:

1 To add a column from Available columns, such as Log in Disabled, select the column and choose the right arrow. Log in Disabled appears in the Selected columns list.

2 To remove a column from Selected columns, such as Description, select the column and choose the left arrow. Description appears in the Available columns list.

3 To move a column up in the Selected columns list, such as Log in Disabled, select the column and choose the up arrow. Log in Disabled appears above Home Folder in the Selected columns list.

4 To move a column down in the Selected columns list, such as Email Address, select the column and choose the down arrow. Email Address appears below Log in Disabled in the Selected columns list.

Figure 1-16 shows the available and selected columns for Options—Users.

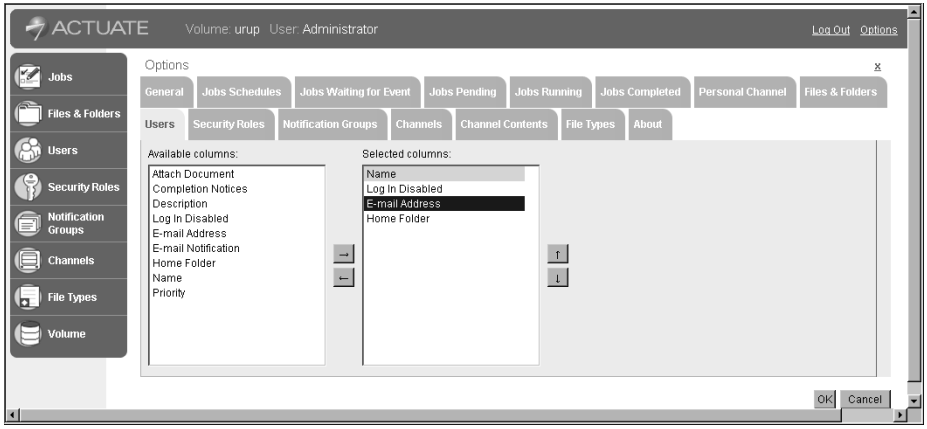

Figure 1-16 Modifying the tabular list in Options—Users

5 Choose OK.

Figure 1-17 shows the results of these changes in Users.

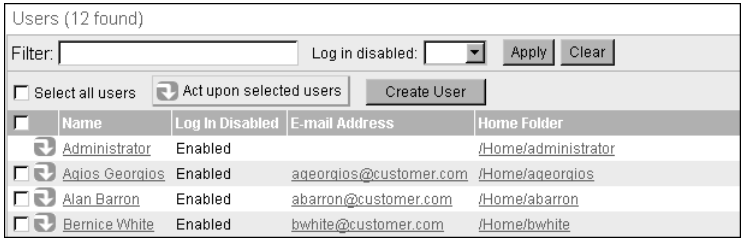

Figure 1-17 Viewing the modified tabular list in Users

Options—General contains the following settings, as shown in Figure 1-18:

- Number of rows to display per page in normal lists
  Reduces scrolling by controlling how many rows display in a normal list.

- Number of rows to display per page in search result lists
  Reduces scrolling by controlling how many rows display in a search result list.
- Locale
  Specifies the locale, such as English (United States)
- Time Zone
  Specifies the time zone, such as America/Los_Angeles

To modify these settings, type or select the appropriate setting information.

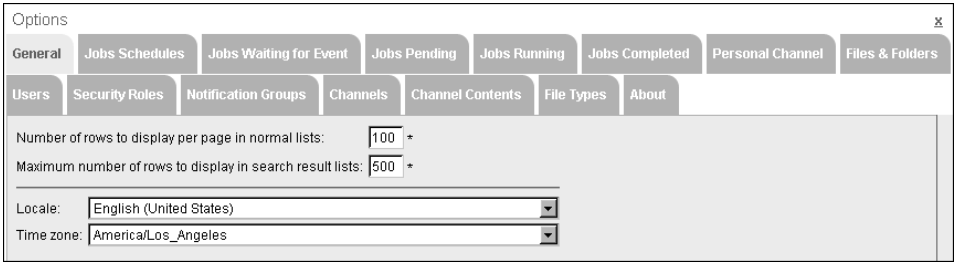

Figure 1-18 Modifying settings in Options—General

Options—About contains the following general information about the iServer installation, as shown in Figure 1-19:

- Actuate Management Console version
- Actuate iServer System name
- Volume name
- Actuate iServer System version
- License category
- User name
- Current language
- Current time zone
- Copyright

Filtering Encyclopedia volume data

Management Console provides filters that can reduce the number of rows displayed in a tabular list. Filtering is done by specifying the object name, or the predefined categories available for a particular option. For example, the Users filter supports filtering by user name and a predefined category specifying whether Login disabled is set to Yes or No.

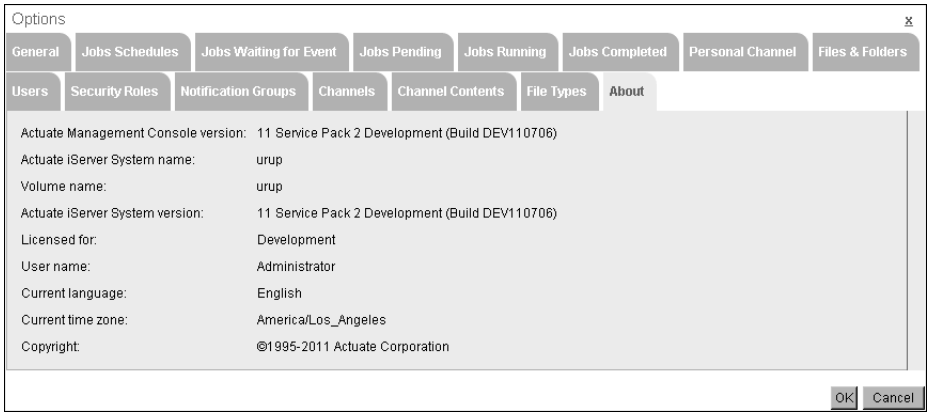

Figure 1-19 Viewing installation information in Options—About

The following menu options contain a filter:

- Jobs
- Files and folders
- Users
- Security roles
- Notification groups
- Channels

How to filter by name

This procedure uses the example of an administrator who wants to limit the user list to those users whose names start with the letter A. On Users, type A* in Filter. The asterisk (*) is a wildcard that means zero or more characters, excluding spaces and punctuation. To run the filter, choose Apply. Figure 1-20 shows the results.

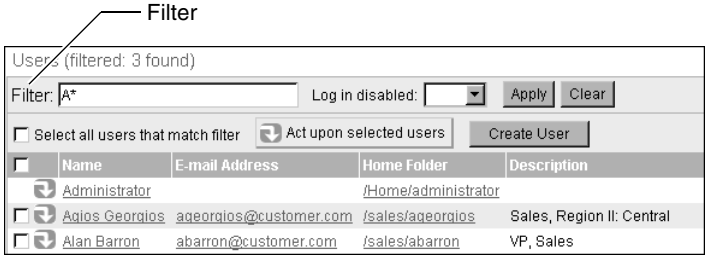

Figure 1-20 Filtering for “A”

How to use special characters in searches

If a search expression contains one or more special characters, a backslash (\) must precede each special character.

The following special characters are also operators in search expressions:

- Ampersand (&)
- Asterisk (*)
- Backslash (\)
- Close square bracket (])
- Comma (,)
- Equal sign (=)
- Exclamation point (!)
- Greater than sign (>)
- Hyphen (-)
- Less than sign (<)
- Number sign (#)
- Open square bracket ([)
- Pipe sign (|)
- Question mark (?)
- Single quotation mark (‘)

For example, to search for the user name user#, you must type the following search expression:

```
user\#
```

If you type user#, the search returns user names that begin with user and end with a number, such as user1, user2, and so on.

How to filter using a predefined option

The Log in disabled drop-down list enables you to filter user lists to those whose login accounts are either enabled or disabled.

To display only users whose logins are not disabled, select No for Log in disabled. Selecting Yes filters for disabled logins, as shown in Figure 1-21.

Figure 1-21 Filtering for disabled login accounts

To run the filter, choose Apply.

To clear a filter and retrieve all rows or items, choose Clear.

Performing a search

Search filters Encyclopedia volume data based on a broad range of criteria. For example, a search on user data supports using criteria such as name, e-mail address, home folder, licensed option, maximum job priority, or job notification.

Search also supports selecting the columns that appear in a tabular list. Search results appear sorted in ascending order by name.

How to search

To specify a search, perform the following tasks:

1 Choose the menu option on which you want to search, such as Users. The tabular list of users appears, as shown in Figure 1-22.

Figure 1-22 Searching for users meeting a specific criteria

2 Choose Search. Search—Criteria appears.

3 Specify the search criteria. For example, search for users who meet the following criteria, as shown in Figure 1-23:

- E-mail address ends with @customer.com.
- Maximum job priority is greater than 500.
- Preference is to receive e-mail notification for jobs that fail.
- Channel subscriptions include the Sales channel.

4 Choose Columns. On Search—Columns, specify the columns to display in the search results by performing the following tasks.

The example shows how to display the following columns from left to right:

- Name
- Priority
- E-mail Notification
- Completion Notices

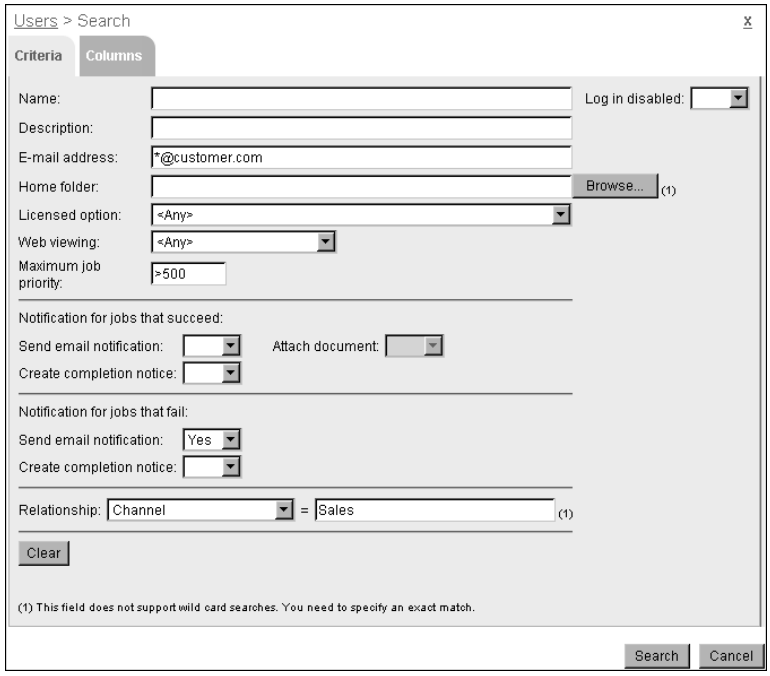

Figure 1-23 Users—Search—Criteria

1 Move the following fields from Selected columns to Available columns, using the left arrow:

- E-mail Address
- Home Folder
- Description

2 Move the following fields from Available columns to Selected columns, using the right arrow:

- Completion Notices
- E-mail Notification
- Priority

3 To change the order in Selected columns, perform the following tasks:

1 Select Priority. Choose the up arrow twice to move Priority to the position below Name.

2 Select Completion Notices. Choose the down arrow once to move Completion Notices below E-mail Notification.

Figure 1-24 shows Search—Columns.

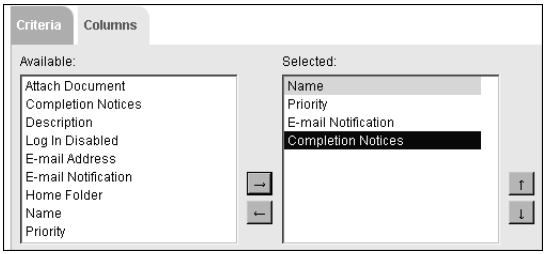

Figure 1-24 Users—Search—Columns

5 To generate the results, choose Search. Figure 1-25 shows the search results.

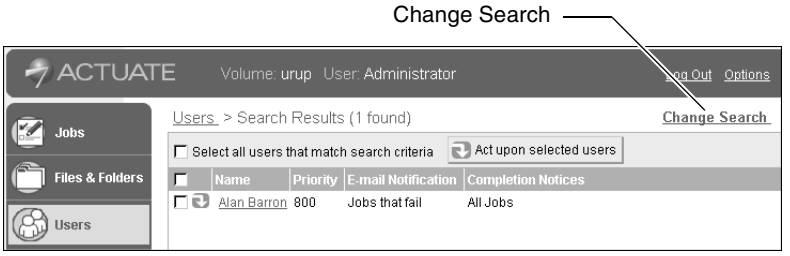

Figure 1-25 Users—Search Results

To modify the criteria or column list, choose Change Search.

Chapter

2

Managing users

This chapter contains the following topics:

- About user accounts
- Creating a user account
- Modifying user properties
- Cloning a user
- Deleting a user

About user accounts

The administrator creates, configures, and manages user accounts. Administrator tasks include assigning and updating privileges, creating and managing membership in security roles, and providing access to channels. During installation, the installer configures the Administrator user account.

User privileges control access to the Encyclopedia volume and its items. Security roles are groups of users who share the same privileges. A channel is a service that provides a subscribing user access to particular types of documents.

A user accesses an Encyclopedia volume by using a unique login name and password. The administrator has full access to the volume and can change any user password. A user can change only his or her password.

In Management Console, the administrator chooses Users to view and configure user properties, as shown in Figure 2-1.

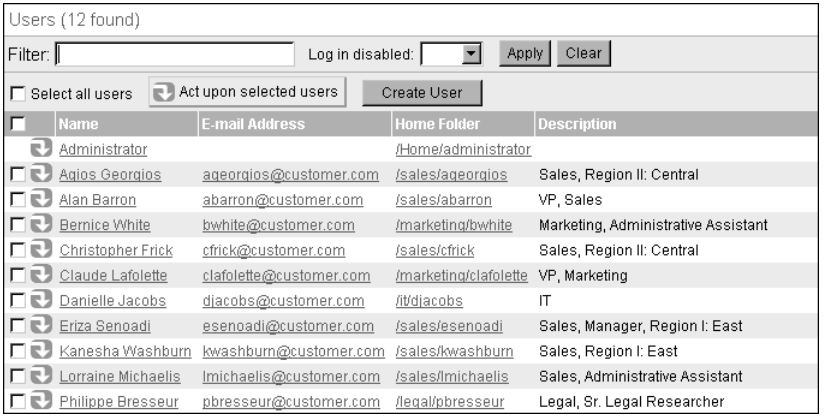

Figure 2-1 Viewing Users

In Users, the administrator performs the following tasks:

- Create a new user account.
- Update an existing user account.
- Subscribe a user to a channel.
- Clone a user.
- Delete a user.
- View, filter, or search the list of current user accounts.

The following sections describe how to perform these tasks.

Creating a user account

In Management Console, creating a user account involves specifying the following properties:

- General
  User name, description, password, e-mail address, home folder, and whether the login is disabled.
- Jobs
  Maximum job priority and notification options for jobs that succeed and fail.
- Roles
  Security roles from the available list, such as Administrator and Operator.
- Groups
  Notification groups from the available list defined by the administrator.
- Privilege Template
  Users and roles from the available list, to which the administrator assigns privileges, such as visible, execute, grant, read, secure read, write, and delete, on items a selected user creates.
- Printing
  Printer and settings, including scale, resolution, mode, number of copies, duplex or simplex, horizontal or vertical, page size, and paper tray.
- Licensed Option
  Licensed options from the available list that a user can access, such as BIRT Spreadsheet or BIRT option.

You can control the priority that iServer gives to running a user's designs. When you create a user account, you specify the maximum priority that the user can assign to running a design. Settings include:

- Low (200)
- Medium (500)
- High (800)
- Other (1–1000)

If you choose Other, a text field opens in which you can type a specific number.

If Actuate Open Security is enabled, and the user's maximum job priority is defined in an external security source, a Management Console setting cannot change the external setting.

How to create a user account

The following steps create a user account for a newly hired sales manager, Eriza Senoadi:

1. On Users, choose Create User.
2. On New User—General, shown in Figure 2-2, complete the following tasks:
   - Type a user name, description, and password for this user. Confirm the password.

     User names and passwords are strings of 1 to 50 characters.
     - Name is a required field. A user name can include any character except a control character. The user name is not case-sensitive. The Encyclopedia volume stores the user name in mixed case and displays the name exactly as you typed it during creation.
     - The description and password are not required. If you use a password, security experts recommend a password containing at least eight characters, including numeric and mixed-case alphabetic characters. A password is case-sensitive and cannot include a control character or space.
   - Type the user's e-mail address. iServer uses this address for e-mail notification of jobs that succeed and fail.
   - Optionally, specify a path and folder name as the home folder. If you use a home folder name that does not exist, iServer creates the folder, and any folders in the path that do not exist. iServer assigns visible privilege to the user on the new folders in the path and assigns visible, read, and write privileges to the user on the home folder.

     If the home folder is on a pre-existing path, the user must have visible privilege on all folders in the path. For example, on a volume named widgetco, if the home folder location is /widgetco/sales/esenoadi, the user, esenoadi, must have visible privilege on each of the following folders:
     - /widgetco
     - /sales

     If the Encyclopedia volume uses an Open Security RSSE application, you must assign privileges to the user home folder manually. The user home folder privileges are not automatically updated.
   - To prevent the user from logging in, such as when you create a user account before the user begins work at the company, select Log in disabled, as shown in Figure 2-2.

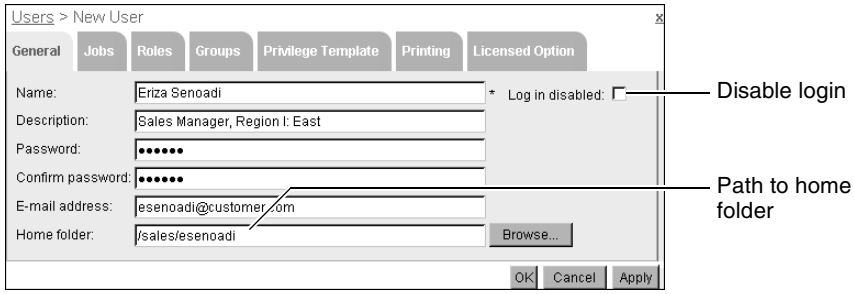

Figure 2-2 Making selections on New User—General

Choose Jobs.

3 On Jobs, shown in Figure 2-3, specify job-related preferences, such as how iServer notifies the user when a job succeeds or fails.

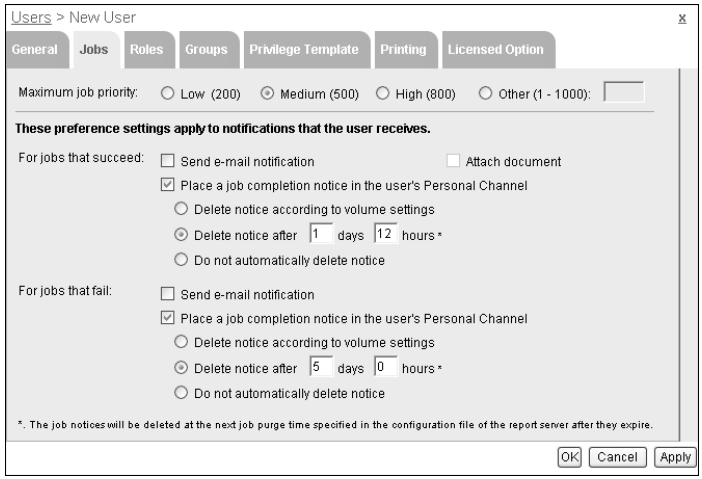

Figure 2-3 Making selections on New User—Jobs

Specify job-related preferences as follows:

- Maximum job priority

  Specify the maximum job priority level the user can assign to a job, from 1–1000.

- Send e-mail notification

  iServer notifies the user by e-mail when a job completes. The e-mail notification contains a hyperlink to the document.

- Attach document

  iServer sends the document as an attachment to the e-mail notification. The user must have read privilege on the document. If the user does not have

read privilege, only the hyperlink to the document appears in the e-mail notification.

- Place a job completion notice in the user's Personal Channel
  iServer sends a notice to that channel. Selecting Place a job completion notice in the user's Personal Channel enables the following options:
  - Delete notice according to volume settings
    iServer purges job notices from the volume after the number of days and hours that Default user notice purging setting for this volume specifies in Volume—Properties—Archiving and Purging. The default time for purging notices is 2:15 A.M. On Configuration Console Advanced view, in Volumes—General, Schedule for purging notices specifies the time to purge job notices.
  - Delete notice after n days n hours, where n is a number you specify
    iServer does not delete job notices until after the specified number of days and hours expires.
  - Do not automatically delete notice
    iServer does not delete this user's job notices.

Choose Roles.

4 On Roles, assign membership in one or more security roles. To assign a user to a security role, select the role in Available and move the role to Selected. For example, assign a new user to the Sales role by selecting the Sales role in Available and moving the Sales role to Selected, as shown in Figure 2-4.

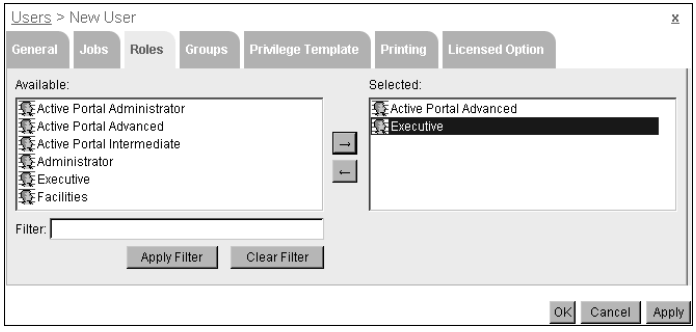

Figure 2-4 Assigning a user to a security role in New User—Roles

Choose Groups.

5 On Groups, assign a new user to one or more notification groups. To assign a user to a group, select the group in Available and move the group to Selected. For example, to assign the new user to the Managerial Staff and Sales Staff groups, in Available, select Managerial Staff and move it to Selected, then repeat the action for the Sales Staff group, as shown in Figure 2-5.

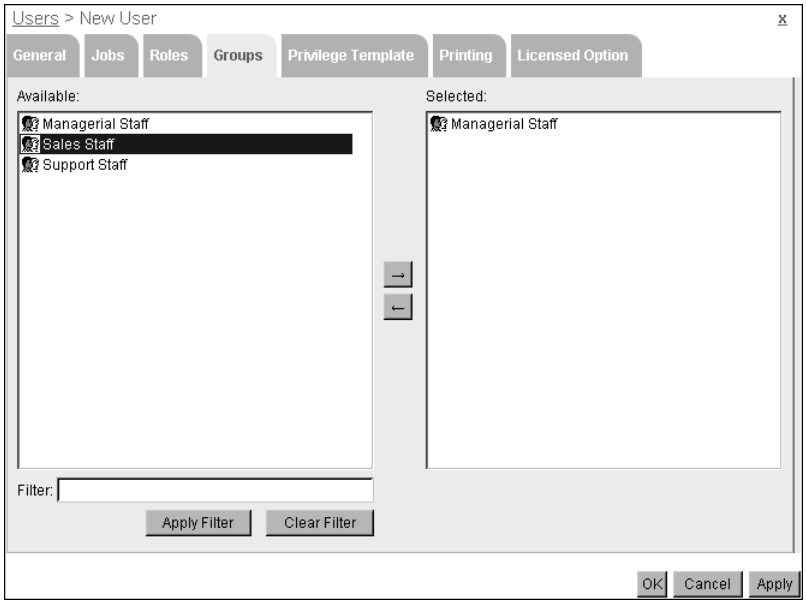

Figure 2-5 Assigning a user to a notification group in New User—Groups

Choose Privilege Template.

6 On Privilege Template, assign privileges to other users and security roles for access to items that the new user creates by performing the following steps:

1. Move security roles from Available to Selected.
2. Assign privileges, such as Visible, Read, or Write

   For example, select Roles. Use Filter to display security roles that include the word Manager. Move the following roles from Available to Selected:

   - Accounting Managers
   - Marketing Managers
   - Operations Manager
   - Sales Managers

   Assign visible and secure read privileges to the Accounting, Marketing, and Operations Managers roles. Assign visible, read, and write privileges to the Sales Managers role, as shown in Figure 2-6.

   The privileges you assign to the roles in Selected apply to items that the new user creates.

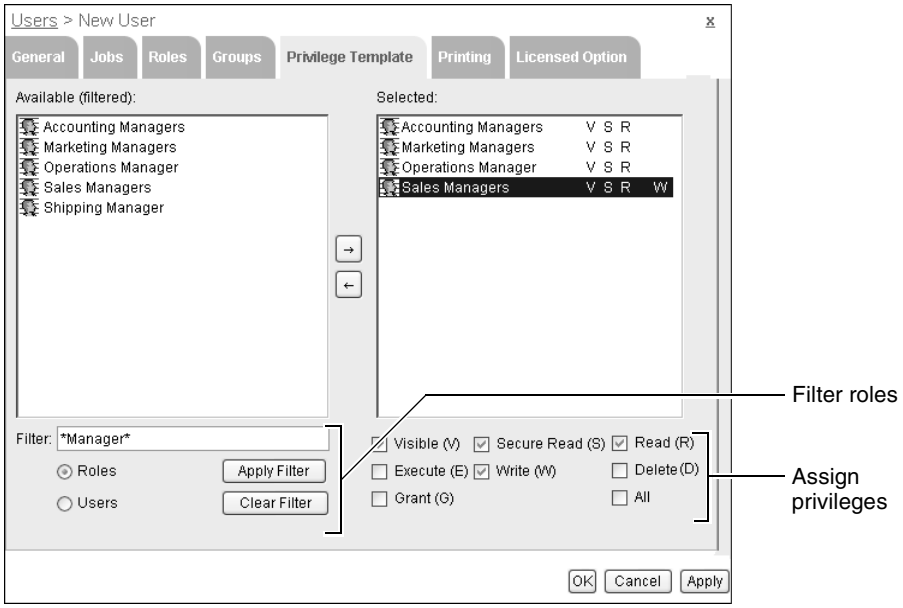

Figure 2-6 Assigning privileges on New User—Privilege Template

Choose Printing.

7 On New User—Printing, you can specify a default printer and other printer settings for the new user. These preferences override volume-level settings. For example, in Figure 2-7, you specify the printer called Freedom as the new user's default printer. You also make selections for the following options:

- Scale
- Resolution
- Printer mode, meaning black-and-white or color
- Default number of copies
- Duplex versus simplex printing
- Page size
- Paper tray

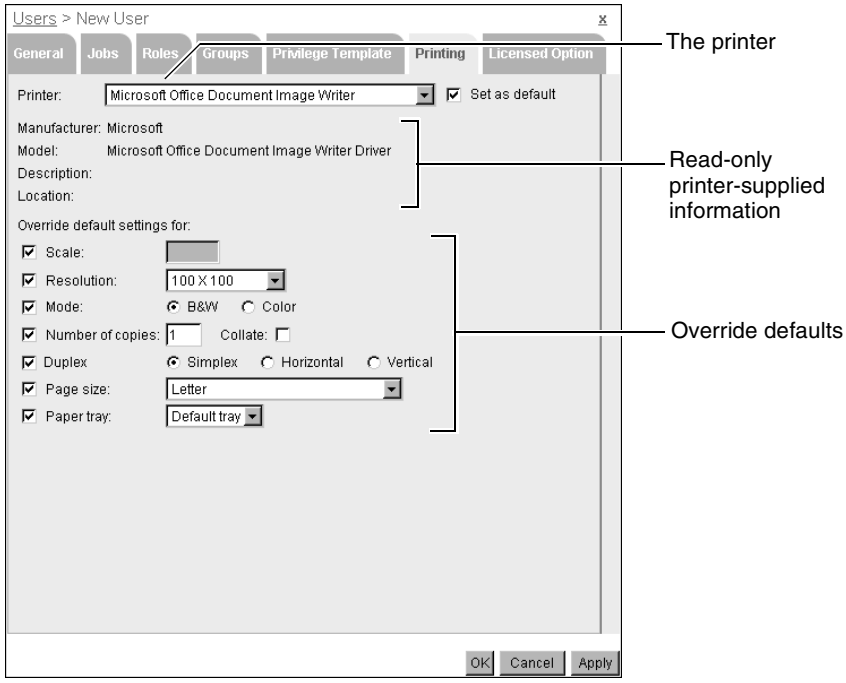

Figure 2-7 Selecting printing options on New User—Printing

Choose Licensed Option.

8 On Licensed Option, assign and remove licensed options available to a user by performing the following tasks:

- Assign licensed options by moving one or more options from Available to Selected.
- Remove licensed options by moving one or more options from Selected to Available.

The licensed options table shows the number of purchased options and the number of options assigned to users on the volume. Choosing Apply or OK updates # Assigned to this Volume and creates the user, as shown in Figure 2-8.

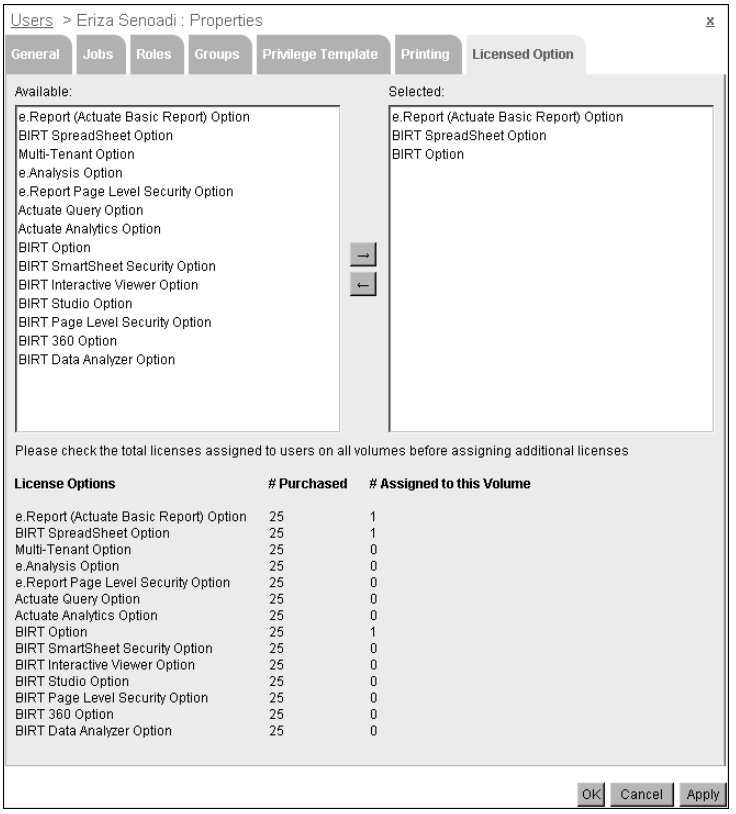

Figure 2-8 Assigning license options on New User—Licensed Option

Modifying user properties

You can modify user properties for one account or many. This section describes how to perform the following tasks for a single user:

- Modify user properties.
- Subscribe a user to one or more channels.

How to modify a user's properties

1 On Users, point to the arrow next to the user name, and choose Properties, as shown in Figure 2-9.

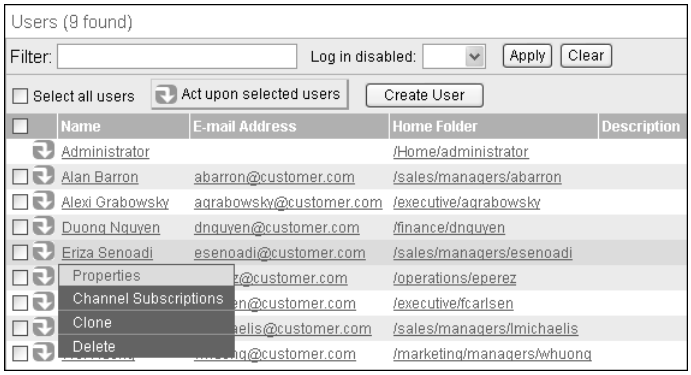

Figure 2-9 Accessing Users—Properties

2 Users—Properties displays the same properties as Users—New User, as shown in Figure 2-10:

- General
- Jobs
- Roles
- Groups
- Privilege Template
- Printing
- Licensed Option

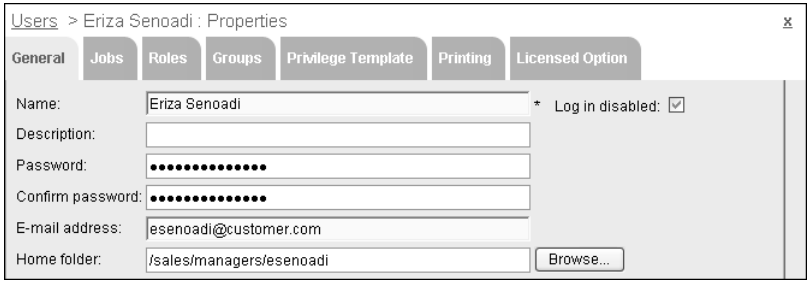

Figure 2-10 Viewing Users—Properties

Modifying existing user properties involves the same tasks as specifying new user properties.

How to subscribe a user to a channel

When the administrator creates a new user, iServer automatically subscribes the user to a personal channel. After creating the user, the administrator can subscribe the user to additional channels.

1 On Users, point to the arrow next to the user name, and choose Channel Subscriptions, as shown in Figure 2-11.

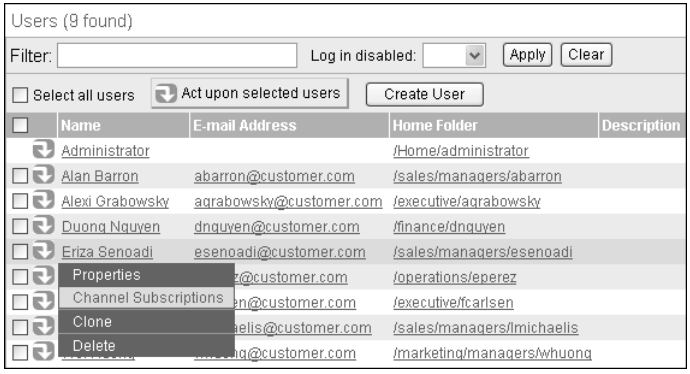

Figure 2-11 Accessing Users—Channel Subscriptions

2 On Users—Channel Subscriptions, move a channel from Available to Selected to assign a user to that channel. A channel appears in Available only if the Administrator has given the user read access to the channel, either as a user or as a member of a security role. A user can also have write privilege on a channel.

For example, to subscribe the user, Eriza Senoadi, to the Managers and Sales channels, select the Managers channel in Available and move it to Selected, then repeat the action for the Sales channel. Figure 2-12 shows the results of these actions.

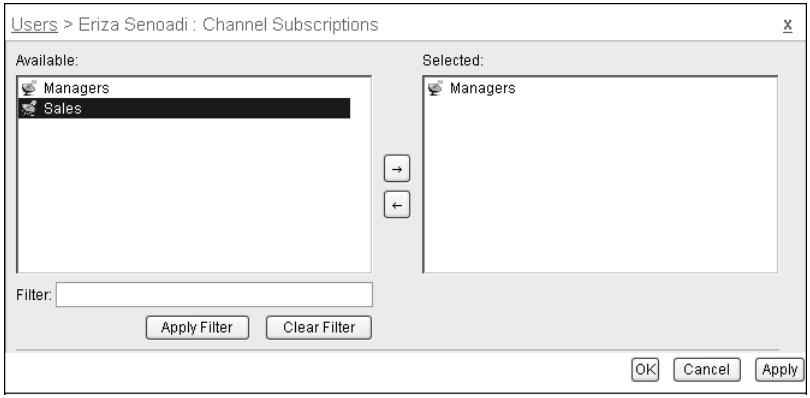

Figure 2-12 Subscribing a user to a channel

Choose OK.

Modifying user properties for multiple accounts

Use Act upon selected users to change the property settings for multiple users in one step.

How to modify properties for multiple users

1 On Users, select the individual users whose properties you want to modify. Figure 2-13 shows two user names selected.

Alternatively, to select all users on the page, select the box next to Name. To select all the users in the Encyclopedia volume, select

Select all users

Point to Act upon selected users.

Choose Properties, as shown in Figure 2-13.

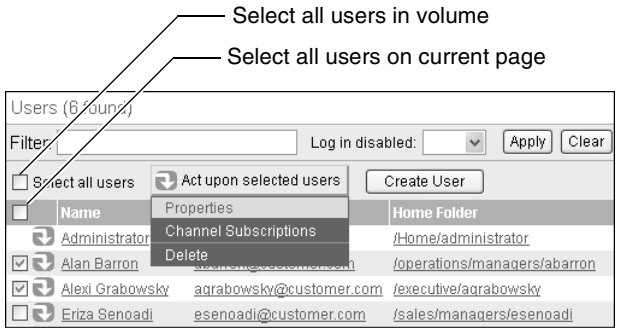

Figure 2-13 Select the properties for multiple users

2 On Users—Properties, make the following changes:

- On General, enable or disable the user logins and change the description and home folder. Figure 2-14 shows general properties for multiple users.

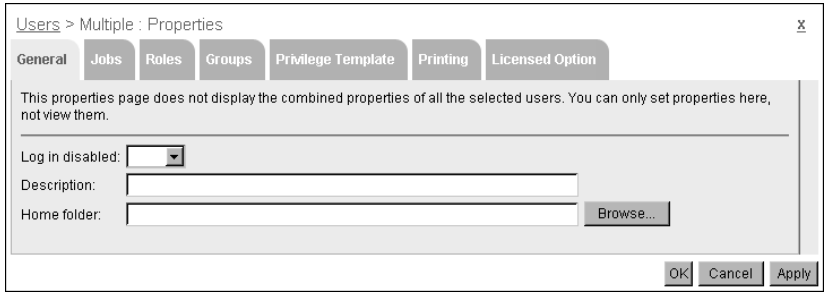

Figure 2-14 Modifying General properties for multiple users

- On Jobs, set the maximum job priority for users and set notification preferences for jobs that succeed or fail.

  Figure 2-15 shows Jobs.

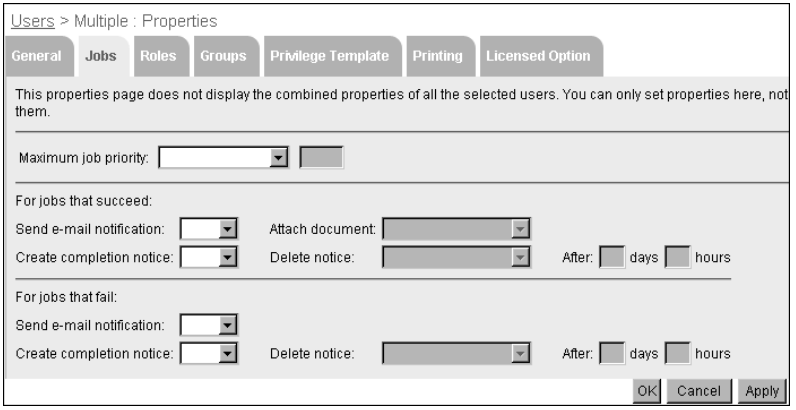

Figure 2-15 Modifying Job properties for multiple users

- On Roles, make modifications to role assignments by moving the security roles in Available either to Remove these roles or Add these roles. Select Remove all to remove all roles from the selected users. Figure 2-16 shows Roles.

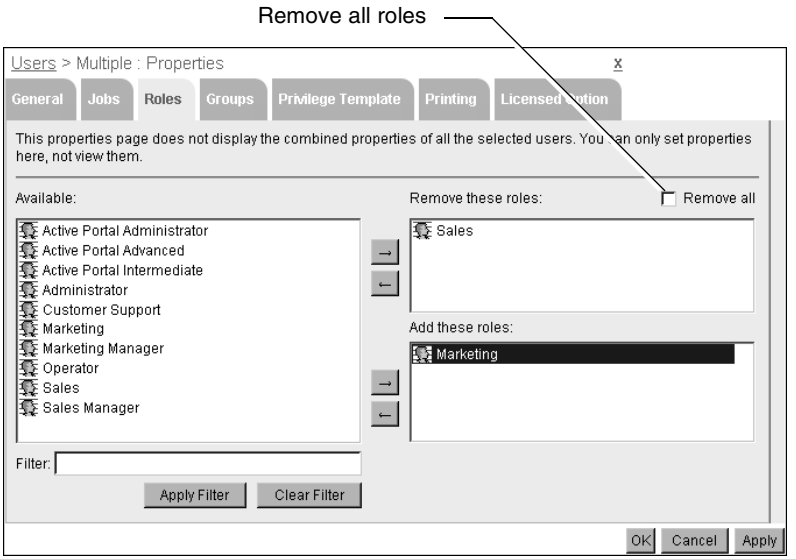

Figure 2-16 Modifying Role properties for multiple users

- On Groups, move the notification groups from Available to Remove these groups or Add these groups. Select Remove all to remove all groups from the selected users. Figure 2-17 shows Groups.

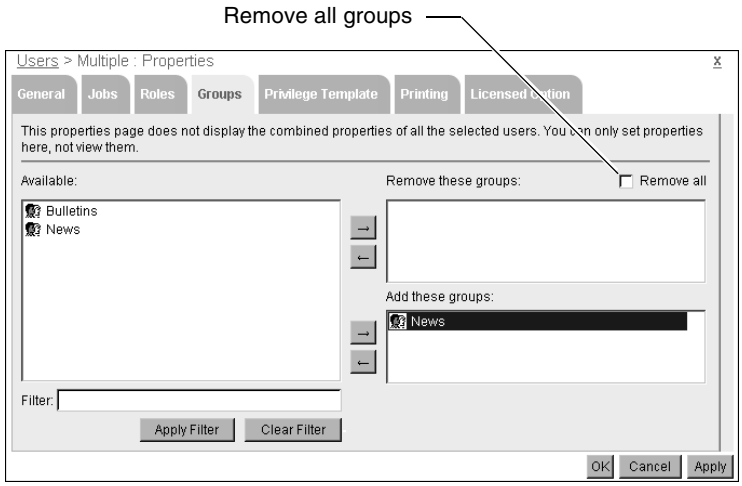

Figure 2-17 Modifying Groups properties for multiple users

- On Privilege Template, move Roles or Users from Available to Remove these privileges or Add these privileges. With a role or user selected in Remove these privileges, deselect privileges you want the role or user to keep. Select Remove all to remove all privileges any role or user has on items the selected users create. With a role or user selected in add these privileges, assign privileges by selecting from the list of privileges. Figure 2-18 shows Privilege Template.

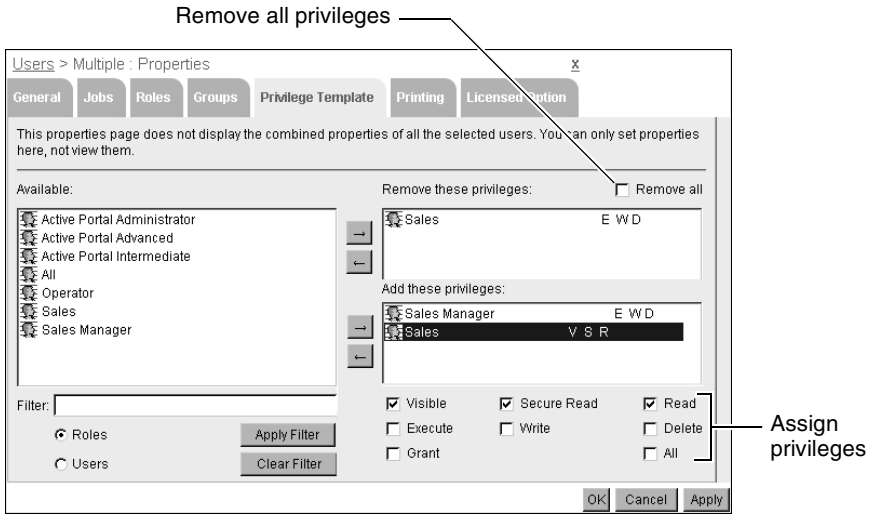

Figure 2-18 Modifying Privilege Template properties for multiple users

- On Printing, specify the printer you send the document to, and choose whether it is the default printer. Use default printer settings specified by the selected users or selectively override individual printer settings. Figure 2-19 shows Printing properties.

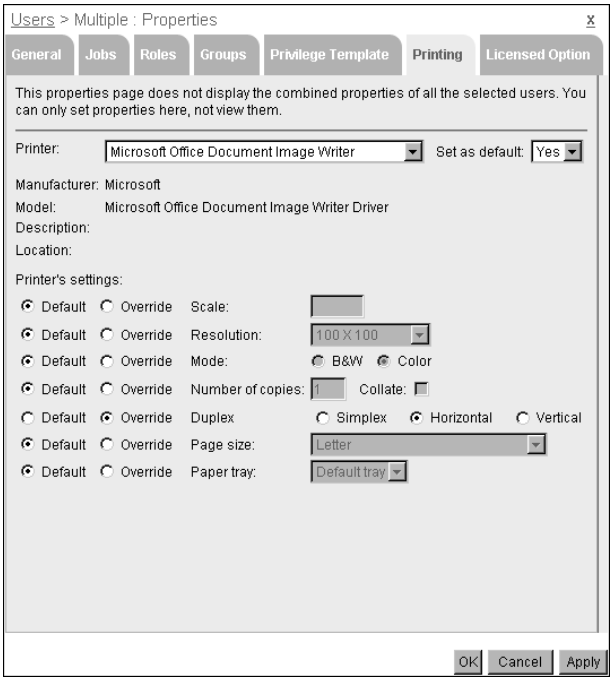

Figure 2-19 Modifying Printing properties for multiple users

- On Licensed Option, shown in Figure 2-20, assign and remove the licensed options that selected users can access by performing the following actions:
  - Remove licensed options by moving one or more options from Available to Remove these licensed options. Remove all removes the licensed options from the selected users.
  - Assign licensed options by moving one or more options from Available to Add these licensed options.

  Licensed Options lists each licensed option, showing # Purchased and # Assigned to this Volume. Figure 2-20 shows Licensed Option.

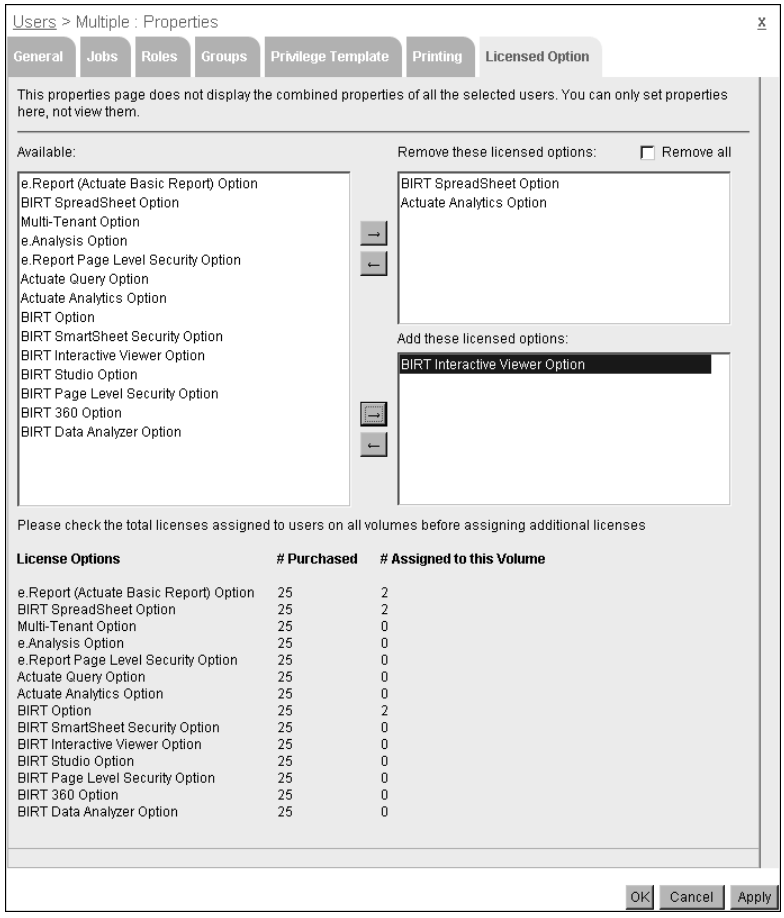

Figure 2-20 Adding and removing licensed options for multiple users

Choosing Apply or OK updates the # Assigned to this Volume value for an option you select.

Choose OK. Management Console returns to Users.

How to modify channel subscriptions for multiple users

1 On Users, select the users whose channel subscriptions you want to modify. Alternatively, to select all users on the current page, select the box next to Name. To select all the users in the Encyclopedia volume, select Select all users.

Point to Act upon selected users, and choose Channel Subscriptions.

2 On Channel Subscriptions, move a channel in Available to Remove these subscriptions or Add these subscriptions. A channel appears in Available only

if the Administrator has given at least one selected user read access to the channel, either as a user or as a member of a security role.

Select Remove all to remove all channel subscriptions from the selected users. Figure 2-21 shows Channel Subscriptions.

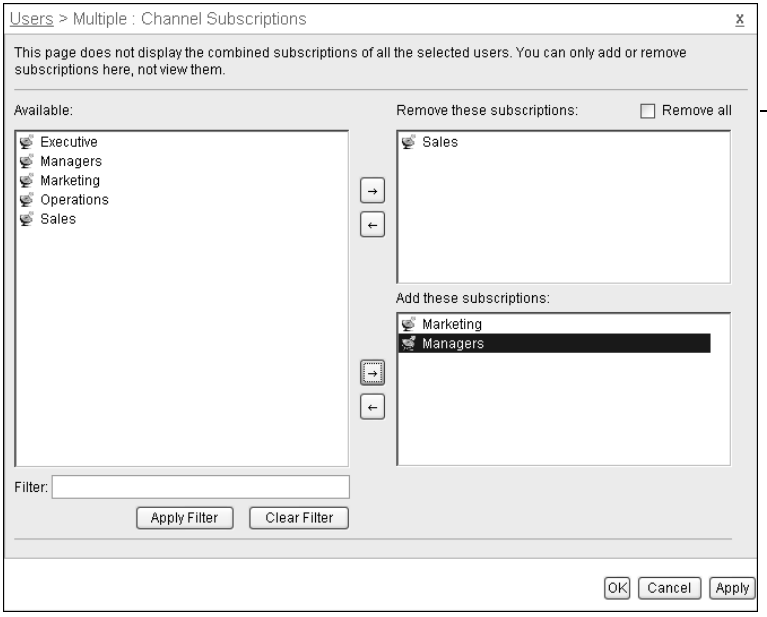

Figure 2-21 Modifying channel subscriptions for multiple users

3 Confirm that all users have read access to the channels to which you subscribe them, either directly or through a security role.

Cloning a user

Cloning creates a copy of a user, enabling the administrator to use the properties of an existing user as a basis for a new user.

How to clone a user account

1 On Users, point to the arrow next to the user name.

Choose Clone, as shown in Figure 2-22.

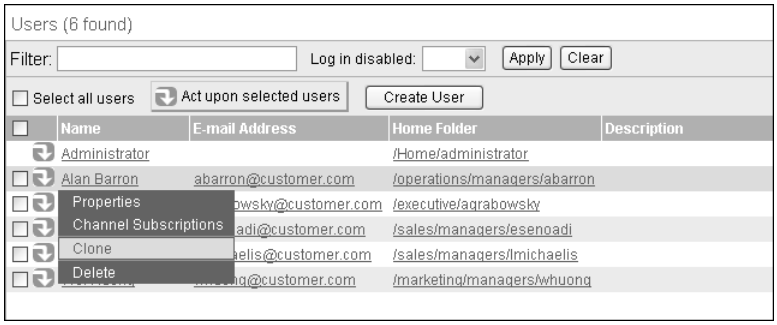

Figure 2-22 Choosing to clone a user

Figure 2-23 shows the properties of the cloned user, Alan Barron, in Users—New User.

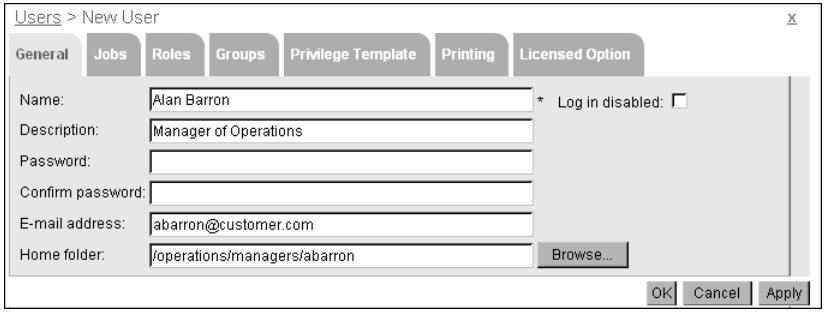

Figure 2-23 Creating a new user account with properties of a cloned user

2 On New User—General, change the cloned user's name and password. Modify any other properties as needed, then choose OK.

Deleting a user

When the administrator deletes a user account, the administrator becomes the owner of any files or folders that the user owned. iServer does not delete any files or folders from the Encyclopedia volume.

How to delete a user account

On Users, point to the arrow next to the user's name, and choose Delete, as shown in Figure 2-24.

Figure 2-24 Deleting a user account

When the confirmation prompt appears, choose OK.

How to delete multiple user accounts

On Users, select the names of the users you want to delete. Alternatively, to select all users on the current page, select the box next to Name. To select all the users in the Encyclopedia volume, select Select all users.

Point to Act upon selected users, and choose Delete, as shown in Figure 2-25.

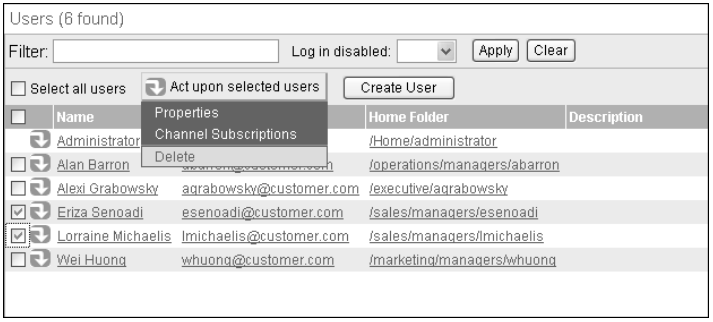

Figure 2-25 Deleting multiple users

Confirm the deletion.

Chapter

3

Working with security roles

This chapter contains the following topics:

- About security roles
- Managing security roles

About security roles

Security roles simplify privilege assignment and maintenance. A single security role can specify privileges for accessing many items. The administrator creates a security role to configure a set of privileges common to a group of users, then assigns the users to the role.

The administrator can:

- Create a security role.
- Assign privileges on files, folders, and channels to a security role.
- Modify security roles.
- Access the list of users belonging to a security role.

In Figure 3-1, Sales has read and execute privileges on the Sales Invoice design. Marketing cannot run the design. Sales and Marketing both can read the document that the Sales Invoice design creates.

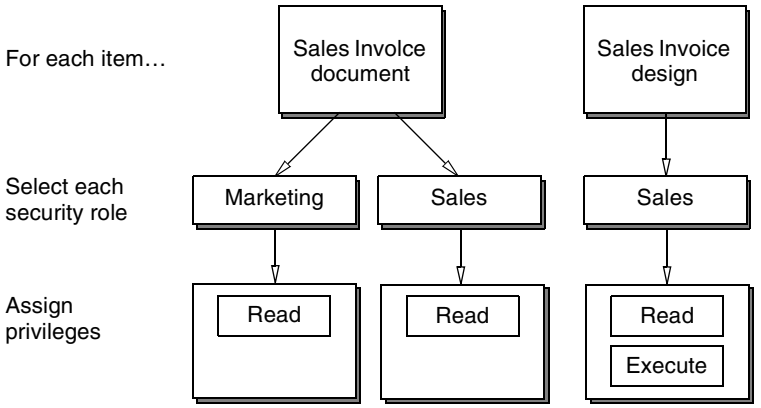

Figure 3-1 Assigning privileges to security roles

About hierarchical security roles

A user can belong to more than one security role. Security roles can also belong to other security roles and form a hierarchy. If you add a security role to another, the role you add becomes a parent or a child role. A role inherits privileges from a parent, and passes privileges to a child.

To remove an inherited privilege, the administrator must remove the privilege from every parent role that has the privilege.

iServer does not support using nested roles with pass-through security.

Figure 3-2 shows three security roles. The Sales role is the parent role of Sales-Lead, and Sales-Lead is the parent role of Mgr-Sales. Sales-Lead inherits privileges from Sales. Mgr-Sales inherits privileges from both Sales-Lead and Sales.

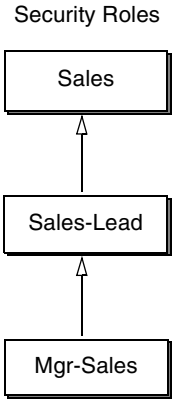

Figure 3-2 Viewing a security roles hierarchy

Table 3-1 shows the privileges that Sales and Mgr-Sales have on a folder, /Public /Sales, and on a design file, /Public/Sales/Sales Invoice.

Table 3-1 Privileges for roles on a folder and a file

Security Role	Public/Sales	Public/Sales/Sales Invoice
Sales	Read	Read
Mgr-Sales	Write	Execute

As an example, Pamela Castillo belongs to the Mgr-Sales role. To execute Sales Invoice, Pamela Castillo requires read and execute privileges on Sales Invoice. Pamela Castillo also requires write privilege, and either visible, secure read, or read privilege on /Public/Sales, the folder containing Sales Invoice.

As a member of the Mgr-Sales role, Pamela Castillo has write privilege on /Public/Sales, and execute privilege on /Public/Sales/Sales Invoice. Pamela Castillo inherits read privilege on /Public/Sales and read privilege on Sales Invoice from the Sales role.

About system-defined security roles

iServer defines the following security roles, which the administrator cannot delete or rename:

- Administrator
  Has full access to the Encyclopedia volume and all files and folders on the volume.

- All
  Supports the administrator assigning privileges to all users in the Encyclopedia volume.
- Operator
  Performs operations such as backing up and archiving the Encyclopedia volume.

About Information Console functionality levels

Actuate Information Console supports users running designs, and viewing and interacting with documents from a web browser.

Information Console provides functionality levels that control the features available to a user. The Information Console administrator can customize these levels in the Information Console configuration files. These functionality levels map to the following security roles in Management Console:

- Active Portal Administrator
  Includes all privileges of the Active Portal Advanced role, and also allows users to clone and customize Information Console skins.
- Active Portal Advanced
  Includes all privileges of the Active Portal Intermediate role, and also allows users to perform tasks such as creating and deleting folders.
- Active Portal Intermediate
  Includes the privileges assigned to the All role, and also allows users to perform tasks such as searching documents and subscribing to channels.

Table 3-2 shows which tasks each role can execute by default.

Table 3-2 Information Console tasks and roles

Information Console tasks	Intermediate	Advanced	Administrator
Customize skins.			X
Create a folder.		X	X
Delete a folder.		X	X
Search for files and folders.	X	X	X
Send e-mail notification with attachments to oneself.	X	X	X
Share and set privileges on a file or folder.		X	X
Subscribe to a channel.	X	X	X

Managing security roles

When creating a security role, the administrator specifies the following properties:

- Security role names and descriptions
- Parent and child roles
- Channel privileges
- User membership

When using Management Console to administer security roles, the administrator performs the following tasks:

- View the list of security roles.
- Create new security roles.
- View or modify properties for one or more security roles.
- View a list of users assigned to one or more security roles.
- Add and remove users from one or more security roles.
- Clone a security role.
- Delete one or more security roles.

How to manage a security role

1 In Management Console, choose Security Roles from the side menu.

The list of security roles appears, as shown in Figure 3-3.

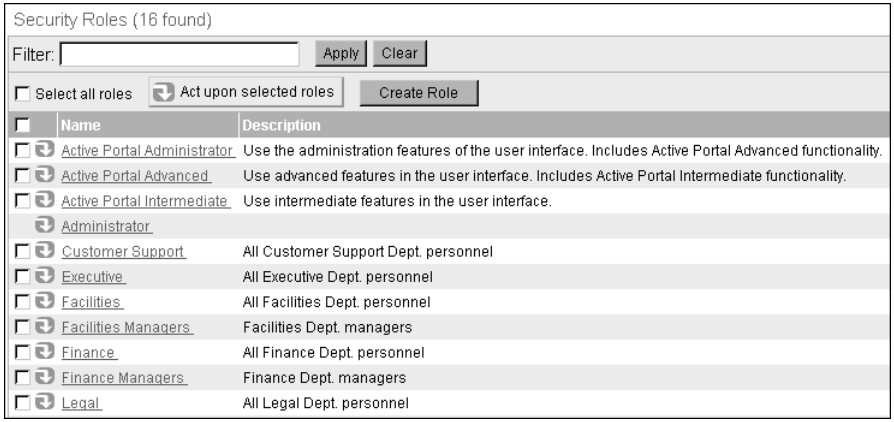

Figure 3-3 Viewing the security roles list

To access the properties of a security role, point to the arrow next to the name of an existing role and choose Properties, as shown in Figure 3-4.

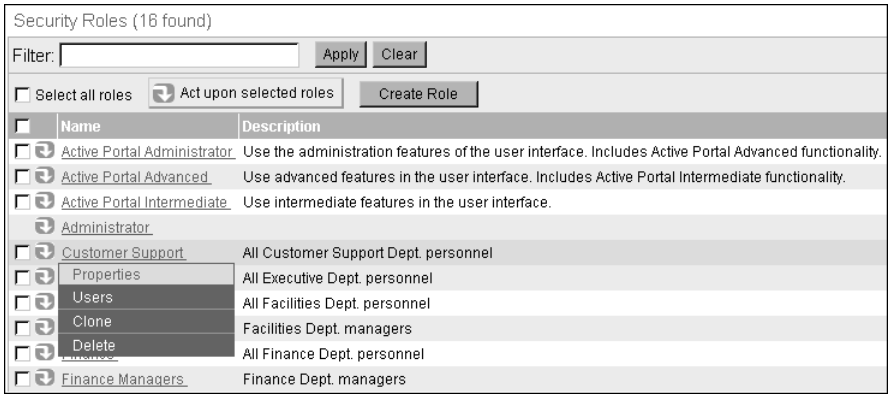

Figure 3-4 Accessing a security role's properties

Alternatively, to create a new security role, choose Create Role.

2 On New Security Role—General, type the name of the security role and a description, as shown in Figure 3-5.

Figure 3-5 Specifying a name and description for a new security role

Choose Parent Roles.

3 On Parent Roles, in Available, select one or more roles from which you want this role to inherit privileges, then move the role or roles to Selected by choosing the right arrow, as shown in Figure 3-6.

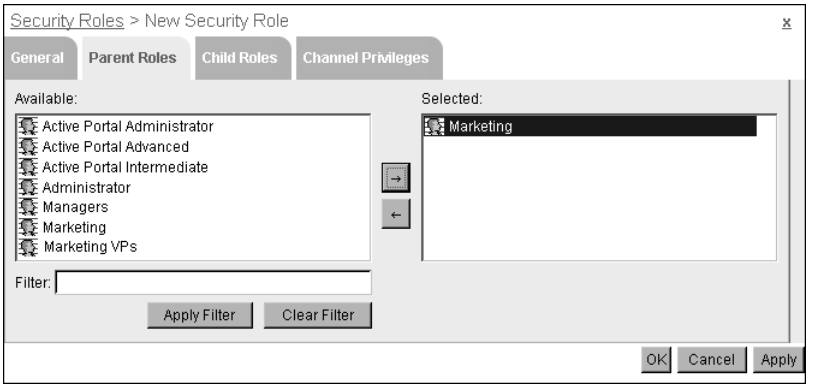

Figure 3-6 Specifying one or more parent roles

Choose Child Roles.

4 On Child Roles, in Available, select one or more roles for which you want privileges inherited from this role, then move the role or roles to Selected by choosing the right arrow, as shown in Figure 3-7.

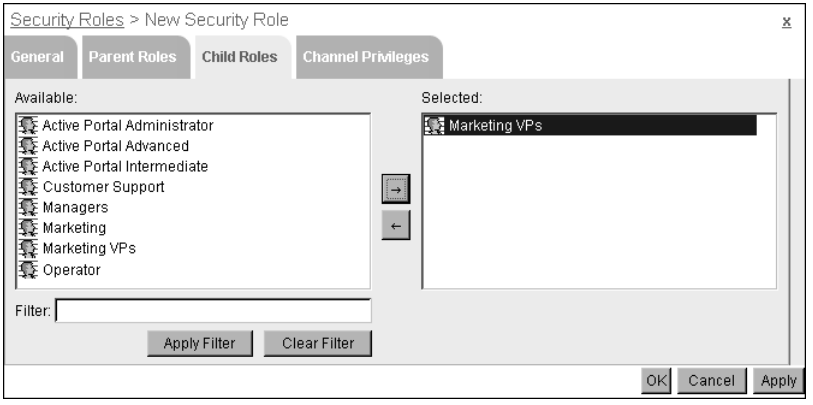

Figure 3-7 Specifying one or more child roles

Choose Channel Privileges.

5 On Channel Privileges, assign channel privileges to this role by moving channels from Available to Selected, then selecting Read, Write, or both privileges, as shown in Figure 3-8.

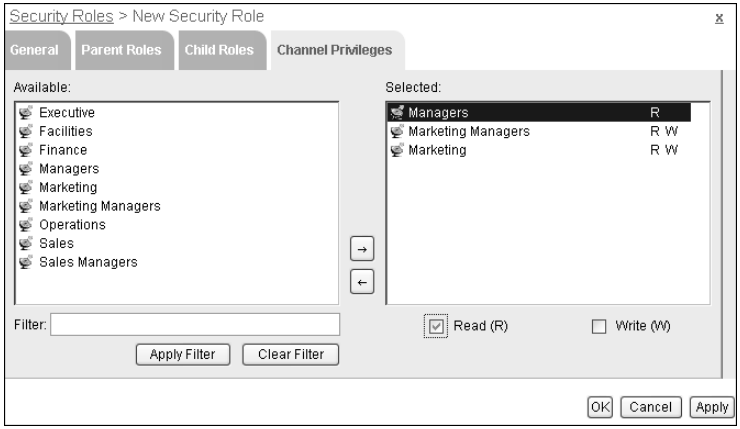

Figure 3-8 Assigning privileges on channels to a security role

Choose OK.

To modify the properties of an existing security role, choose General, Parent Roles, Child Roles, or Channel Privileges, and modify these properties similar to the way in which you specify properties for a new user.

How to add and remove a user from a security role

1 On Security Roles, point to the arrow next to the security role name, and choose Users, as shown in Figure 3-9.

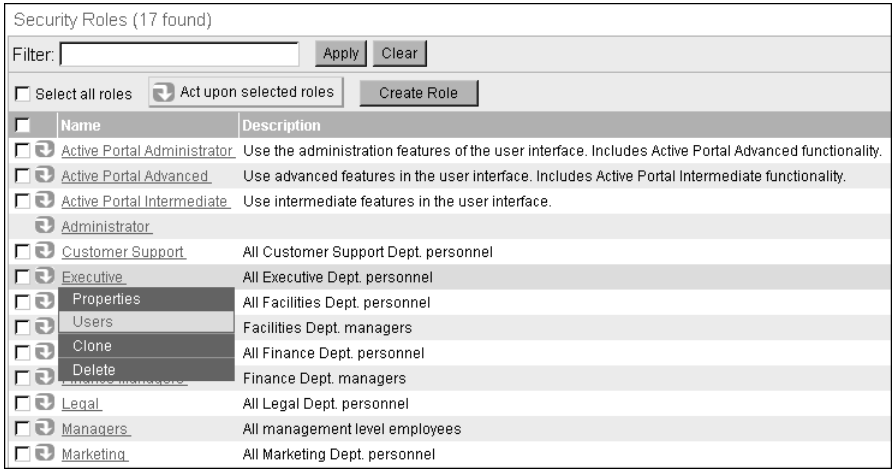

Figure 3-9 Choosing to view a security role membership list

2 On Security Roles—Users, as shown in Figure 3-10, perform the following tasks:

- To add users:
  Choose Add. On Users—Add, perform the following tasks:
  1. Move the user or users you want to add from Available to Add.
  2. Choose OK.
- To remove users:
  1. Select the user or users you want to remove.
  2. Choose Remove.
  3. Confirm the deletion.

Figure 3-10 Adding and removing security role members

Choose Close.

How to clone a security role

You can create a new security role by cloning an existing role. Cloning creates a copy of the role, enabling you to use the properties of an existing role as the basis for a new role.

1. On Security Roles, point to the arrow next to the security role name, and choose Clone, as shown in Figure 3-11.

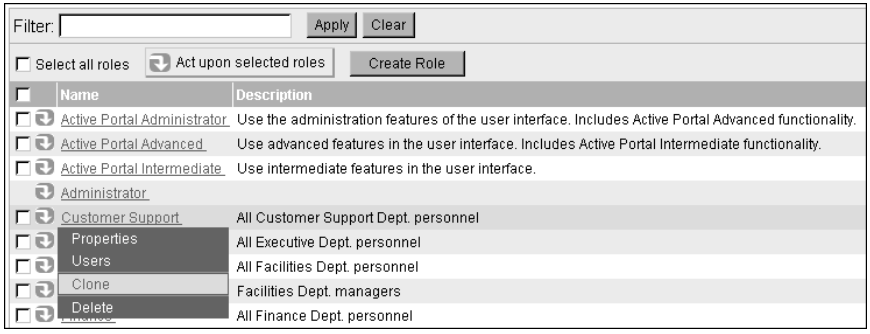

Figure 3-11 Choosing to clone a security role

2 On New Security Role—General, change the cloned role name. Modify any other properties as needed, then choose OK.

How to delete a single security role

On Security Roles, point to the arrow next to the security role name.

Choose Delete, as shown in Figure 3-12.

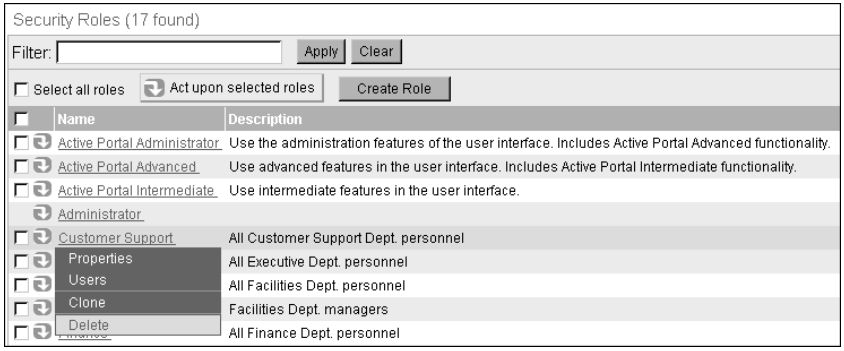

Figure 3-12 Deleting a security role

Confirm the deletion.

How to modify properties for multiple roles

To change the properties for multiple roles, perform the following actions:

1 On Security Roles, select the roles whose properties you want to modify. Figure 3-13 shows two role names selected.

Alternatively, to select all roles on the current page, select the box next to Name. To select all the roles in the Encyclopedia volume, select Select all roles.

Point to Act upon selected roles and choose Properties, as shown in Figure 3-13.

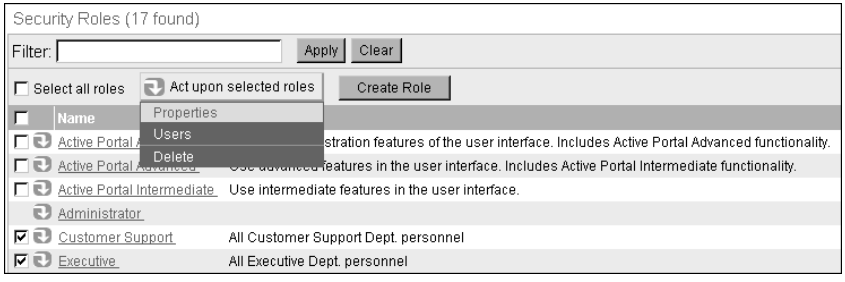

Figure 3-13 Modifying the properties of multiple roles

2 On Security Roles—Properties, make the following changes:

- On General, modify the description field. Figure 3-14 shows General properties.

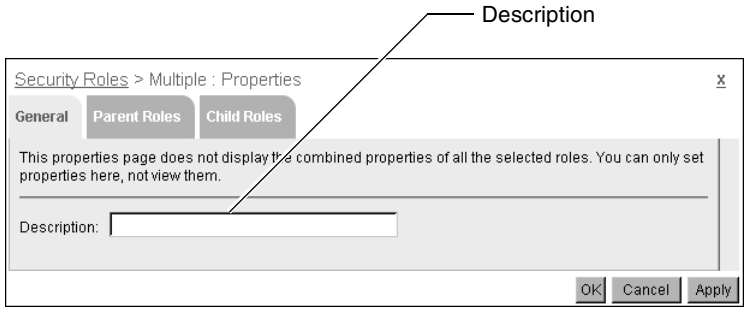

Figure 3-14 Modifying General properties for multiple roles

- On Parent Roles, make modifications by moving security roles in Available to Remove these roles or Add these roles. Select Remove all to remove all parent roles from the selected roles. Selecting Remove all does not remove a parent role that you move to Add these roles from the selected roles. Figure 3-15 shows Parent Roles.

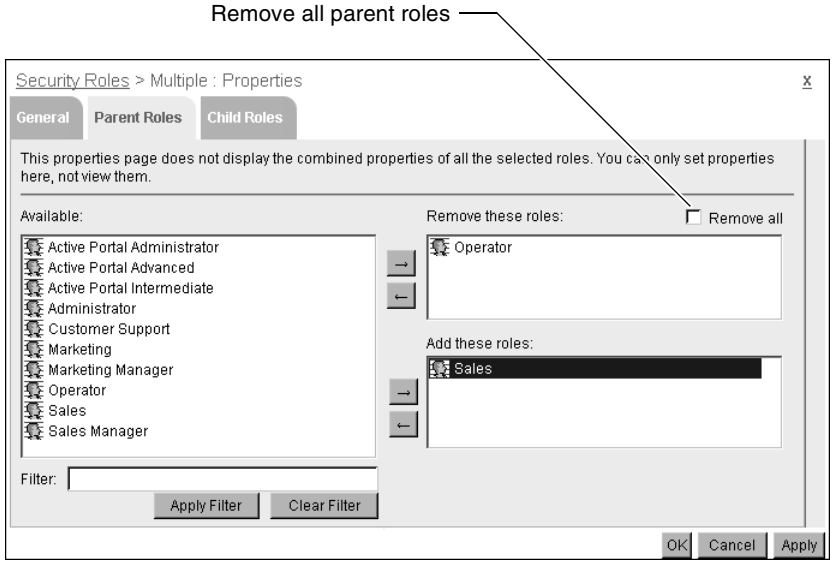

Figure 3-15 Modifying Parent Roles properties for multiple roles

- On Child Roles, make modifications by moving security roles in Available to Remove these roles or Add these roles. Select Remove all to remove all child roles from the selected roles. Selecting Remove all does not remove a child role that you move to Add these roles from the selected roles. Figure 3-16 shows Child Roles.

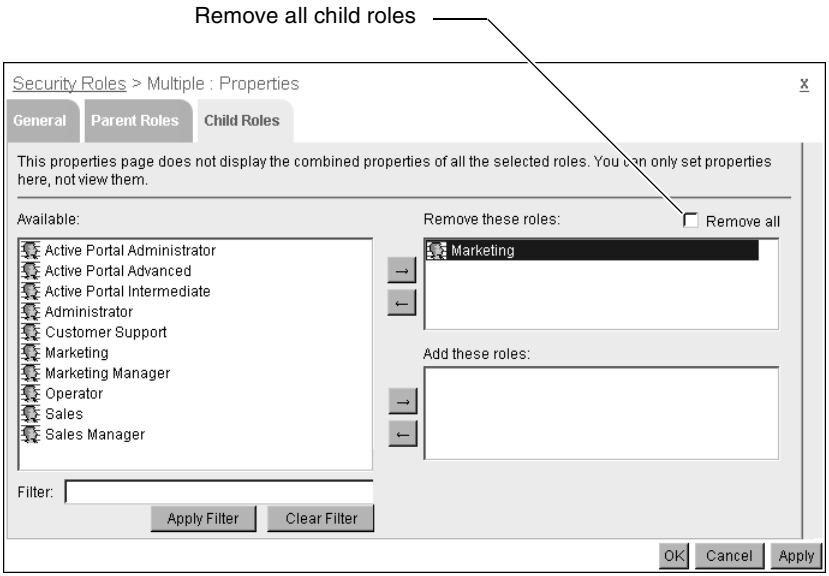

Figure 3-16 Modifying Child Roles properties for multiple roles

How to add and remove users from multiple roles

1 On Security Roles, select the roles for which you want to add or remove users, then point to Act upon selected Roles, and choose Users, as shown in Figure 3-17.

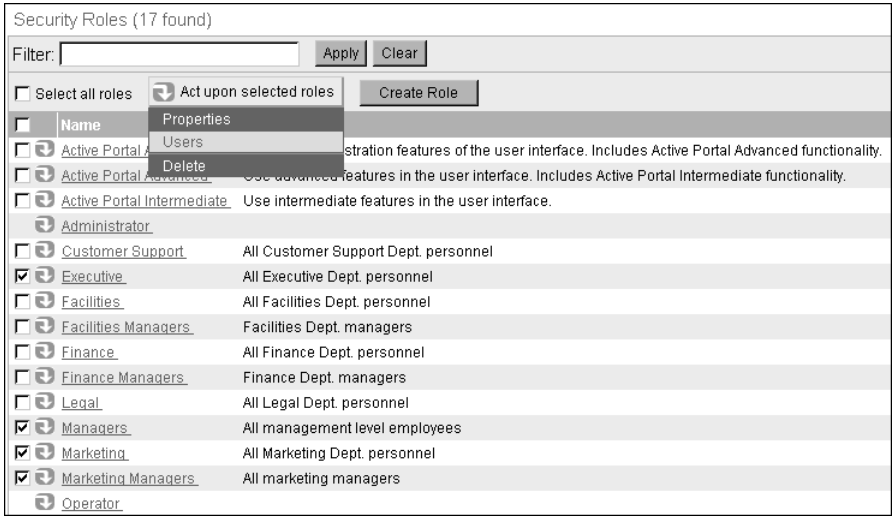

Figure 3-17 Choosing to add and remove users to and from multiple roles

2 On Security Roles—Users, make modifications by moving the users in Available to Remove these users or Add these users. Select Remove all to remove all users from the selected roles. Figure 3-18 shows Security Roles—Users.

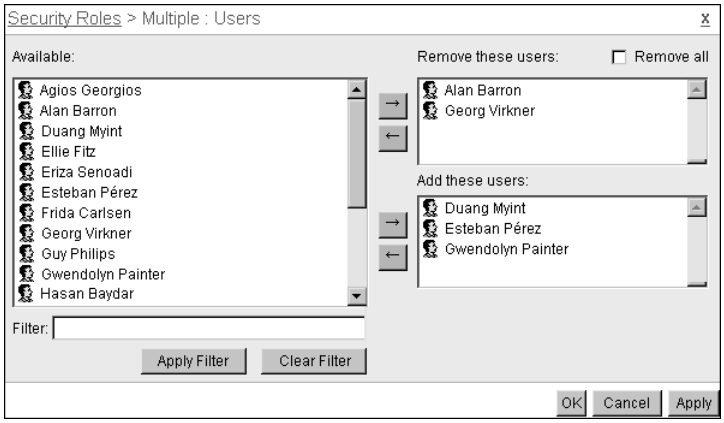

Figure 3-18 Adding and removing users to and from multiple roles

Choose OK.

How to delete multiple security roles

On Security Roles, select the roles that you want to delete. Alternatively, to select all roles on the current page, select the box next to Name. To select all the roles in the Encyclopedia volume, select Select all roles.

Point to Act upon selected roles, and choose Delete, as shown in Figure 3-19.

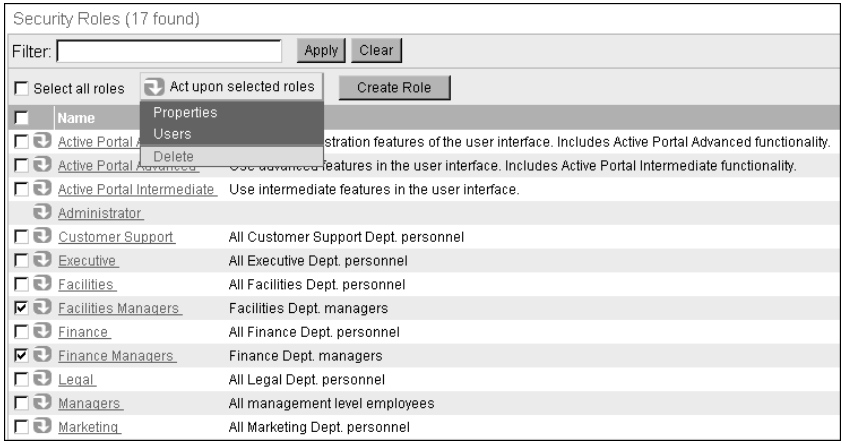

Figure 3-19 Deleting multiple security roles

Confirm the deletion.

Chapter

4

Managing files and folders

This chapter contains the following topics:

- About files and folders
- Adding files and folders to the Encyclopedia volume
- Understanding file and folder properties
- Deleting, copying, moving, and downloading a file or folder
- Managing Actuate queries
- Caching information objects

About files and folders

In managing an Encyclopedia volume, the administrator performs tasks such as creating folders, copying and moving files and folders, and assigning privileges to control access to files and folders. The administrator can see the entire contents of the Encyclopedia volume. Privileges determine what contents a user can see.

When a user logs in to an Encyclopedia volume, Management Console initially displays the contents of the user's home folder. Typically, the home folder is a user's working environment. If the user does not have a home folder, Management Console displays the contents of the volume root folder. Users have read, write, and execute privilege on the root folder by default.

Files and Folders displays the following file or folder information by default:

- Name
  Name of the file or folder
- Type
  Folder or file type description
- Version
  Version number of a file
- Version name
  Version name of a file
- Size
  Size of a file
- Pages
  Number of pages in a document

Figure 4-1 shows the administrator's home folder in the Encyclopedia volume.

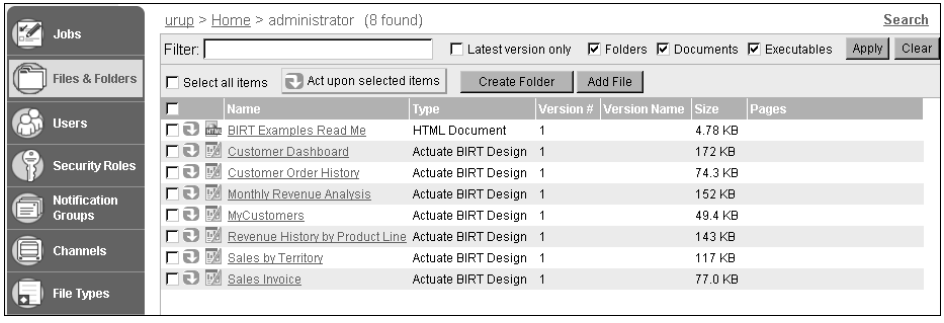

Figure 4-1 Viewing Files and Folders

From Files and Folders, you can perform the following tasks:

- Perform the following tasks for folders only:
  - Create a new folder.
  - View the contents of a folder.
- Perform the following tasks for files only:
  - Upload a document or design file from your desktop.
  - Add and remove file dependencies.
  - Run designs and queries.
  - Download a file to your desktop.
- Get detailed information about files and folders.
- View and set privileges.
- Copy and move files and folders.
- Delete files and folders.
- Set autoarchiving policies for files and folders.

Understanding file and folder properties

Files and Folders displays the following information about a file or folder:

- Name of the file or folder
- Type, which is a folder or file type description
- Version number of a file
- Version name of a file
- Size of a file
- Number of pages in a document.

To get more detailed information about a file or folder, point to the arrow next to the file name and choose Properties, as shown in Figure 4-2.

The Encyclopedia volume divides file properties into four categories, as shown in Table 4-1. The categories for folder properties are the same as for file properties except folder properties do not contain the Dependencies category.

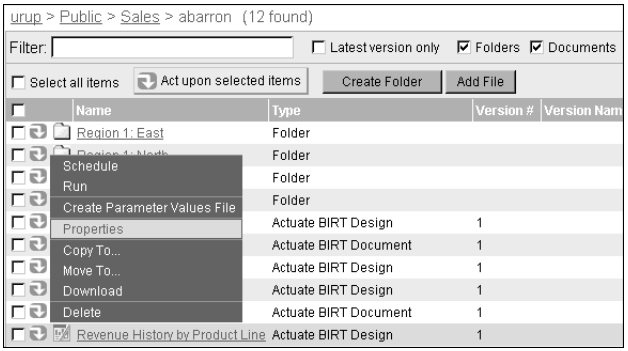

Figure 4-2 Accessing Files and Folders—Properties

Table 4-1 Files and Folders—Properties

Property	Description
Properties—General	Specifies name, description, and user for a file or folder. For a file, additional information includes file type, version name, and whether to replace, create, or keep a version.
Properties—Privileges	Specifies whether users and roles can access a file or folder and if so, which privileges are available, such as Visible, Execute, Grant, Secure Read, Write, Read, Delete, or All.
Properties—Dependencies	Add or remove file dependencies.
Properties—Auto Archive	Specifies the auto archive policy for a file, such as whether to use the inherited policy for the file type and Do not automatically delete this file.

About General properties

Properties—General provides the means to uniquely identify a file or folder.

For a file, Properties—General specifies:

- Name
- File type
- Version number and name
- Size, by page count if applicable, and by size on disk
- Description
- Owner
- Creation date

If you are uploading a file or changing the name or type of a file, Properties—General supports replacing the latest version of a file, or creating a new version, while keeping a specified number of existing versions. Figure 4-3 shows an example of Properties—General for a file, Revenue History by Product Line.rptdesign.

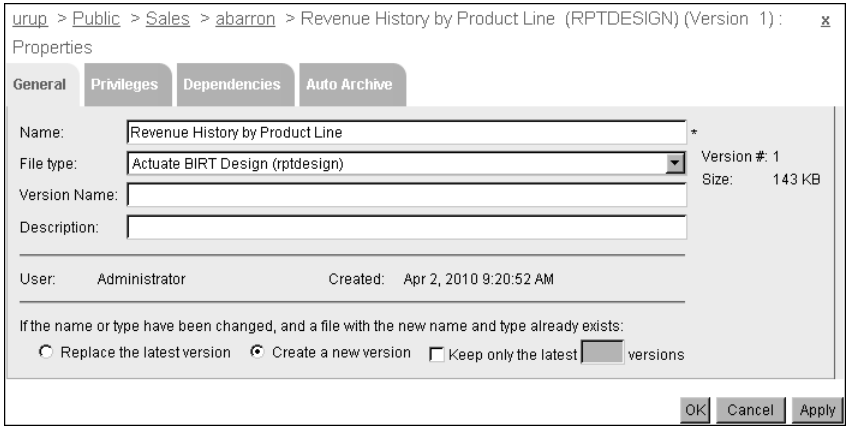

Figure 4-3 Viewing Properties—General for a file

For a folder, Properties—General specifies:

- Name
- Description
- Owner
- Last modified date

Figure 4-4 shows Properties—General for a folder, /Public/Sales/abarron.

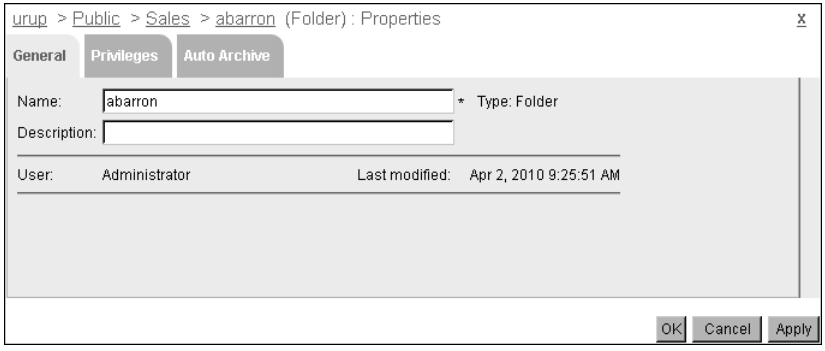

Figure 4-4 Viewing Properties—General for a folder

About file and folder privileges

The administrator provides access to files and folders by assigning privileges to users or security roles. Privileges determine what Encyclopedia volume content a user can see.

If a file or folder is shared, the owner and Encyclopedia volume administrator can set privileges for other users. Only the owner and Encyclopedia volume administrator can access a file or folder that is not shared.

About folder privileges

The Encyclopedia volume supports the following privileges for a folder:

- Read or visible
  A user can see a folder.
- Write
  A user can create, change, and rename a folder.
- Delete
  A user can delete a folder.
- Grant
  A user can change privileges for a folder.

Privileges for Encyclopedia volume folders differ from privileges for folders in other file systems, such as Windows and UNIX, in the following ways:

- Read privilege on a folder does not extend read privileges to items in the folder.
- Write privilege on a folder does not include read or delete privilege.
- Grant privilege is separate from write privilege.

About file privileges

The Encyclopedia volume supports the following privileges for a file:

- Delete
  A user can delete the file.
- Grant
  A user can grant privileges on the file to other users.
- Read and execute
  Privileges on design and document files allow users to perform the following actions:
  - A user can view the contents of a document file while hiding the design file by giving the user read or secure read privilege on the document file only.

- A user can view a design file, but not run it by giving the user both execute and secure read privileges. The file properties and schedule are visible.
- A user can view and run a design file by giving the user both read and execute privileges. If a user has only execute or only read privilege, the design is not visible in the folder and cannot be run.

- Secure read

  Restricts viewing of a file to DHTML format and prohibits downloading. Typically, the administrator assigns Secure read privilege to a user accessing the following:

  - Actuate Basic documents with the e.Report Page Level Security option
  - BIRT Spreadsheet documents with the BIRT SmartSheet Security option
  - BIRT documents with the BIRT Page Level Security option

  As an example, a design developer creates a design that uses one of the security options. The administrator assigns a user secure read privilege and the BIRT Page Level Security option. The user's ID and privileges determine what parts of a document generated from a BIRT design using BIRT page-level security the user can view.

  Read privilege overrides the secure read privilege. If a user has both read and secure read privileges on a document, the user can view and download the entire document.

- Trusted execute

  Permits users to execute an information object without having execute privilege for an information object's underlying data sources. This privilege applies only to Actuate information object (.iob) files and data source map (.sma) files.

  The trusted execute privilege is only available for IOB and SMA files when you set privileges using Management Console. Only a user with administrator privileges can grant the trusted execute privilege. The trusted execute privilege is not inherited.

- Visible

  Permits a user to see a file, but not open it.

Setting privileges on a folder or file

You set folder or file privileges on Properties—Privileges. Figure 4-5 shows the privileges for the Region 1: East folder. The letters beside each user name or security role in Selected are abbreviations for the assigned privileges.

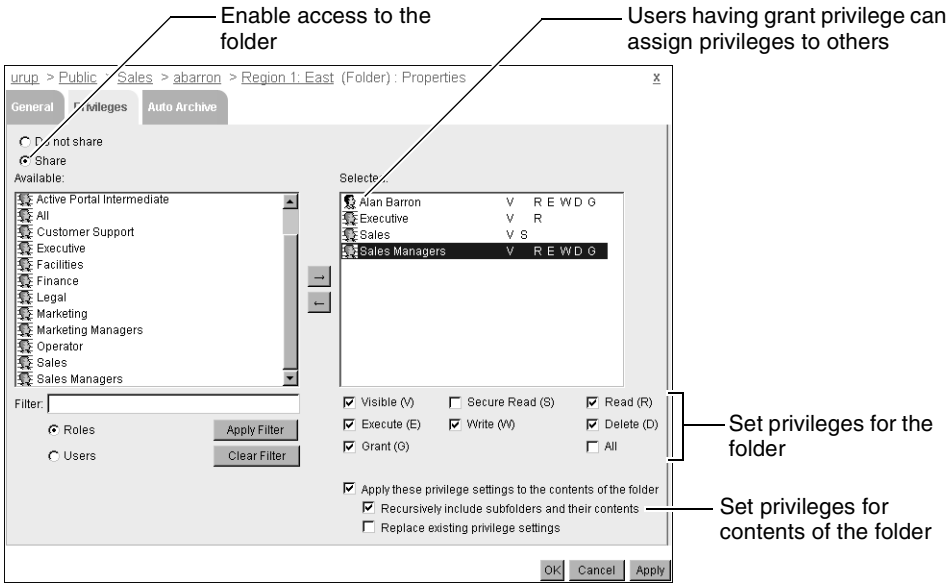

Figure 4-5 Setting privileges on Files and Folders—Properties—Privileges

If a folder or file has shared access, the owner can assign privileges to other users. A user who is not the owner of a file or folder can assign privileges on the file or folder if it is shared and the user has grant privilege on it. The administrator can always assign privileges on the item. By default, all files except Actuate Analytics cube reports are shared. If the administrator or owner does not want other users to have access to a folder or file, that individual can make it private by selecting Do not share.

The Available list contains either security roles or users, depending on whether you select Roles or Users. For example, in Figure 4-5, selecting Roles displays the list of security roles in Available. You can select any of the roles or users in Available and, by choosing the right arrow, move items, one or more at a time, to Selected. In Selected, assign privileges to each user or role by selecting the privileges in the list below Selected.

How to modify privileges on existing files and folders

When setting privileges, you can modify privileges on a single file or folder, or apply the same settings to multiple files or folders simultaneously.

1 On Files and Folders, select items to modify as follows:

- To select a single item, point to the arrow next to the item name and choose Properties. Figure 4-6 shows a folder selected in the single folder example.
- To select multiple files or folders, you can select items individually, as shown in the multiple files example in Figure 4-6, which shows two files selected. Alternatively, to select all items on the current page, select the box next to

Name. To select all the items at this level in the Encyclopedia volume, select Select all items.

Point to Act upon selected items and choose Properties, as shown in the multiple files example in Figure 4-6.

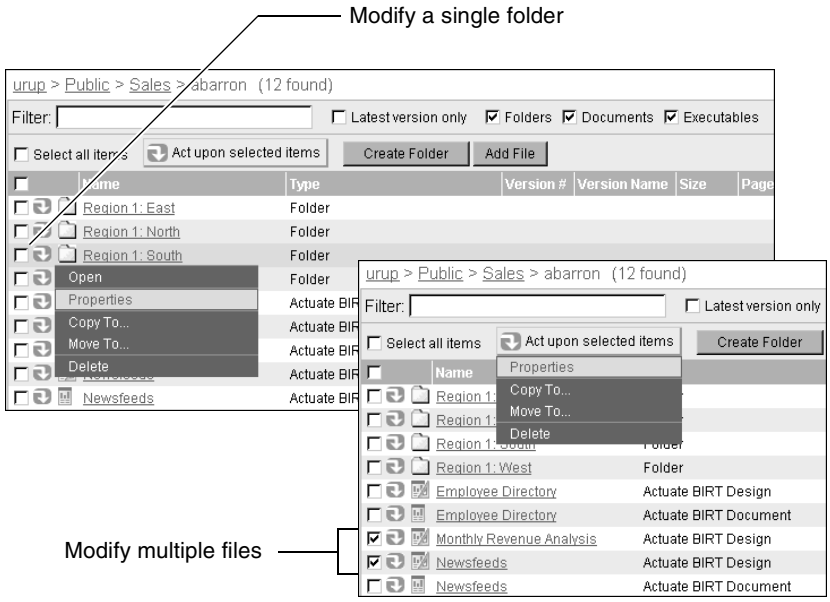

Figure 4-6 Selecting properties for a single item or for multiple items

On Properties, choose Privileges.

2 On Privileges, perform the following tasks, as shown in Figure 4-7:

- Specify whether the items are shared or private.
  Select Set file access type, then select Do not share or Share. By default, items are shared.
- View a list of roles or users in Available.
  Select Roles or Users.

- Remove privileges on the items.
  Move roles or users from Available to Remove these privileges. iServer assigns all privileges to a role or user you move to Remove these privileges. To select privileges that you want a role or user to keep, select the role or user in Remove these privileges, then deselect the privileges.
- Remove all privileges on the items.
  Select Remove all. Selecting Remove all does not remove privileges you assign in Add these privileges.

- Assign privileges on the items.
  Move roles or users from Available to Add these privileges.

  In Add these privileges, select one or more roles or users, then select privileges from the privilege list.

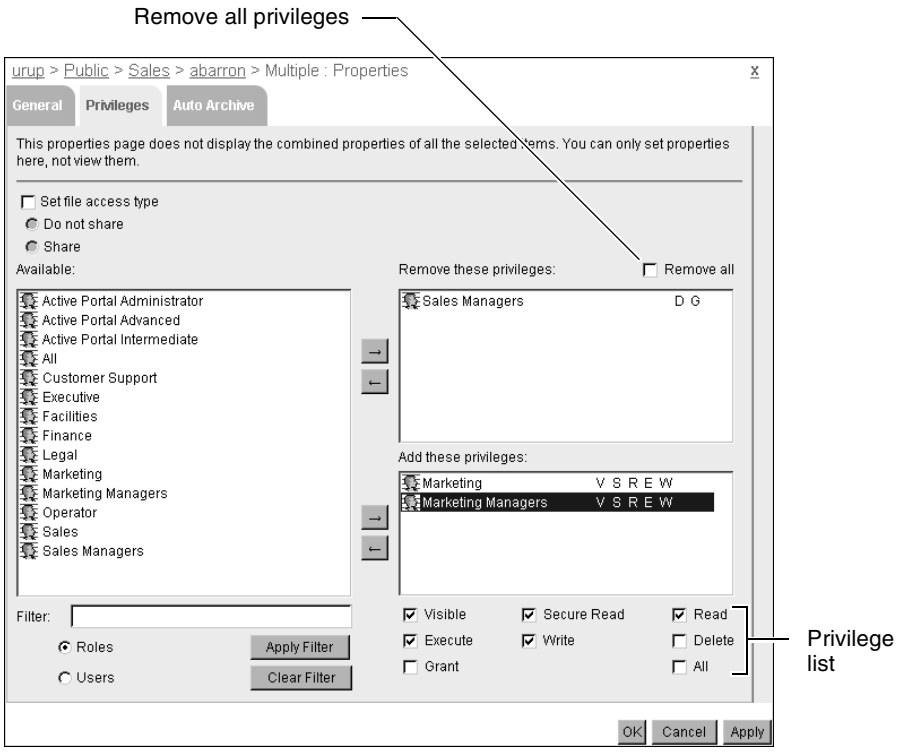

Figure 4-7 Modifying privilege settings for multiple files or folders

Choose OK.

About dependencies

To open an Actuate report document (.roi), it must have a dependency on an Actuate report executable (.rox) of the same name. When the executable runs, the generated document has a dependency on the executable.

On Files and Folders, Properties—Dependencies displays the location of the report executable, as shown in Figure 4-8.

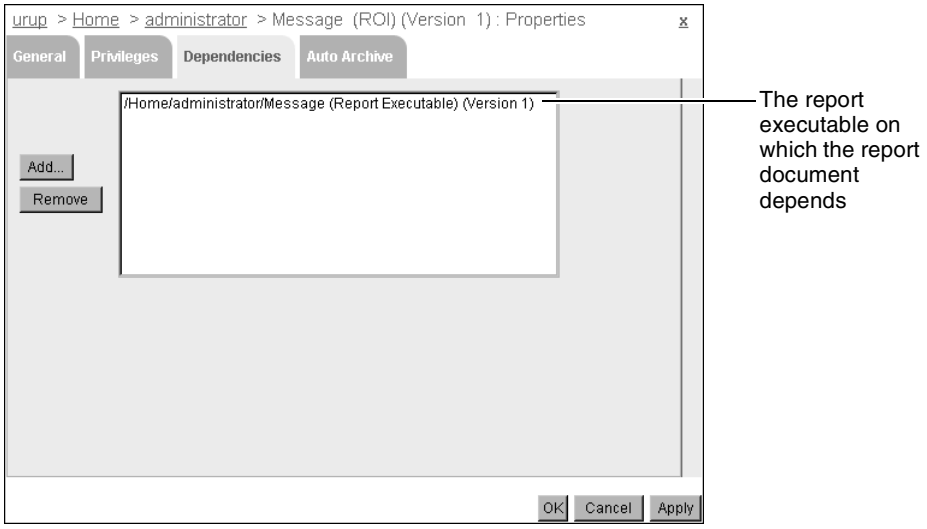

Figure 4-8 Viewing the location of the report executable

A parameter values file also has a dependency on an Actuate report executable file of the same name or a BIRT design file of the same name, depending from which file type the user created the parameter values file. To run a parameter values file, a user must have read and execute privileges on the report executable or BIRT design file on which the parameter values file depends. iServer updates the dependency information if a user moves the report executable or BIRT design to a different location on the Encyclopedia volume.

About autoarchiving

Autoarchiving is an iServer file management capability that supports file and folder archiving and deletion based on the age of the item. You specify the age for an item in days and hours, or alternatively, by specifying a date and time in the future. When the item reaches that age, the item expires and iServer can delete the item from the volume. You can specify that iServer archive the item before deleting it. You can also specify that iServer not delete the item.

You can assign an age to an item by specifying an age for the item itself, for the file type of the item, for the folder containing the item, or for the entire Encyclopedia volume.

Set autoarchive properties on Properties—Auto Archive. Property names on Auto Archive display differently depending on whether a user selects a file, folder, or multiple files or folders.

Figure 4-9 shows Properties—Auto Archive for a file.

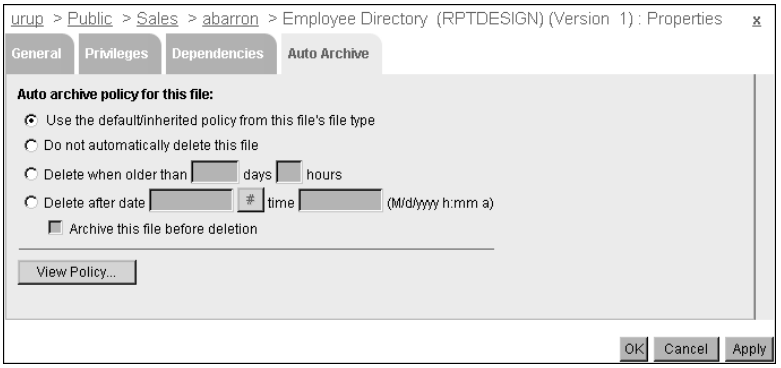

Figure 4-9 Viewing Properties—Auto Archive for a file

Figure 4-10 shows Properties—Auto Archive for a folder.

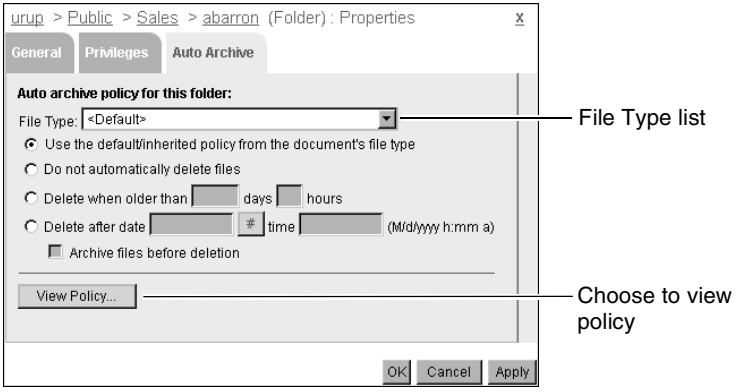

Figure 4-10 Viewing Properties—Auto Archive for a folder

Figure 4-11 shows Properties—Auto Archive for multiple items.

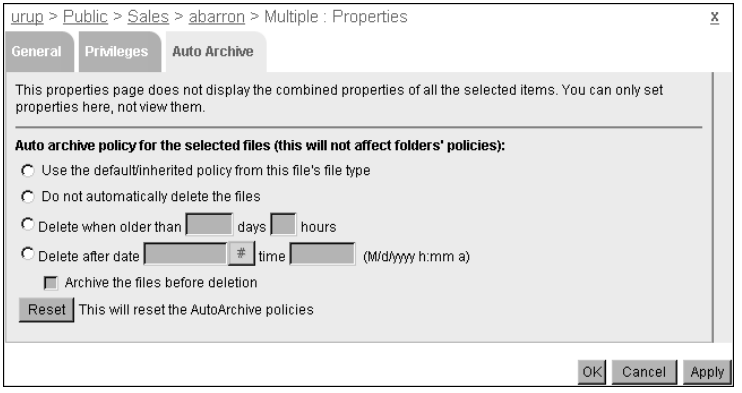

Figure 4-11 Viewing Properties—Auto Archive for multiple items

Table 4-2 lists the configurable properties on Properties—Auto Archive for a file or folder. These properties support setting and changing the archiving policy for a single file, for a folder, or for the following groupings of Encyclopedia volume items:

- A folder's contents
- A folder and its contents
- Multiple files or folders

Table 4-2 Autoarchive properties

Field	Definition
File Type (folder only)	Use this list of known file types to configure the autoarchive policy for a folder and its contents.
Use the default/inherited policy from: ■ The document's file type (folder) ■ The file's file type (file)	For a folder, select to inherit the parent folder or volume policy. For a file, select to inherit the file type default policy.
Do not automatically delete: ■ Files (folder) ■ This file (file) ■ The files (multiple files)	Select to prevent deletion by the autoarchive process.
Delete when older than *n* days *n* hours.	Select to delete items automatically after being on the system for the number of days and hours you specify.
Delete after date *M/d/yyyy* time *h:mm a.*	Select to delete items automatically after the date and time you specify.
View Policy (not multiple files)	Choose to view the autoarchive policy for the selected folder or file.
Reset (multiple files or folders only)	Choose to deselect all options on Properties—Auto Archive.

Using the File Type list

When working with a folder, the File Type list supports setting the autoarchive policy for the folder, as well as its contents, by file type, as shown in Figure 4-12.

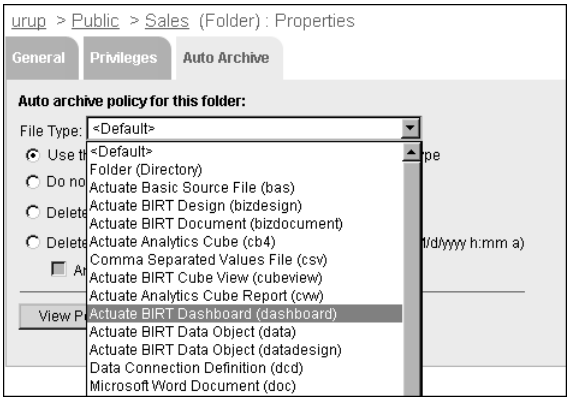

Figure 4-12 Selecting a file type for which to set autoarchive policy

When setting the autoarchive policy for a folder, the settings you make apply to all subfolders and files in the folder that inherit their archive policy from the selected folder. This includes for example, a file or folder that inherits its archive policy from its parent folder, which inherits its policy from the selected folder.

A file or folder for which you select an archive policy option other than Use the default/inherited policy, retains the policy you set. For example, if you set an archive policy of Do not automatically delete for a specific .rptdesign file, then from its parent folder, you set an archive policy of Delete after 1 day 0 hours for .rptdesign type files, the policy that you set for the specific .rptdesign file does not change. The same is true when setting the archive policy for a group of files or folders.

File Type includes the following selections:

- <Default>
  Determines the default autoarchive policy for the selected folder and its contents.
- Folder (Directory)
  Determines the default autoarchive policy for subfolders of the selected folder. The policy does not apply to files in subfolders of the selected folder. If you select to delete subfolders, by specifying either a period of days and hours, or a date and time, iServer deletes a subfolder only under the following conditions:
  - The subfolder is empty.
  - The subfolder contains only the following:
    - Files whose autoarchive policy indicates that the files have expired.
    - Empty subfolders.

- All file types known to iServer

  Determines the default autoarchive policy for the file type you select. When you select a file type in File Type, property settings on Auto Archive display the current settings for the selected file type.

You can set the archive option value for one file type after another before choosing OK to implement the changes. Management Console retains the values you set for multiple file types and applies the values when you choose OK.

About the default or inherited archiving policy

A folder at the root level inherits the autoarchive policy set on Volume—Properties—Archiving and Purging. Auto archive property settings you make for a folder and its contents become the default autoarchive settings for any subfolder and its contents.

By default:

- The autoarchive policy for all file types and folders is Do not automatically delete this file and Do not archive file before deletion. If you run Auto Archive without changing the policy for any item from the default policy, iServer deletes no file or folder on the Encyclopedia volume.
- When you select Properties—Auto Archive for a folder, Management Console selects <Default> for File Type and Use the default/inherited policy from this document's file type. This folder and its contents inherit the autoarchive policy of the parent folder and its contents.
- When you select Properties—Auto Archive for a file, Management Console selects Use the default/inherited policy from this file's file type. This file inherits the autoarchive policy that exists for a file of the same type in the parent folder.

When you select Properties—Auto Archive for multiple files or folders, Management Console does not select a policy setting, but Use the default/inherited policy from this file's file type functions the same as when you select Properties—Auto Archive for a single file. The selected files inherit the auto archive policy for files of the same type in the parent folder.

About setting the autoarchive policy for multiple folders

You can set the autoarchive policy for multiple folders at the same time. The archive option values you choose for the selected folders will apply also to any item in a selected folder that inherits its archive policy from that selected folder.

Viewing the existing archive policy

To view the autoarchive policy for a file or folder, choose View Policy on Properties—Auto Archive. Figure 4-13 shows sample archive policy information for a BIRT Document file.

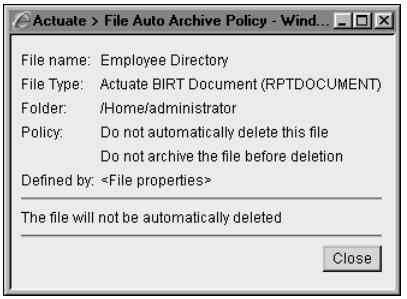

Figure 4-13 Viewing the autoarchive policy

Selecting not to delete automatically

To prevent the autoarchive process from removing a selected folder and its contents, or a selected file or files, select Do not automatically delete files.

Selecting to delete by specifying a time or date

To specify an age an item must reach before the autoarchive process can delete the item, select Delete when older than *n* days *n* hours and type values for *n*.

To specify a date and time before which the autoarchive process cannot remove an item, select Delete after date *M/d/yyyy* time *h:mm a*. When you select this option, Management Console inserts the current date + 2 days for the date and the current time + 2 hours for the time. The language you log in to Management Console with determines the date and time format. For example, when the locale is English (United States), the following formats apply:

- *M/d/yyyy*
  A date expression that translates to, for example, 12/1/2009 or 1/6/2010
- h:mm a
  A time expression that translates to, for example, 1:59 P.M.

To select a date from a calendar when using the Delete after date *M/d/yyyy* time *h:mm a* option, choose the calendar option #.

If you define an autoarchive driver for the volume, selecting one of the Delete options supports specifying whether iServer archives the selected file, folder, or selected multiple files before the autoarchive process deletes the selected file, folder, or multiple files. Depending on the following conditions, the name of the option appears differently on Properties-Auto Archive:

- If setting the archive policy for a folder, the option name is Archive files before deletion.
- If setting the archive policy for a file, the option name is Archive this file before deletion.

- If setting the archive policy for multiple files, the option name is Archive the files before deletion.

How to set or modify archive policy for a folder

1. On Files and Folders, point to the arrow next to the folder name, and choose Properties.

   On Properties, choose Auto Archive.

2. On Auto Archive, leave File Type set to <Default> if you want to set the policy for the selected folder and its contents, or select a file type from File Type if you want to set the policy only for files of that type within the selected folder.

3. Select one of the following options:

   - Use the default/inherited policy from the document's file type.
   - Do not automatically delete files.
   - Delete when older than *n* days *n* hours.
   - Delete after date *M/d/yyyy* time *h:mm a.*

   If you define an autoarchive driver for the volume and you select one of the Delete options, you can also select Archive files before deletion.

4. To set values for multiple file types, set archiving option values for each selection you make from File Type.

   Choose OK.

How to set or modify the archive policy for a single file

1. On Files and Folders, point to the arrow next to the file name, and choose Properties. On Properties, choose Auto Archive, as shown in Figure 4-14.

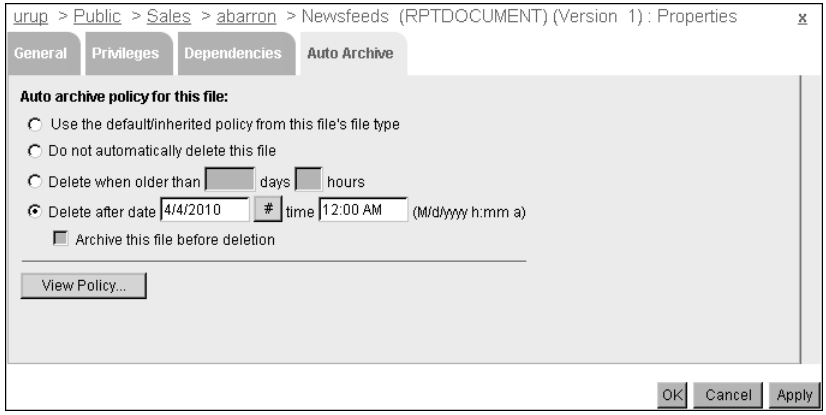

Figure 4-14 Setting autoarchive properties for a file

2 On Auto Archive, specify or modify the following options:

- Use the default/inherited policy from this file's file type.
- Do not automatically delete the file.
- Delete when older than *n* days *n* hours.
- Delete after date *M/d/yyyy* time *h:mm a.*

If you define an autoarchive driver for the volume and you select one of the Delete options, you can also select Archive this file before deletion.

Choose OK.

How to set archive policy for multiple items simultaneously

1 On Files and Folders, select the items for which you want to set the archive policy. To select all items on the current page, select the box to the left of Name. Alternatively, to select the items at this level on all pages, choose Select all items.

Point to Act upon selected items, and choose Properties, as shown in Figure 4-15.

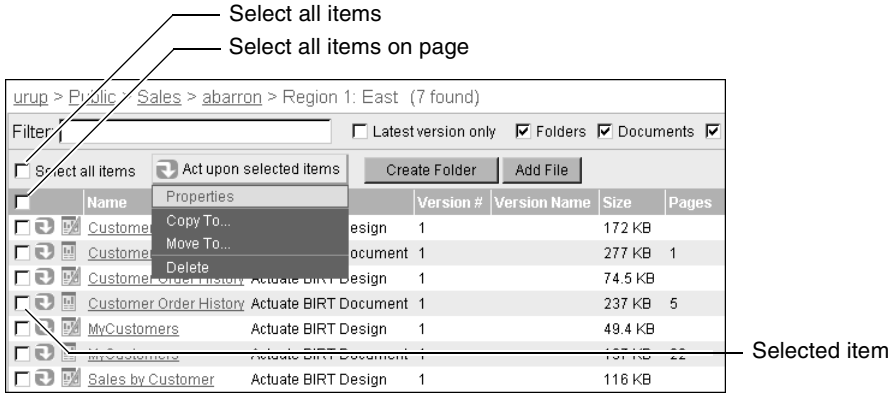

Figure 4-15 Selecting multiple files for which to set archive policy

On Properties, choose Auto Archive.

2 On Properties—Auto Archive, specify or modify the following options:

- Use the default/inherited policy from this file's file type.
- Do not automatically delete the files.
- Delete when older than *n* days *n* hours.
- Delete after date *M/d/yyyy* time *h:mm a.*

If you define an autoarchive driver for the volume and you select one of the Delete options, you can also select Archive the files before deletion.

3 Optionally, choose Reset to deselect all selections you make on Properties—Auto Archive.

Choose OK.

Adding files and folders to the Encyclopedia volume

You create a folder in the Encyclopedia volume to contain files, such as design, document, information object, and Actuate query files. Design developers use design tools to create design files to upload or publish to the Encyclopedia volume.

In the volume, you can generate document files as output by running a design or an Actuate query.

Creating a folder

The administrator can create a folder and set privileges for security roles and individual users.

How to create a new folder

1 On Files and Folders, choose Create Folder.

2 On New Folder—General, specify a folder name and optionally, a description, as shown in Figure 4-16.

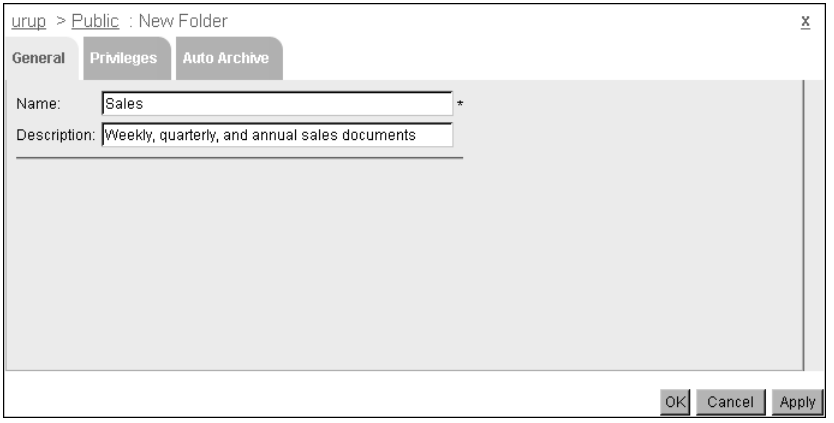

Figure 4-16 Specifying a name and description for a folder

3 On New Folder—Privileges, assign privileges to roles and users, as shown in Figure 4-17.

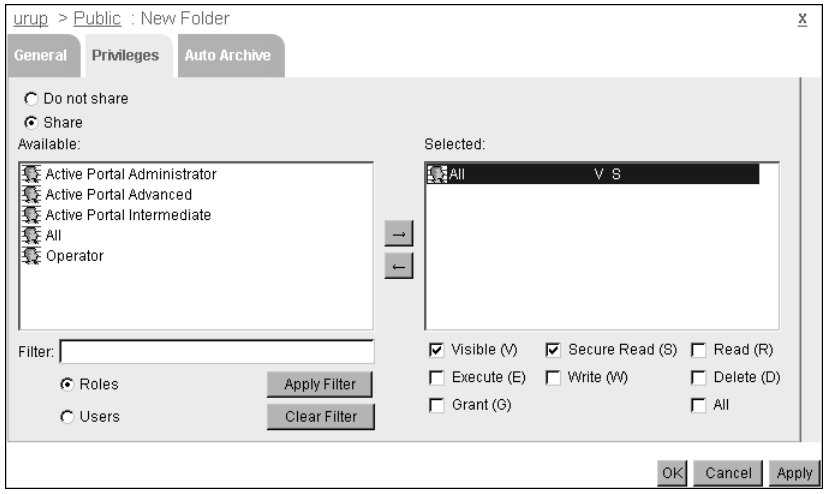

Figure 4-17 Assigning privileges to roles and users

On Privileges, perform the following tasks:

1. Specify whether the item is shared or private. By default, files and folders are shared. To make an item private, select Do not share.

2. Select one or more roles or users in Available and move them to Selected.
3. With the roles or users moved and selected, assign privileges from the list of privileges such as Visible, Secure Read, or Read.
4. To set privileges for a folder, but not its contents, or for a file, choose OK.
5. To set privileges for the contents of a folder, use the selections below the list of privileges as follows:
   - To set privileges for the folder and contents, including the subfolders and files at that level, select Apply these privilege settings to the contents of the folder.
   - To set privileges for the folder and contents, including the subfolders and files at all levels below it, select Recursively include subfolders and their contents.
   - To replace the existing privilege settings on the folder and contents and specify new privileges, select Replace existing privilege settings.

6. To remove access to an item, move one or more security roles or users from Selected to Available.

4. On New Folder—Auto Archive, specify the policy by which iServer deletes the folder, and whether iServer archives the folder before deleting it, as shown in Figure 4-18.

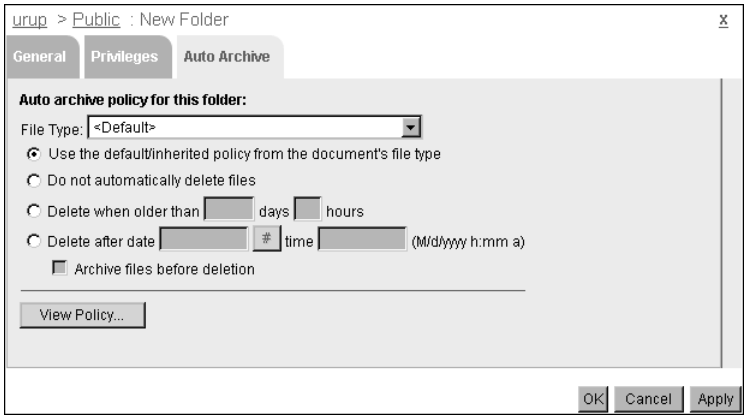

Figure 4-18 Specifying the autoarchiving policy on a folder

For more information about auto archiving, see "About autoarchiving," earlier in this chapter. Choose OK.

Uploading a file

When a user adds a file to the volume, the file's creator and users having the Administrator role have full privileges on the file. A user must have write privilege on the folder containing the uploaded file as well as visible, secure read, or read privileges.

How to upload a file

1. On Files and Folders, choose Add File.
2. On Add File, choose Browse.

   In Choose file to upload, perform the following tasks:

   1. Navigate to and select the file to upload.
   2. Choose Open. The path to the file appears in Add File, as shown in Figure 4-19.
3. If the file you are uploading already exists, make selections among the following options:

   - Replace the latest version.
     Uploading the file overwrites the previous version. You can also migrate dependencies for files. For DCD, IOB, and SMA files, always replace the latest version and migrate dependencies. Do not create a new version.
   - Create a new version.
     Use this option to create a new version of the file. You can also specify how many versions to keep. The new version replaces the oldest version.

- Copy the following properties from the latest version of the file. Select any, or none, of the following options:
  - Description
    Note that provides information about the file.
  - Permissions
    Access privileges that a user has to items in a volume.
  - Auto archive rules
    File management rules that support file archiving and deletion based on the age of the file, a specific date, or the number of versions.

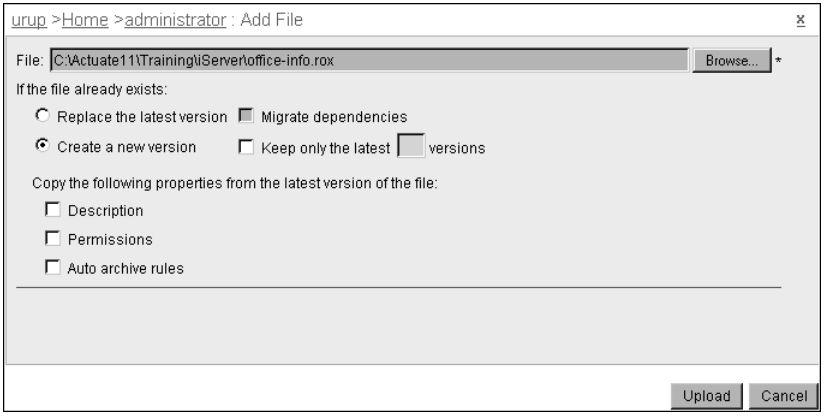

Figure 4-19 Selecting the file to upload

4 Choose Upload.

After uploading a file, Management Console displays Files and Folders—Properties—General, where you specify the file property values.

How to specify file property values

1 In Files and Folders—Properties—General, specify file property values, as shown in Figure 4-20.

Properties—General contains the following properties:

- Name
  Name of the file
- File type
  Encyclopedia volume file type, such as Actuate Report Document (ROI), Actuate Report Executable (ROX), BIRT Design (RPTDESIGN), BIRT Document (RPTDOCUMENT), or Actuate Information Object (IOB)

- Version number
  Version number of the file
- Version name
  Optional name of this version of the file
- Size
  Size of the file
- Description
  Optional description of the file
- User
  Name of the user that owns the file
- Created
  Date on which iServer created the file

If you change the Name or File type property, and a file with the new name and type already exists, select from the following properties:

- Replace the latest version
  iServer replaces the latest version of the file with the new version.
- Create a new version
  iServer creates a new version of the file.
- Keep only the latest *n* versions
  Selecting Create a new version enables this option. iServer replaces the oldest version of the file with the new version, and keeps only the latest *n* versions, where *n* is the number you specify.

Figure 4-20 Specifying uploaded file properties

2 On Properties—Privileges, set privileges for a file by selecting Share, then for Filter, select Roles or Users. Move roles or users from Available to Selected, and assign privileges, as shown in Figure 4-21.

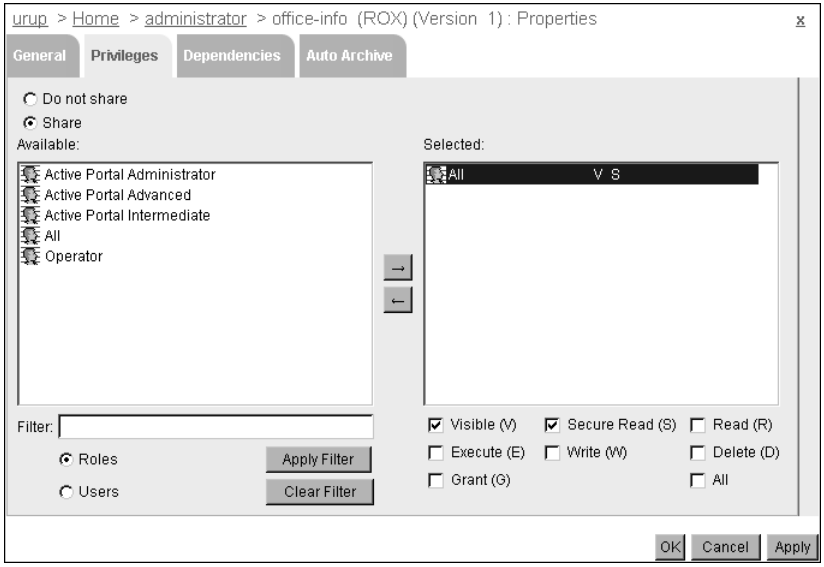

Figure 4-21 Specifying uploaded file privileges

3 On Properties—Dependencies, add or remove dependencies on other files. Choose Add and browse for the file on which the file depends. For example, to view an Actuate report document file (.roi), it must have a dependency on an Actuate report executable file (.rox). For a .rox, you do not need to set a dependency on a .roi. Figure 4-22 shows Properties—Dependencies.

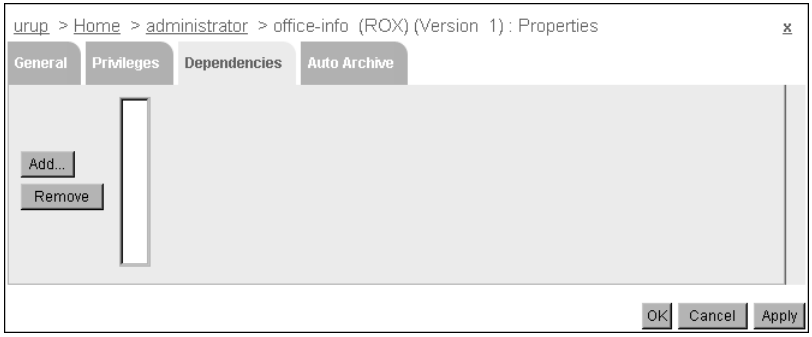

Figure 4-22 Specifying uploaded file privileges

4 On Properties—Auto Archive, specify the file archive policy using the following options, as shown in Figure 4-23:

- Use the inherited policy for the file type

- Do not automatically delete
- Delete based on age or date
- Archive the file before deletion

Choose View Policy to view the auto archive policy for the file.

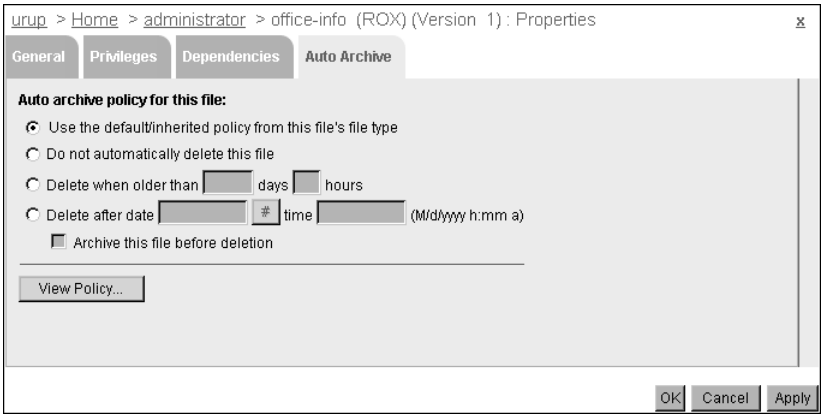

Figure 4-23 Specifying the autoarchive policy for the uploaded file

5 Select one of the following options:

- Use the default/inherited policy from the document's file type.
  The file inherits the autoarchive policy existing for a file of the same type in the parent folder.
- Do not automatically delete files.
  An auto archive run does not delete the file.
- Delete when older than *n* days *n* hours.
  Specify the number of days and hours.
- Delete after date *M/d/yyyy* time *h:mm a.*
  Specify the date and time of day. The format for both expressions depends on the iServer locale setting.

6 If you select one of the Delete options and you have an autoarchive driver defined for the volume, you can also select Archive files before deletion.

Choose OK.

7 The file, named office-info in this example, now appears as a report executable file on Files and Folders, as shown in Figure 4-24.

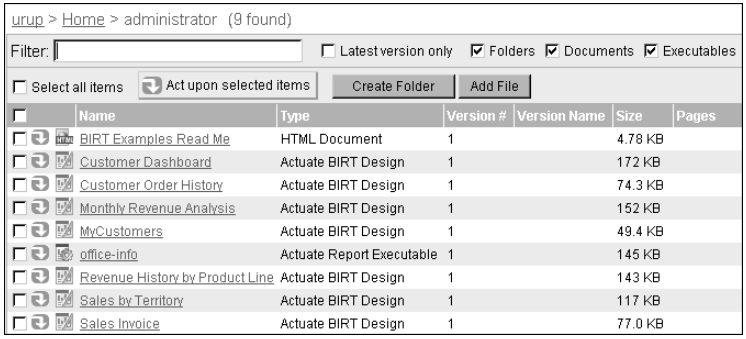

Figure 4-24 Viewing the files and folders list, including office-info

When you create a folder or upload a file, consider the string length that you use for that item's name and options. Management Console imposes a fixed upper limit on the length of text strings that you provide for options such as names, descriptions, file types, and URLs.

Deleting, copying, moving, and downloading a file or folder

The following sections describe how to delete, copy, move, and download a file or folder in an Encyclopedia volume.

Deleting a file or folder

Users can delete a file or folder from the Encyclopedia volume only if they have the delete privilege for the item. A user has the delete privilege for a folder or file if:

- The user owns the folder or file.
  Users own items that they create.
- The user is an administrator.
- The user has been granted the delete privilege by the administrator or owner of the folder or file.

If a user does not have the delete privilege for an item that the user tries to delete, iServer displays a message stating that the user lacks the necessary permission.

How to delete a single file or folder

On Files and Folders, point to the arrow next to the file or folder name, and choose Delete, as shown in Figure 4-25.

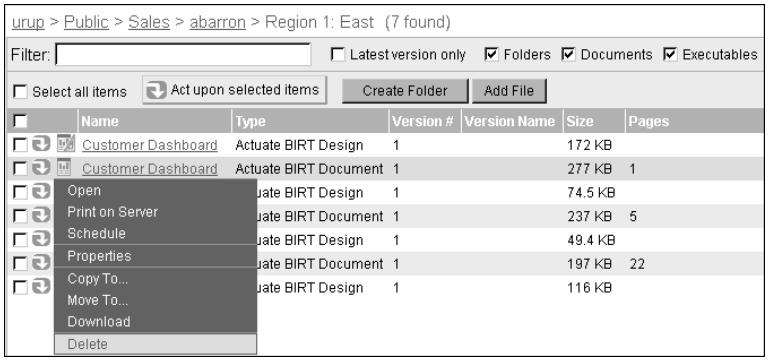

Figure 4-25 Deleting a file or folder

Choose OK to confirm the deletion.

How to delete multiple files or folders

On Files and Folders, select the names of the files or folders to delete. Alternatively, to select all files on the current page, select the box next to Name. To select all the files at this level on all pages, select Select all items.

Point to Act upon selected items, and choose Delete as shown in Figure 4-26.

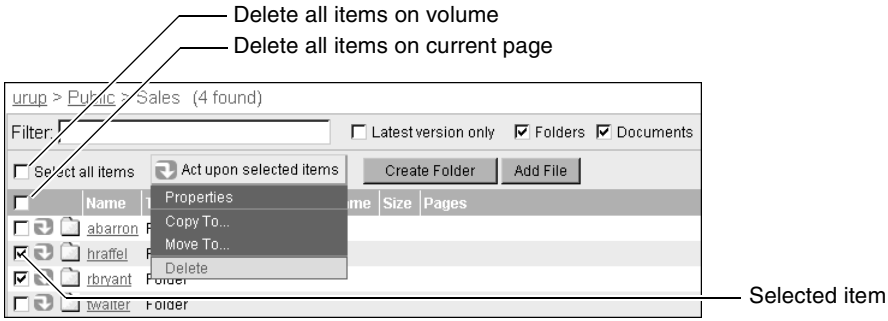

Figure 4-26 Deleting multiple folders

Choose OK to confirm the deletion.

Copying or moving a file or folder

You can copy or move a single file or folder or multiple files and folders from one place on the Encyclopedia volume to another. You can also download a file or folder to an external location.

How to copy or move a single file or folder

1 In Files and Folders, point to the arrow next to the file or folder name, and choose Copy To or Move To, as shown in Figure 4-27.

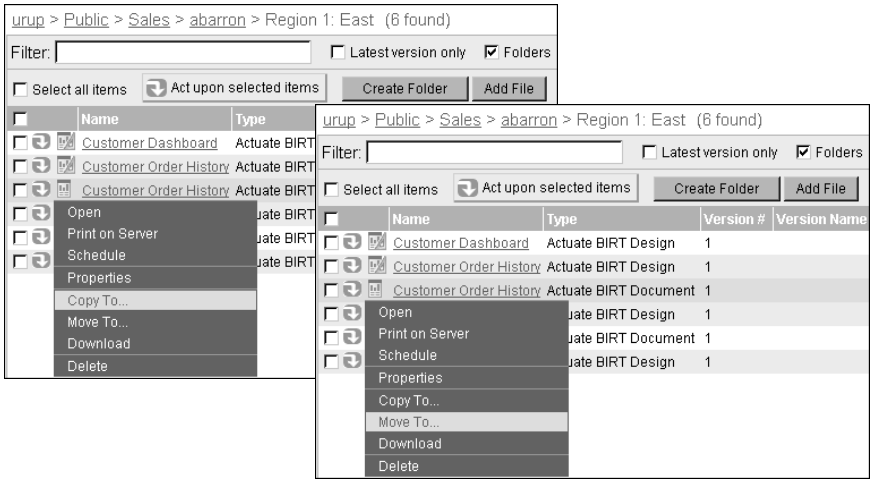

Figure 4-27 Choosing to copy or move a single file or folder

Copy or Move appears. You provide the same information, in the same way, whether copying or moving an item. Figure 4-28 shows Copy.

Figure 4-28 Copying or moving a file

2 On Copy or Move, perform the following tasks:

- Specify a new item name.
  Type the name.
- Specify a destination folder.
  Type the name or choose Browse to navigate to and choose the folder.
- If you are copying or moving a file, and the file already exists at the destination, make selections among the following options:
  - Replace the latest version.
    iServer replaces the latest version of the file with the new version.

- Create a new version.
  iServer creates a new version of the file.
- Keep only the latest *n* versions.
  Selecting Create a new version enables this option. iServer replaces the oldest version of the file with the new version, and keeps only the latest *n* versions, where *n* is the number you specify.

- If you are copying or moving a folder, and the folder already exists at the destination, handle any duplicate files by making selections among the following options, as shown in Figure 4-29:
  - Replace the latest versions.
    iServer replaces the latest version of any file in the folder or in any subfolder, with the new version.
  - Create new versions.
    iServer creates a new version of any file in the folder or in any subfolder.
  - Keep only the latest *n* versions.
    Selecting Create new versions enables this option. iServer replaces the oldest version of any file in the folder or in any subfolder, with the new version, and keeps only the latest *n* versions, where *n* is the number you specify.

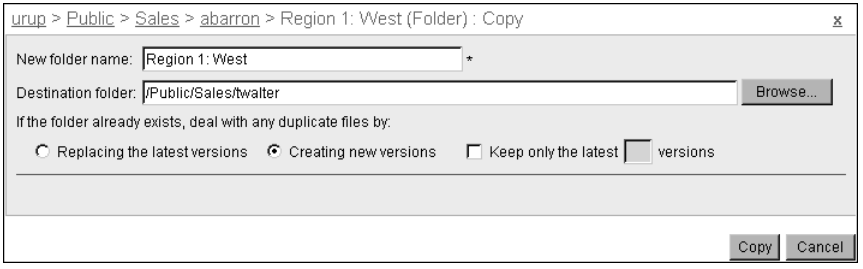

Figure 4-29 Copying or moving a folder

How to copy or move multiple files and folders

1 For multiple files or folders, select the items you want to copy or move. Alternatively, to select all items on the current page, select the box next to Name. To select all items at this level on all pages, select Select all items. Point to Act upon selected items, and choose Copy to or Move to, as shown in Figure 4-30.

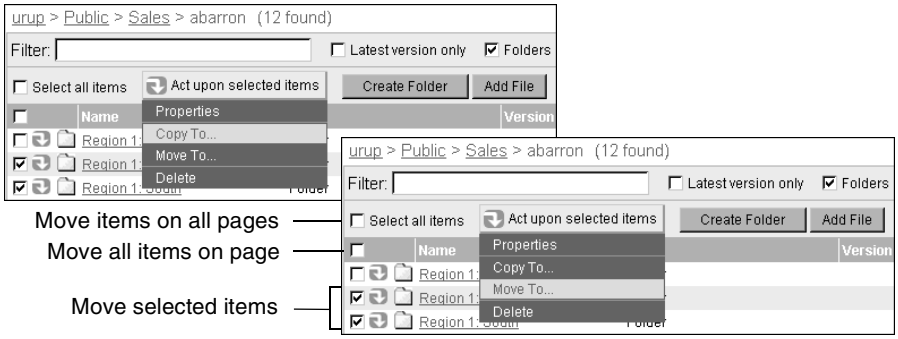

Figure 4-30 Copying and moving files or folders

2 If you are copying or moving multiple items, which can include both files and folders, perform the following tasks, as shown in Figure 4-31:

- Specify a destination folder.
  Type the name or choose Browse to navigate to the folder.
- If any files already exist at the destination, you handle any duplicates by making selections among the following options:
  - Creating new versions
    iServer creates a new version of the file.
  - Replacing all previous versions
    iServer replaces the latest version of any file with the new version. iServer does not replace all previous versions of a file with the new version.

Figure 4-31 Copying or moving multiple items

Choose Copy or Move.

How to download a file

1 On Files and Folders, point to the arrow next to the file name.

Choose Download, as shown in Figure 4-32.

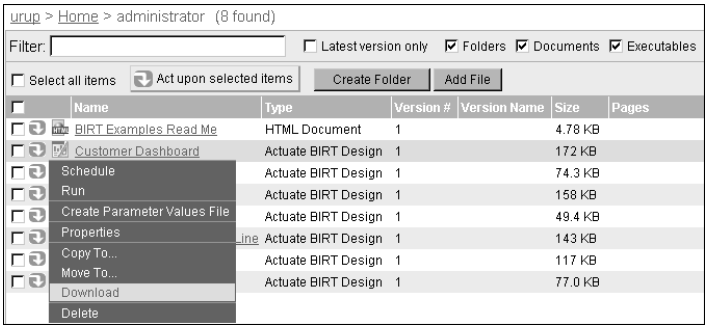

Figure 4-32 Downloading a file

2 On File Download, specify whether to open the file or save it to a new location. Selecting Save opens a Save As dialog.

3 On Save As, specify the destination to which you want to download the file.

Choose OK.

Managing Actuate queries

This section describes how to use Management Console to create a query for an information object. You create a query as an alternative to creating a design when it is more important to get a quick view of the data than to work on the presentation of data.

First, a designer creates an information object in Actuate Information Object Designer and publishes it to an Encyclopedia volume on iServer. The information object contains data source and SQL specifications. Next, in Management Console you create a Query Definition (.dov) file for the information object using the Query Wizard. Finally, you run or schedule the query, which generates the Query Output document (.doi) file, a plain view of the data you specify.

Creating a query

To create a new query, you must have read privilege on the information object from which you derive the data source information and SQL specifications. You can make the query available to other users by granting read and execute privileges on the DOV to the appropriate users and security roles. Users having those privileges can edit and run the query definition to generate query output.

How to create a query

1 On Files and Folders, locate the information object you want to use.

2 Point to the arrow next to the information object name and choose Create Query, as shown in Figure 4-33.

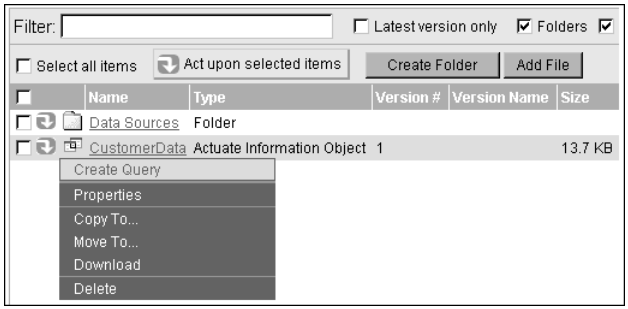

Figure 4-33 Choosing to create a query

3 Use the Actuate Query Wizard to create and save the query, as shown in Figure 4-34.

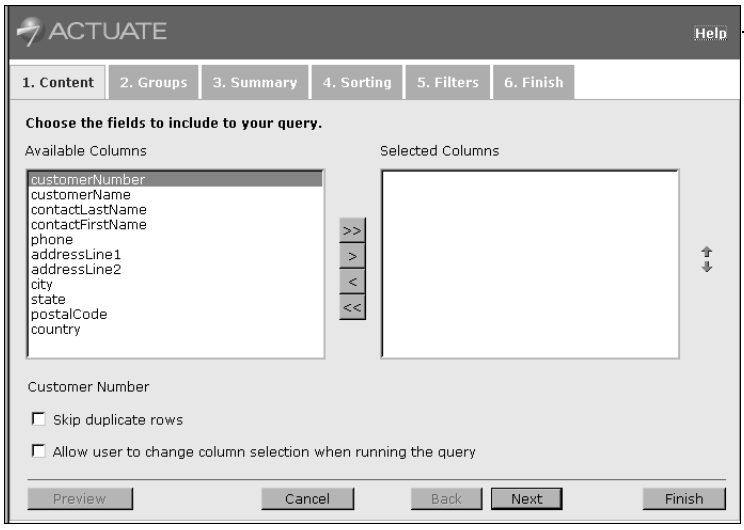

Figure 4-34 Creating a query using Actuate Query Wizard

For more information, choose Help.

You can create multiple versions of a query in an Encyclopedia volume. If you modify an existing DOV or create a new version of a DOV, it inherits the properties, such as privileges and scheduling information, from the original DOV.

Editing a query

If you have write privileges on a DOV, you can modify a query and save the revised version in the Encyclopedia volume. If not, you can save the revised version of the query using a different name or save it to a different location.

1 Point to the arrow next to the Actuate Query Definition and choose Edit Query, as shown in Figure 4-35.

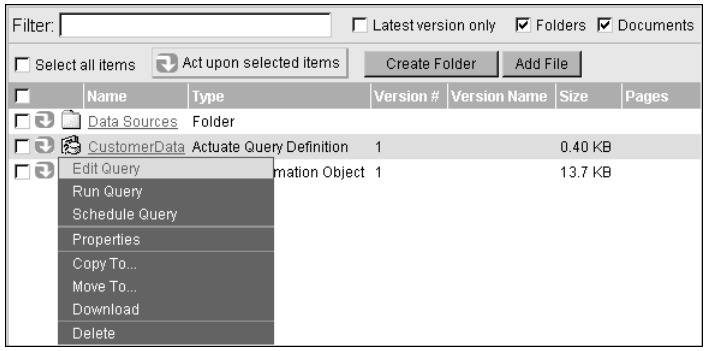

Figure 4-35 Choosing to edit a query

2 On Actuate Query Wizard, modify the settings in Content, Groups, Summary, Sorting, Filters, and Finish.

Running and scheduling a query

In Management Console, point to the arrow next to an Actuate Query Definition. Choose Run Query to run the query and immediately view the query output. Choose Schedule Query to run the query in the future, on a recurring basis, or right now and save the output. When you choose Schedule and schedule a query to run right now, iServer saves the query output in the Encyclopedia volume. When you choose Run Query, iServer displays the query output without saving it.

How to schedule a query

1 Point to the arrow next to the Actuate Query Definition and choose Schedule Query, as shown in Figure 4-36.

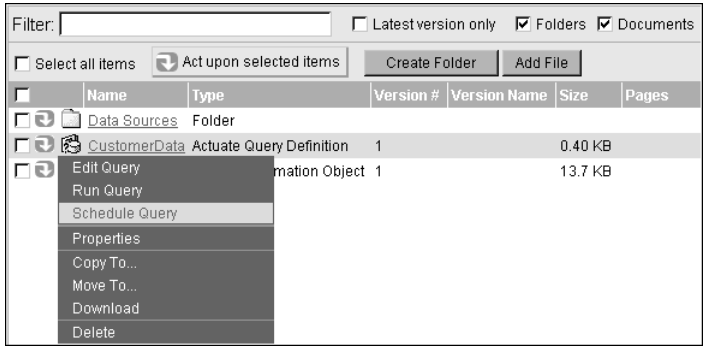

Figure 4-36 Choosing to schedule a job to run a query

2 Choose Finish.

3 To receive an e-mail notification when the job completes, on Finish, select Send me an e-mail notification. To attach the output document to the e-mail, select a format for the attachment. The available formats are PDF, Excel, RTF, and Fully Editable RTF.

4 Choose Submit.

Caching information objects

You can improve the performance of your databases by using the iServer Caching service to cache information objects in a separate database. Caching information objects in a cache database reduces the load on your production databases. To cache an information object, you use Information Object Designer to create a cache connection definition and cache object. Using Management Console, you activate the cache object and populate the cache table. A cache connection definition defines the connection properties. A cache object associates the object with a table in the cache database.

Activating a cache object

An inactive cache object does not have an associated table in the cache database. Designs that consume the source information object do not use cached data. To create a cache table, log in to iServer as Administrator, and activate the cache object as described in the following procedure.

How to activate a cache object

1 On Files and Folders, navigate to the cache object that you created in Information Object Designer and published to iServer.

2 Point to the arrow next to the file name and choose Properties, as shown in Figure 4-37.

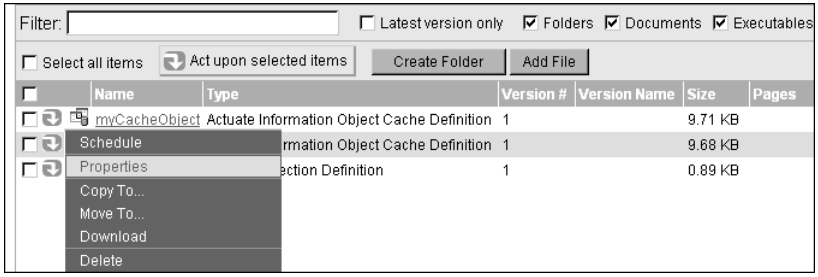

Figure 4-37 Choosing properties of a cache object

3 On Configure, select Activate, as shown in Figure 4-38. Configure shows the status of the cache object. Accept the default, Select Delete cache table when cache object is deleted, to remove obsolete tables.

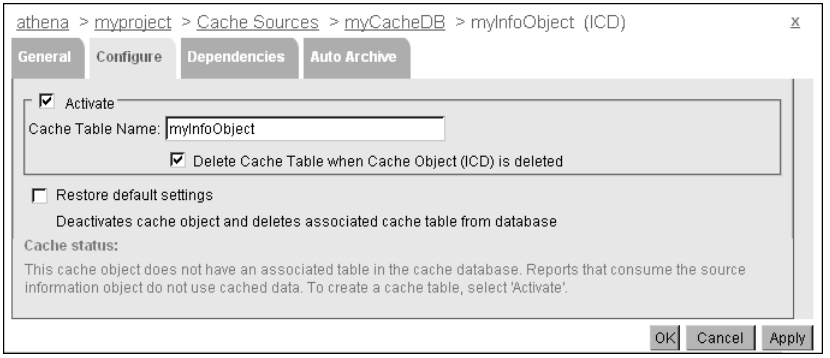

Figure 4-38 Activating the cache object

Understanding the status of a cache object

A cache object is in one of the following states:

- Fresh
  This cache object does not have an associated table in the cache database. Reports that consume the source information object do not use cached data. To create a cache table, select Activate.
- Activated
  This cache object is associated with a specific table in the cache database, but the table is empty. Reports that consume the source information object do not use cached data. To populate the cache table, schedule a job for the cache object.
- Activated and in use
  This cache object is associated with a specific table in the cache database. The Management Console status message tells you when the table was last populated. Reports that consume the source information object use cached data.

  To periodically refresh the data rows in the cache table, schedule a recurring job for the cache object.
- Deactivated
  This cache object is not active. Reports that consume the source information object do not use cached data. To deactivate the cache object, deselect Activate.

Populating the cache table

To periodically refresh the data rows in the cache table, you schedule a recurring job for the cache object as described in the following procedure.

How to populate the cache table

1 On Files and Folders, navigate to the cache object that you created in Information Object Designer and published to iServer.

2 Point to the arrow next to the file name and choose Schedule, as shown in Figure 4-39.

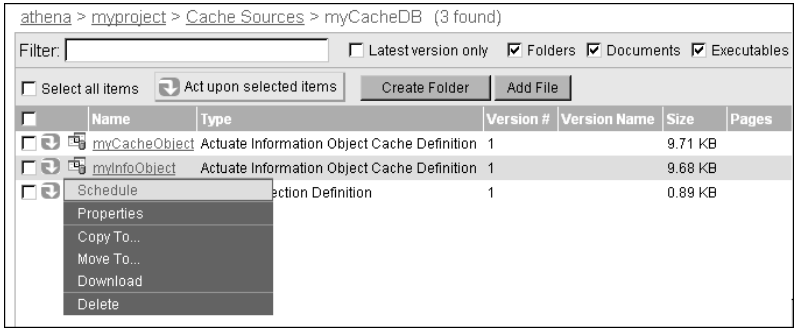

Figure 4-39 Populating the cache database

3 On Schedule, choose Recurring and select a time to repeatedly run the job, as shown in Figure 4-40.

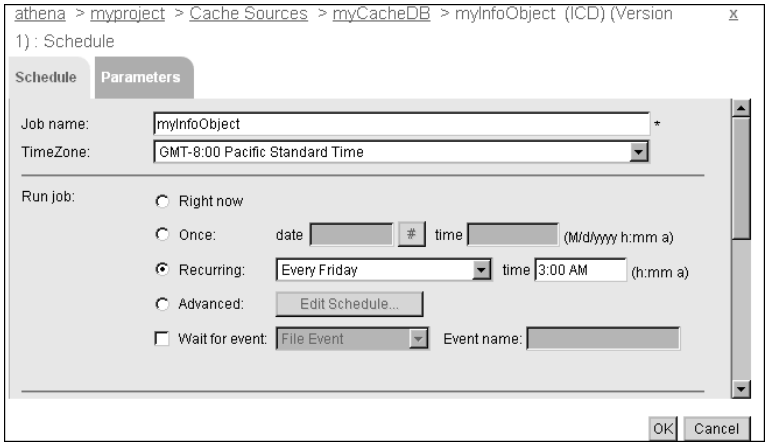

Figure 4-40 Scheduling a recurring job

4 Choose OK.

Chapter

5

Scheduling, running, and managing designs

This chapter contains the following topics:

- Understanding how to run a design
- Running a design
- Scheduling a job
- Troubleshooting problems
- Using a date-and-time expression in a document or version name
- Monitoring job status

Understanding how to run a design

A design contains formatting and data source specifications. You can think of a design as a data-less template.

You run a design from a file such as a BIRT Design, BIRT Spreadsheet, parameter values file, or a query. When iServer executes the design, iServer retrieves data from the database, formats it, and generates a document.

You access a design from Files and Folders. If you schedule a job to run a design, you can monitor the scheduled job and view the generated document on Jobs. If you run a design, iServer executes the design immediately without creating a job, and displays the generated document.

You access Files and Folders and Jobs from the side menu, as shown in Figure 5-1.

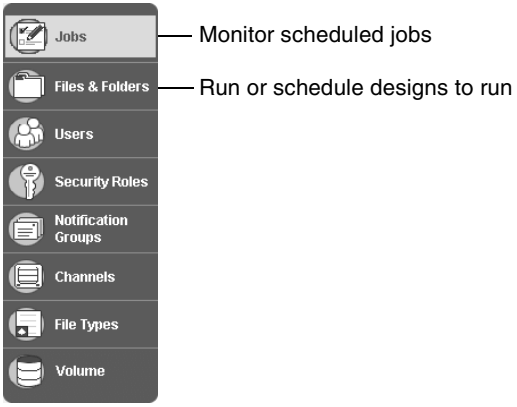

Figure 5-1 Accessing Jobs and Files and Folders from the side menu

In Files and Folders, you point to the arrow next to the file name, as shown in Figure 5-2, to access the context menu for scheduling or running a design.

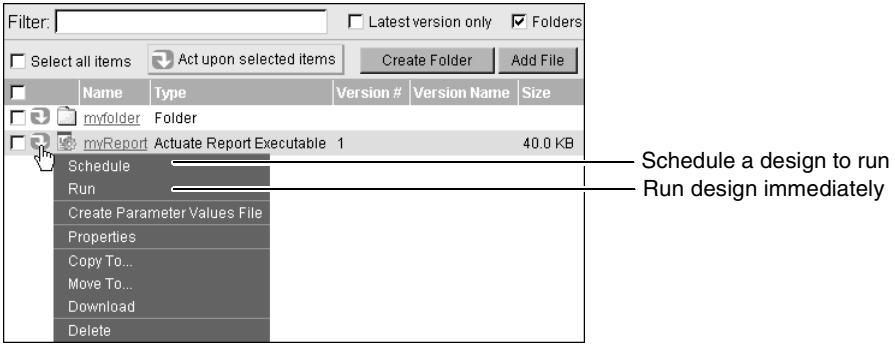

Figure 5-2 Accessing the menu for scheduling or running a design

Running a design

You can run a design using the default execution settings. iServer simply displays the generated document without saving it. Alternatively, you can specify properties such as parameter values, whether to save the document, where to save it, and privileges on the document.

How to run a design

1 On Files and Folders, navigate to the folder that contains the design to run.

Point to the arrow next to the design file name. Choose Run, as shown in Figure 5-3.

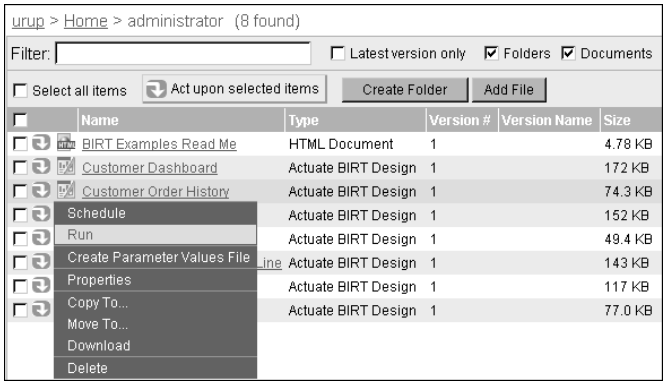

Figure 5-3 Choosing to run a design

2 If the design contains parameters, provide values, or accept the default values on Parameters. If you want to save the document, select Save the output document on Parameters, as shown in Figure 5-4.

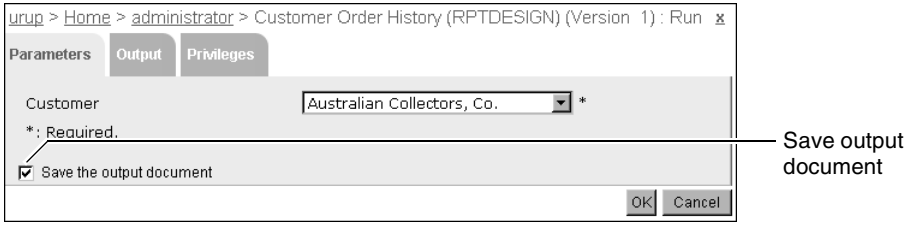

Figure 5-4 Saving the output when running a design

Selecting Save the output document enables Output and Privileges.

Select Output.

3 On Output, as shown in Figure 5-5, you can perform the following optional tasks:

- Specify a date-and-time expression in Version Name that evaluates to the run date.
- Specify the folder to which to save the output document.
- Specify how to handle an existing version of the output document.
- Specify the archive policy for the output document.

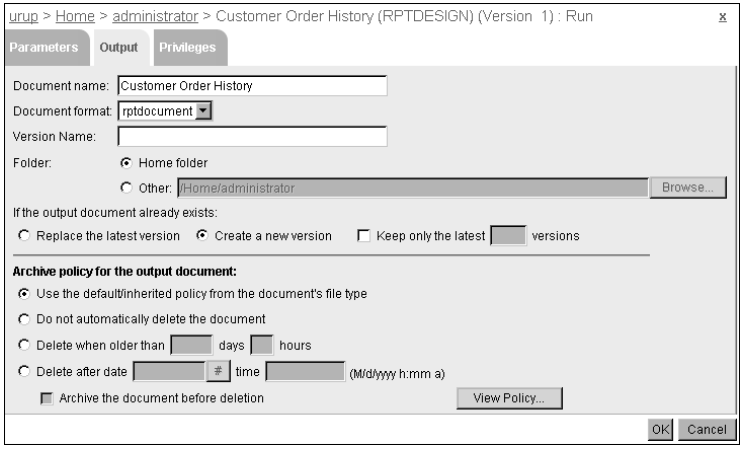

Figure 5-5 Specifying output properties

Select Privileges.

4 On Privileges, perform the following tasks:

1 Select Roles or Users to view the list of security roles and users from which to select in Available, as shown in Figure 5-6.

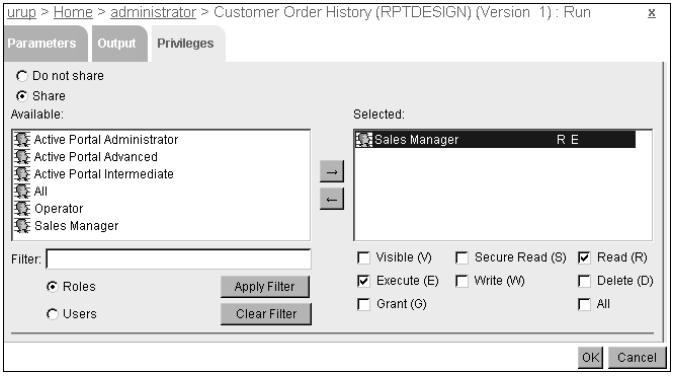

Figure 5-6 Specifying privileges on the output document

2 Move roles or users from Available to Selected.

3 Assign privileges by selecting from the list of privileges such as Visible, Execute, or Read.

4 Cancel all privilege assignments for this job by selecting Do not share. Select Share to reinstate assigned privileges.

Choose OK to generate and view the document.

Running a design produces a temporary document that iServer does not save. This temporary document is sometimes called a transient document.

iServer creates all server-related temporary files in the AC_DATA_HOME \server\tmp directory. The default location of AC_DATA_HOME on a Windows operating system is C:\Actuate11\iServer\data. On a Linux system, it is /<Installation directory>/AcServer/data. The start scripts for iServer on a UNIX or Linux system set TMPDIR to AC_DATA_HOME/server/tmp. Any iServer operation that creates a temporary file is responsible for deleting that file.

When performing an automatic or manual upgrade from a previous release of iServer to release 11, the following files and folders from the previous release remain in their original location:

- AC_SERVER_HOME/etc/acserverconfig.xml
- AC_SERVER_HOME/encyc
- AC_SERVER_HOME/log
- AC_SERVER_HOME/tmp

If you deliberately stop and start the iServer service, iServer retains the temporary document files. For example, if the administrator specifies a new transient report cache location, then stops and starts the iServer service, iServer moves any temporary files to the new location. When iServer restarts or stops abnormally, iServer deletes all temporary files except those with a .lock file-name extension.

To generate a temporary document in a cluster, you must enable both the Factory and the View service on one or more nodes.

Scheduling a job

iServer incorporates a flexible job scheduling model for running designs and queries. The term job refers to the following iServer tasks:

- Generating a document by running a design using a schedule
- Printing a document

- Converting the following document formats:
  - From a BIRT design to BIRT document, Excel, PDF, Postscript, PowerPoint, Word
  - From a BIRT document to CSV, Excel, PDF, Postscript, PowerPoint, PSV, TSV, Word
  - From a BIRT Spreadsheet design or document to Excel
- Querying an information object by running an Actuate Query

After a scheduled job runs, iServer can notify channel users by e-mail about the availability of the document.

In Management Console, you schedule a job in Files and Folders and track Job status in Jobs. In scheduling a job, you specify the following properties:

- Schedule
  Settings include job name, time zone, priorities, version number, number of retries, and other run job settings, such as date and time, recurrence, and event settings.
- Parameters
  Run-time design parameters, if any exist.
- Output
  Properties such as where to store the output document, the file format, and the archive policy.
- Privileges
  Privilege assignments on the output document for users and security roles.
- Channels
  Channels for broadcasting the document and sending job completion and failure notices.
- Notification
  Notification groups and users to notify when a job completes, and notification options, such as notifying by e-mail or by creating a completion notice in a user's personal channel.
- Print
  How to print the output document.

Specifying scheduling properties

You can schedule a job to run immediately or at a scheduled time. You can set the time explicitly or base it on a system event. If you create a job that uses an event-based criteria and schedule the job to run immediately, the job does not run

until the event occurs. If you create a job that uses both a system event and a schedule, the job runs when both conditions occur.

For example, if you specify a schedule to run a job at 4:00 P.M. on Monday after generating the file \\server2\mydocuments\document.xls, iServer runs the job after 4:00 P.M. on Monday if document.xls exists.

If document.xls generates before 4:00 P.M. on Monday, iServer runs the job at 4:00 P.M. on Monday. If iServer is down when a scheduled job tries to run, the job runs when iServer restarts.

Table 5-1 describes the properties of the Run job section of Schedule—Schedule.

Table 5-1 Job scheduling properties

Property	Description
Right now	Run the job immediately.
Once	Run the job once, at some future date and time. Specify the date and time. You can use the calendar option # to select a date. The default date is the current date. The default time is 10 minutes later than the current time.
Recurring	Run the job at regular intervals. Select the interval in Recurring, and specify the time of day.
Advanced	Create a custom schedule. Selecting this option enables Edit Schedule, which invokes Job Schedule Builder, in which you can design a specific schedule.
Wait for event	Set a system event as the criteria for running a job. In Wait for event, select File Event, Job Event, or Custom Event. Optionally, you can provide a file or event name.

Your choice of event type determines the availability of options described in Table 5-2.

Table 5-2 Scheduling event types

Event type	Description
File Event	Specify a fully qualified path to an operating system file or folder as the event criteria. Do not use a relative path. iServer runs the event-based job when it finds the file or folder. If the item does not exist, iServer waits until the item exists before running the job.

(continues)

Table 5-2 Scheduling event types (continued)

Event type	Description
Job Event	Use Job Selector to choose the name of a scheduled job as the event criteria. iServer runs the event-based job when the scheduled job completes. You can specify whether to trigger a job after a successful or a failed job completion event, or both. You can also specify a lag time, in minutes, after which iServer scans previously completed, qualifying jobs. For example, if you specify 60 minutes, iServer scans jobs that completed in the preceding 60 minutes. If a job meets the event-based criteria, iServer runs the event-based job.
Custom Event	Specify a web service that iServer monitors. iServer communicates with the web service and runs a custom event-based job when the web service returns a signal to iServer. To specify a custom event, you must create a web service application and deploy it in the BIRT iServer System environment, then configure the web service in System Volumes—Events in Configuration Console.

About scheduling a job

If a design generates a large document, schedule a job to run the design. Attempting to generate a very large document by running a design unscheduled tends to cause time-out errors. iServer waits a fixed amount of time for the generated document, 30 minutes by default. If document generation takes longer than the wait period, iServer stops waiting for the document and displays a time-out message.

Scheduled jobs run in the background. You do not have to wait for the processing to complete before you perform other tasks, such as submitting another run request. iServer saves the output in the Encyclopedia volume, so you can view it at a later time.

You can schedule a job to generate a weekly document that contains the summary sales figures for a store, for example. iServer generates the document once each week and saves the document in the Encyclopedia volume. Alternatively, you can schedule an event-based job. For example, you can schedule a job that presents sales data for an area after iServer finishes running jobs that present the sales data for individual stores in that area. Conditions that trigger event-based jobs include the following:

- The existence of a specific file in the Encyclopedia volume
- The completion of another job
- The output of a web service event

Finally, you can schedule iServer to run a job that is based both on time and on an event.

When you schedule a job to run, you can also perform the following tasks:

- Schedule printing after iServer generates the document.
- Set priorities for running designs.
- Retry running scheduled designs that fail to run.
- Manage version control.
- Limit user access to the generated document.
- Distribute the document.
- Send notification of the availability of the document.

How to schedule a job to run

1 Navigate to a folder that contains a design. The file can also be a document generated by a design, a parameter values file (.rov), or a query.

Point to the arrow next to the file name, and choose Schedule, as shown in Figure 5-7.

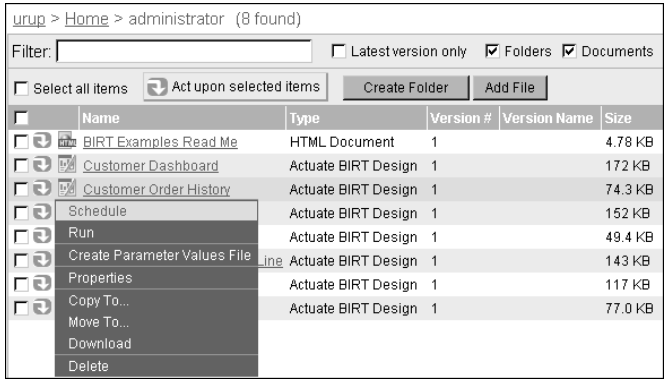

Figure 5-7 Choosing to create a scheduled job

2 On Schedule—Schedule, shown in Figure 5-8, perform the following actions:

- Accept the default job name, which is the file name, or type a new name. The job name identifies the request.
- To schedule the job for a time zone that differs from the current time zone, select a new time zone.
- Specify running the design right now, once or on a recurring basis, or when an event triggers the job, by selecting one of the following options:
  - Right now

- Once
- Recurring
- Advanced
- Wait for Event

- Specify the job priority as low, medium, or high, or assign a priority number.
- Select an executable version option as follows:
  - To use the most recent version, select Always use latest version.
  - To use a specific version of a design, select Always use version number, then type the version number.
- Select a retry option for failed jobs, such as Use the volume default, or specify whether to retry, the number of times, and the number of hours and minutes to wait.

The job runs at the specified time unless prevented by the priority level of your jobs, the availability of iServer processes for generating documents, or the number of jobs in the queue. iServer saves the resulting document in your Home folder if you have one. Otherwise, iServer saves it either in the folder containing the design, or in the folder you specify in Schedule—Output.

About job priority and resource groups

Job priority is one factor that determines how iServer processes jobs. The administrator can set the maximum job priority for each user. If a user selects a job priority that is higher than this maximum, iServer runs the job at the assigned maximum priority level.

A user submitting a job request can also affect when a job executes by specifying a resource group. A resource group is a reserved set of Factory processes in an iServer instance. The administrator can set minimum and maximum priority levels for an asynchronous resource group to expedite job scheduling.

A job with an assigned resource group has priority over a job with no assignment. When two jobs have the same priority, if one job has a resource group assignment and the other does not, the job with the resource group assignment executes first.

If you do not assign a resource group to a job, depending on the type of design the job runs, iServer assigns the job one of the following default resource groups:

- Default BIRT Factory
  Runs a BIRT or BIRT Spreadsheet design as a scheduled job
- Default BIRT Online
  Runs a BIRT or spreadsheet design unscheduled

- Default BIRT Studio
  Used when creating, modifying, and viewing documents using BIRT Studio
- Default BIRT eSS Factory
  Runs a BIRT Spreadsheet design (.sox) or template (.vtf, .vtx) as a scheduled job
- Default BIRT eSS Online
  Runs a BIRT or BIRT Spreadsheet design or template (.vtf, .vtx) unscheduled
- Default BIRT 360
  Runs a BIRT dashboard (.dashboard) or gadget (.gadget) design unscheduled
- Default BIRT Data Analyzer
  Runs a BIRT Cube View (.cubeview) or Data Object Store (.data) design unscheduled
- Default Async
  Runs a design created using e.Report Designer Professional as a scheduled job
- Default Sync
  Runs a design created using e.Report Designer Professional unscheduled
- Info Object Web Services
  Accesses Actuate information object data through a web service

The administrator can create any number of resource groups to run a particular design type. When you schedule a job to run a design, you select from the resource groups available to run that design type in Resource Group on Schedule—Schedule, as shown in Figure 5-8.

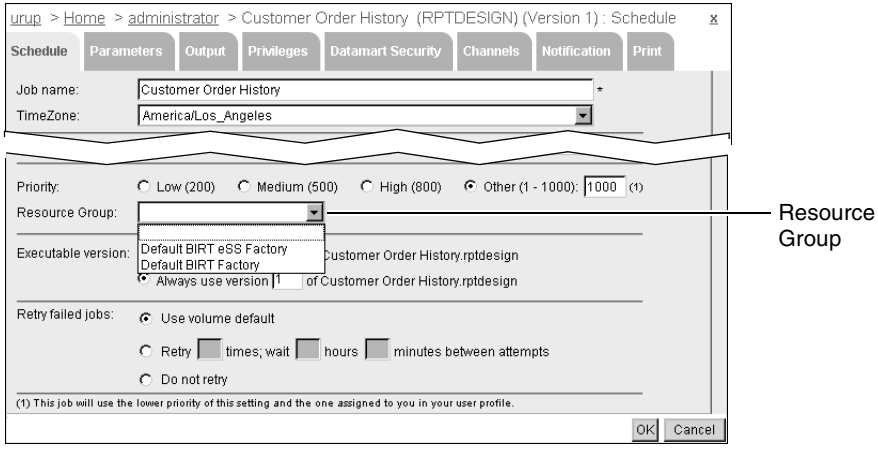

Figure 5-8 Selecting a resource group

If a user submits a scheduled job without assigning the job a resource group, and the priority level the user selects for the job is outside the range the default resource group assigned to the job specifies, the job is pending until the administrator changes the default resource group priority range to include the job priority level.

About retrying a failed job

When scheduling a job, you can specify that iServer run the job again if it fails. The volume-level job retry policy specifies the default policy for all jobs on the volume. When you schedule a job, you can accept or override this policy by setting one of the following options in Retry failed jobs on Schedule—Schedule, as shown in Figure 5-9:

- Use volume default
  Use the volume-level retry settings.
- Retry *n* times; wait *n* hours *n* minutes between attempts
  Specify how many times iServer should retry running the job and how long the system should wait between tries.
- Do not retry
  Make no retry effort.

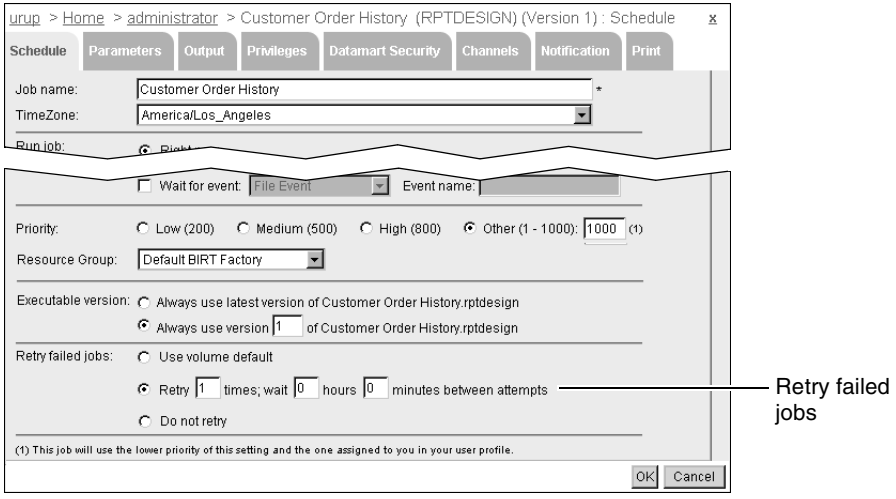

Figure 5-9 Selecting a job retry option

The following conditions affect a job retry policy:

- Retry settings do not apply to jobs that you schedule to run right now.
- For Retry N times, wait H hours M minutes between attempts.

When N is not 0 and H and M are 0, the Encyclopedia volume resubmits the job immediately after a failure.

- iServer cancels a new instance of a scheduled job, with an appropriate message, if the previous instance is still retrying.

  The retry count (N) for the existing instance does not increase.

Setting the Encyclopedia volume job retry policy

You can configure a job retry policy for the Encyclopedia volume, which regulates the repeating attempts to run scheduled jobs that fail, as shown in Figure 5-10. Only the administrator can change the volume job retry policy.

How to set the Encyclopedia volume default job retry policy

1. On Volume, choose Properties.
2. On Properties—General, specify the default job retry policy, then choose OK.

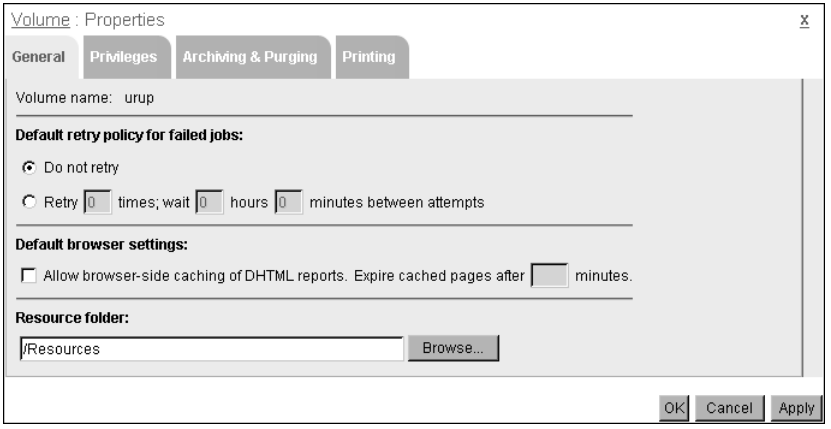

Figure 5-10 Specifying the default job retry policy

Specifying parameters

Parameters are variables that you provide as input to the execution of a design. If the design contains parameters, you can set parameter values on Schedule—Parameters, as shown in Figure 5-11.

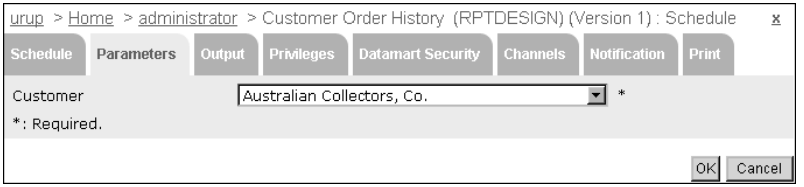

Figure 5-11 Setting parameter values on Schedule—Parameters

Schedule—Parameters does not include the Save option, as Run—Parameters does, because iServer saves all scheduled jobs after they run.

Hidden parameters do not appear on Parameters. iServer identifies each parameter by type, such as string, optional, or required. Parameter values typically influence the data appearing in the output document.

If you do not set any parameter values, iServer uses the default values set by the design developer.

How to specify parameters

On Schedule—Parameters, specify parameter values if the design you are running requires them.

Saving parameter values for reuse

You can save a set of parameter values in a parameter values (.rov) file to avoid having to set the parameter values every time you run a design. You can run the parameter values file or schedule a job to run the file.

How to create and use a parameter values file

1 To create a parameter values file in an Encyclopedia volume, on Files and Folders, point to the arrow next to a design file name and choose Create Parameter Values File, as shown in Figure 5-12.

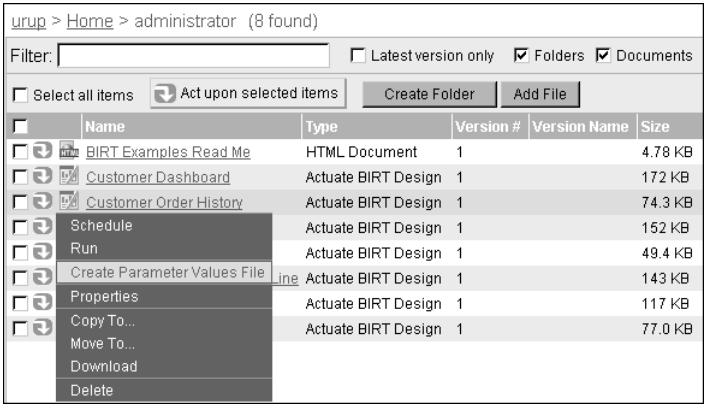

Figure 5-12 Creating a parameter values file

Create Parameter Values File appears, as shown in Figure 5-13.

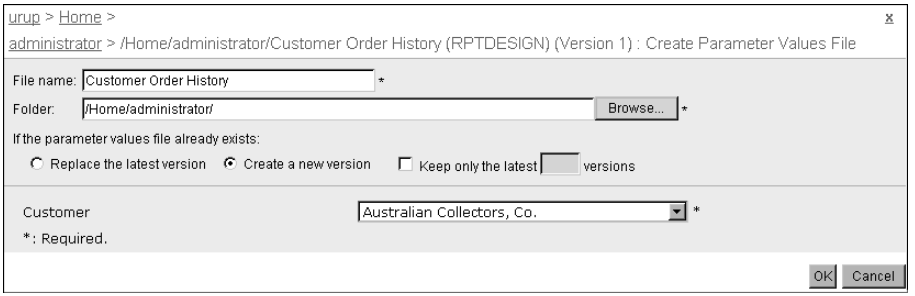

Figure 5-13 Specifying parameter values file properties

2 Specify the following values for the options:

- File name, location, and version information
- Parameter values

Choose OK. Management Console returns to Files and Folders, where the parameter values file now appears in the list of files and folders.

3 To generate a document using a parameter values file, point to the arrow next to the file name, then choose Schedule or Run.

Specifying output settings

On Schedule—Output, shown in Figure 5-14, set properties, such as the document name, output file format, and where to save the file. You can also configure versioning and archiving.

Table 5-3 describes the properties you can set on Output.

Table 5-3 Schedule—Output settings

Property	Description
Document name	The name of the document. You can enter a new name or accept the default. This is a required field. Typing a file extension does not determine the file type. The Document format setting determines the file type.
Document format	Specify the output document format as follows: ■ The format to which you save the output of a BIRT design or convert a BIRT document

(continues)

Table 5-3 Schedule—Output settings (continued)

Property	Description
Document format *(continued)*	■ The format to which you save the output of a BIRT spreadsheet design or convert a spreadsheet document ■ A format, listed in Table 5-5, to which you save the output of an ROX or DOX
Version name	The version name of the output document.
Headline	The headline for the output document. This setting is for scheduled jobs only.
Folder	Specify whether to save the generated document to: ■ The home folder, which iServer pre-selects, if you have a home folder ■ The folder in which the design resides ■ A folder that you specify
Version control	If the file already exists in the volume, specify how to handle multiple versions as follows: ■ Replace the latest version. ■ Create a new version. You can also select whether to keep only the latest *n* versions, where *n* is a number from 1–99.
Autoarchive policy	Set a job-specific autoarchive policy as follows: ■ Use the default/inherited policy from the document's file type. This is the default selection. ■ Do not automatically delete the output file. ■ Specify the age after which to delete in days and hours. ■ Specify a date and time after which to delete. ■ Specify that iServer archive the output document before deleting it.
View Policy	View the current autoarchive policy for the output document file type.
Embed the executable into the document	If scheduling a job to run an Actuate report executable (.rox), you can specify whether to bundle the executable into the document.

How to specify output settings

On Schedule—Output, shown in Figure 5-14, specify the following basic output file properties:

- Accept the default document format, or select a format for the document.
- Supply a version name.
  You can use a date-and-time expression in Version name. The expression evaluates to the date on the output document.
- Specify how to handle an existing version of the document when iServer creates the new version.
- Specify the autoarchive policy for the output document.
  If you specify a time-based or date-based autoarchive policy option, and you also have an autoarchive driver defined for the Encyclopedia volume, Management Console enables the Archive the document before deletion option.
- Select Embed the executable into the document if you want to bundle the Actuate report executable file and the document.

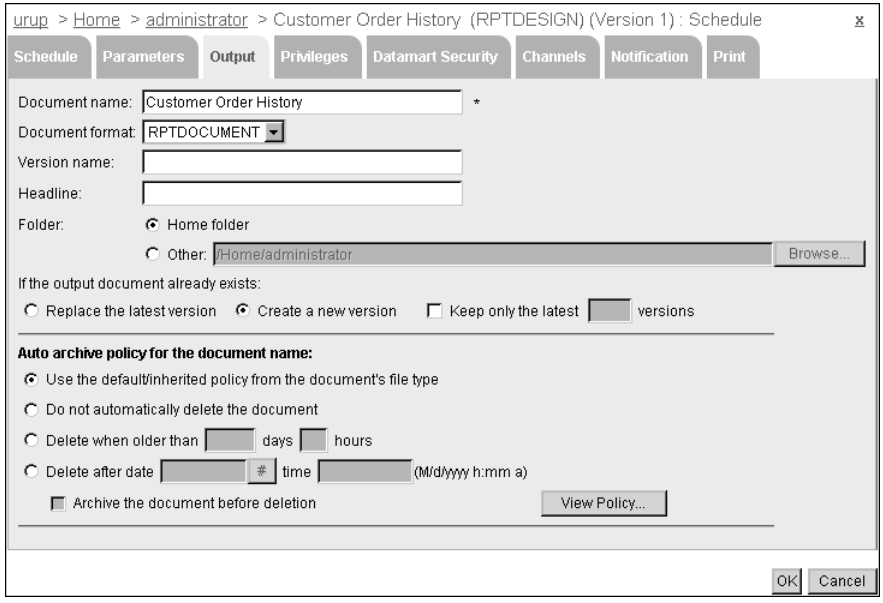

Figure 5-14 Specifying output file properties on Schedule—Output

Bundling an ROI file

When scheduling a job to run an Actuate report executable (.rox) file, Schedule—Output contains an option to embed the ROX in the resulting document, as

shown in Figure 5-15. Running the job with this option selected creates a bundled ROI. Embedding is useful and recommended only if you must send the ROI as an e-mail attachment.

The recipient of the e-mail can upload the bundled file to the Encyclopedia volume, then run the ROX and view the ROI. Bundling interferes with demand paging, a feature that makes parts of the document visible even while it is being generated.

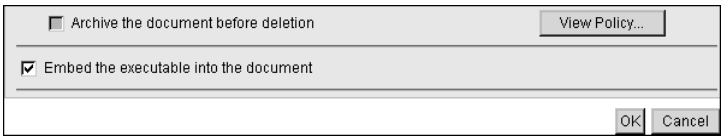

Figure 5-15 Choosing to embed the ROX in the generated document

Specifying a headline

You can specify a headline that becomes a component of the job completion notice that iServer writes to a channel. iServer copies the value you enter in Headline to the Headline field of the notice.

The value you enter for Headline replaces the original value of the headline for this run only.

About the file format of a document

Use the Document format on Schedule—Output, shown in Figure 5-16, to select one of the output formats described in Table 5-4 or Table 5-5.

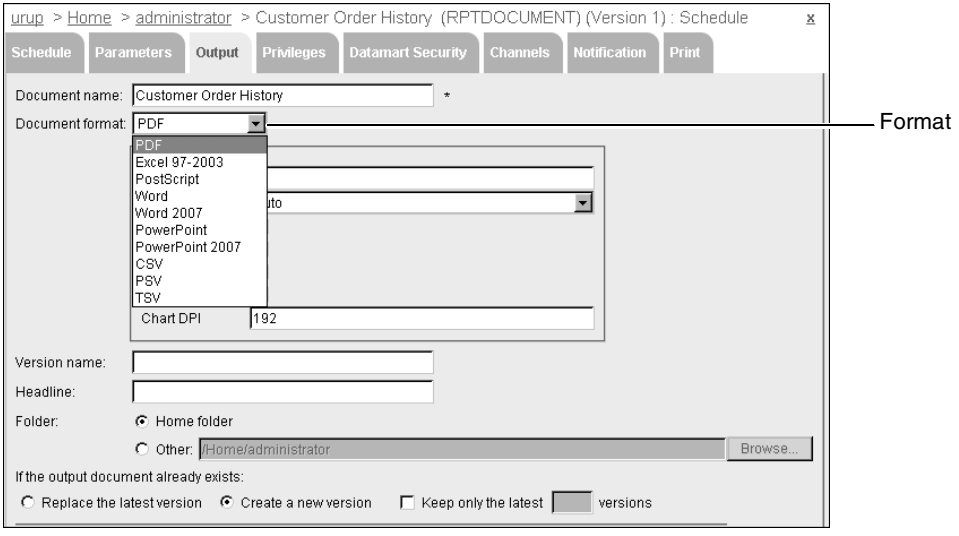

Figure 5-16 Possible file formats for output from a BIRT design

Converting file format of a BIRT or spreadsheet document

By default, when you run a BIRT design (.rptdesign), iServer converts it to a BIRT document (.rptdocument). You can also convert the document file to one of the file formats listed in Table 5-4.

Table 5-4 Document formats for a BIRT document

Output format	Option	Description
CSV, PSV, and TSV	Table name	Selects the name of the data set, which the design uses, from the list of all data sets in the data source.
	Column list	Selects the name of the column, which the design includes in the result, from the names of all columns in the data set.
	Export columns data type	Selected puts the data type of the column in the second row of the output file.
	Locale neutral format	Selected formats date and time according to ISO 8601. The date is formatted YYYY-MM-DD. The time is formatted HH-MM-SS using the 24-hour clock, and includes an offset from UTC time.
	Encoding	Sets either UTF-16LE or UTF-8 encoding of the output data.
	Maximum rows	Sets the maximum number of rows in the output file.
Excel 97-2003	Page range	Selects all pages or selected pages by number or by range, or both.
	Text wrapping	Selected wraps text. Deselected displays on one continuous line.
	Enable pivot table	Selected enables the user to create customized summaries using the data in the document.
	Chart DPI	Selects dots per inch, which determines the resolution of images and print in the document.
	Export charts as images	Selected converts charts to images in the document. Useful when you want only to print the document.

(continues)

Table 5-4 Document formats for a BIRT document (continued)

Output format	Option	Description
PDF, PostScript, or PowerPoint	Page range	Selects all pages or selected pages by number or by range, or both.
	Page style	Sets the size to either the actual size, fit to page width, or fit to whole page.
	BIDI processing	Selected suppresses bi-directional processing of data.
	Text wrapping	Selected wraps text. Deselected displays on one continuous line.
	Font substitution	Selected substitutes fonts on the user's computer in lieu of the fonts specified by the design designer. Deselected prevents font substitution.
	Embedded font	Selected allows font embedding, which ensures that fonts display and print in the way the designer intended from one system to another. Applies to PDF only.
	Chart DPI	Selects dots per inch, which determines the resolution of images and print in the document
Word	Page range	Selects all pages or selected pages by number or by range, or both.
	Chart DPI	Selects dots per inch, which determines the resolution of images and print in the document.

You can also convert a spreadsheet document (.soi) or executable (.sox) file to Excel. You schedule a job to run the spreadsheet design, and select Excel 97-2003 or Excel 2007 in Document format on Schedule—Output. You can specify the conversion of either all pages or selected pages by number or by range. When you schedule a BIRT design (.rptdesign) file to run, the Document format list on Schedule—Output does not contain comma-, pipe-, and tab-separated value (CSV, PSV, or TSV) output formats. When you schedule a BIRT (.rptdocument) document to run, however, the document format list contains these output formats.

How to convert a BIRT document to CSV format

1 Navigate to the example designs in /Public/BIRT and BIRT Studio Examples. Point to the arrow next to a design, such as Employee Directory, and choose Schedule, as shown in Figure 5-17.

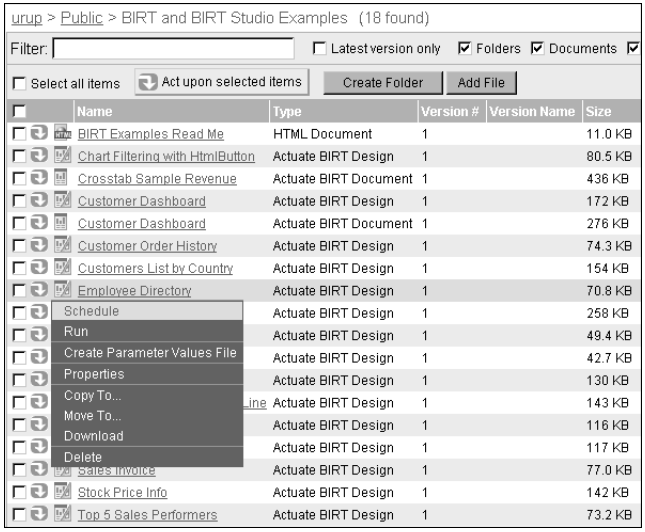

Figure 5-17 Choosing to schedule a BIRT design to run

2 Choose OK to accept the default settings on Schedule and run the design right away.

3 Navigate to your Home folder, as shown in Figure 5-18.

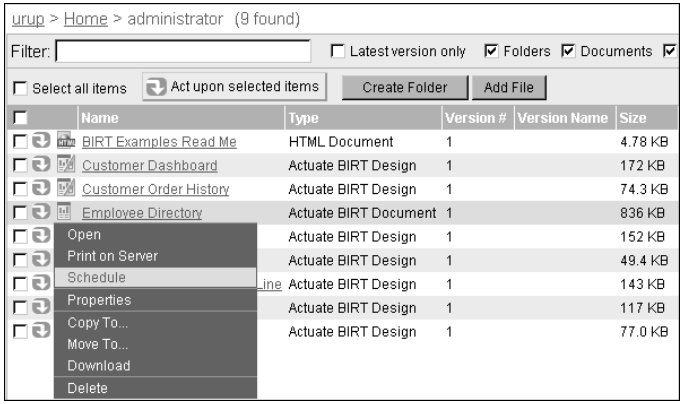

Figure 5-18 Choosing to schedule a format conversion job

The output document, Employee Directory, appears after the scheduled job runs.

Point to the arrow next to Employee Directory and choose Schedule.

On Schedule, choose Output.

4 On Output, perform the following tasks:

1 In Document format, select CSV, as shown in Figure 5-19.

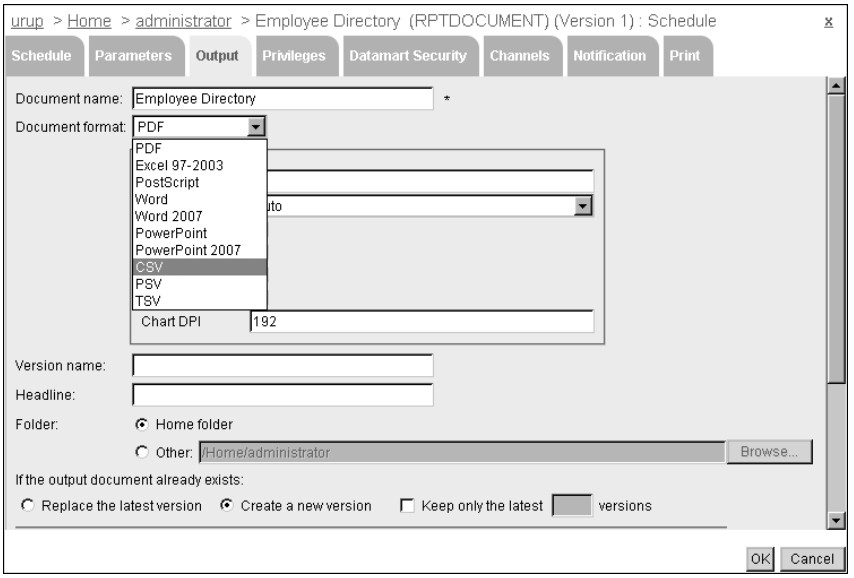

Figure 5-19 Selecting the CSV output format

The conversion options for CSV appear, as shown in Figure 5-20.

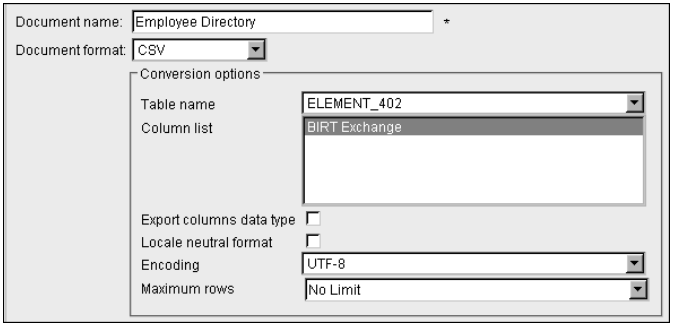

Figure 5-20 Viewing the conversion options for CSV

2 In Table name, select Managers, as shown in Figure 5-21.

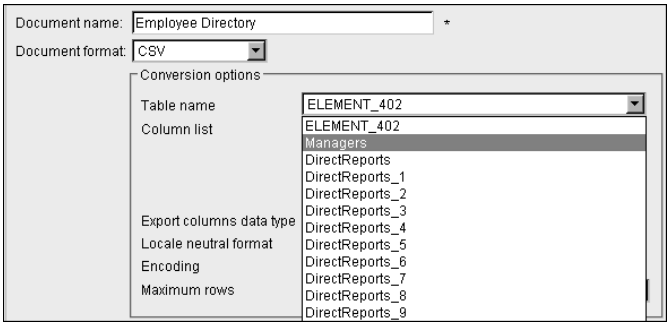

Figure 5-21 Selecting a table name

The list of columns in the Managers table appear, as shown in Figure 5-22.

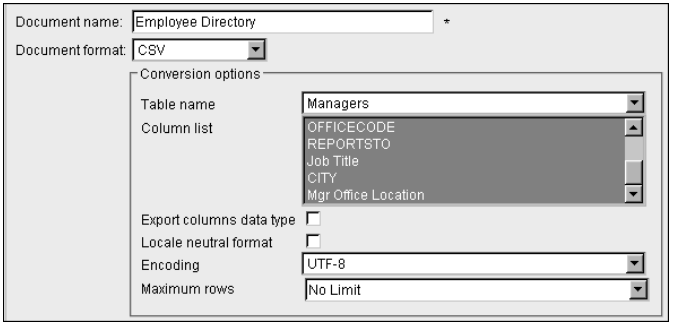

Figure 5-22 Viewing the list of columns in the Managers table

3 Select FIRSTNAME, hold down the CTRL key and select the EMAIL column. Select Export columns data type, as shown in Figure 5-23. Accept other defaults on Output.

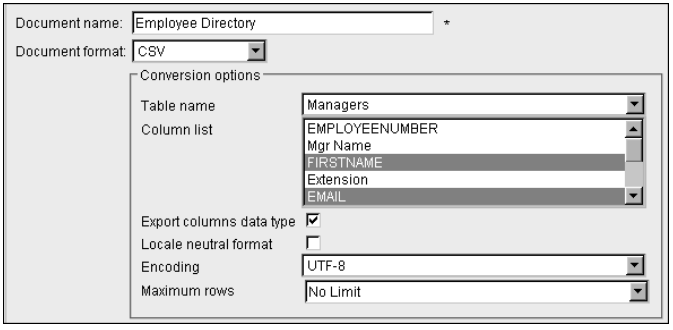

Figure 5-23 Selecting CSV conversion options

Choose OK.

5 Choose Jobs from the side menu, choose Completed, and then select Employee Directory.CSV, as shown in Figure 5-24, from the list of documents.

Figure 5-24 Finding the CSV output file

If you save Customer.CSV on your hard drive and open it in Notepad, you see the comma separated list.

If you open Customer.CSV in Excel, you see the list formatted in Excel columns.

Converting the file format of an Actuate Basic document

Table 5-5 lists the possible Document format settings on Schedule—Output for an Actuate Basic document.

Table 5-5 Document formats for Actuate Basic design output

Output format	Description
Excel Data	A format used mainly for tabular or listing documents. When you export data to Excel, you cannot preserve both the data type and the format. Use this format to export the data and preserve its data type in Excel. To preserve format, use Excel Display for exporting. Generally, the more complicated the document, the greater the discrepancy in the formatting. For example, images and graphs do not appear, background colors of frames and flows are ignored, and component positioning is inaccurate. Also, datetime data is exported as the datetime data type, but the data display might not appear the same in Excel. For example, in the English (United States) locale, a Date Time control that displays the mm/dd/yy h:nn:ss AM/PM format in a document appears in the m/d/yyyy h:mm format in Excel.
Excel Display	A format that resembles, as closely as possible, that of an Excel spreadsheet. The format of the output data is the default Excel format.
Fully Editable RTF	Rich Text Format with more flexibility for manipulating output, such as the ability to move and delete several lines from a document simultaneously. A file in this format is larger than one in the standard RTF format.
PDF	An Adobe Acrobat-readable Portable Document Format (.pdf) file.

Table 5-5 Document formats for Actuate Basic design output

Output format	Description
PowerPoint	A Microsoft PowerPoint (.ppt) file.
ROI	The standard Actuate Basic document format, a report object instance (.roi) file. ROI is the default output format.
RTF	A Rich Text Format (.rtf) file. The document's visual layout is similar to the DHTML viewer layout.

Setting privileges for an output document

Use Schedule—Privileges to assign privileges on the output document. The tasks in Table 5-6 require a combination of privileges.

Table 5-6 Tasks that require a combination of privileges

Task	Privileges
Run a design.	Read and execute
Overwrite an existing version of an output document.	Visible and delete
Assign or revoke access to a document.	Visible and grant

How to set job privileges

On Schedule—Privileges, perform the following tasks:

1. Select Roles or Users to see the security roles and users from which to select in Available.
2. Move roles or users from Available to Selected, as shown in Figure 5-25.

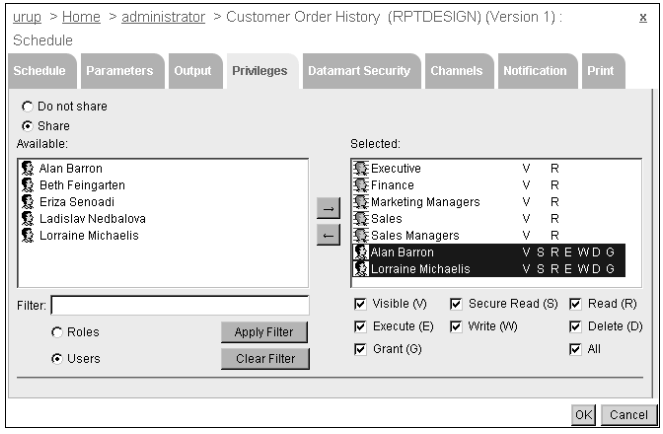

Figure 5-25 Assigning privileges on job output to roles and users

3 Assign privileges by selecting from the list of privileges such as Visible, Execute, or Read.

4 Cancel all privilege assignments for this job by selecting Do not share.

Select Share to reinstate assigned privileges.

About Datamart Security

Datamart Security supports filtering the data a scheduled job generates. Datamart Security is available to the administrator. Select one or more roles or users on Datamart Security before submitting the job. The document the job generates contains only the data that the selected roles or users have permission to view.

Optionally, in Custom role, specify a string that the design recognizes and can also use to filter data the job generates.

For more information about page-level security development, see *Using BIRT iServer Integration Technology.*

How to configure Datamart Security

1 Select Roles or Users to see the security roles and users from which to select in Available.

2 Move roles or users from Available to Selected, as shown in Figure 5-26.

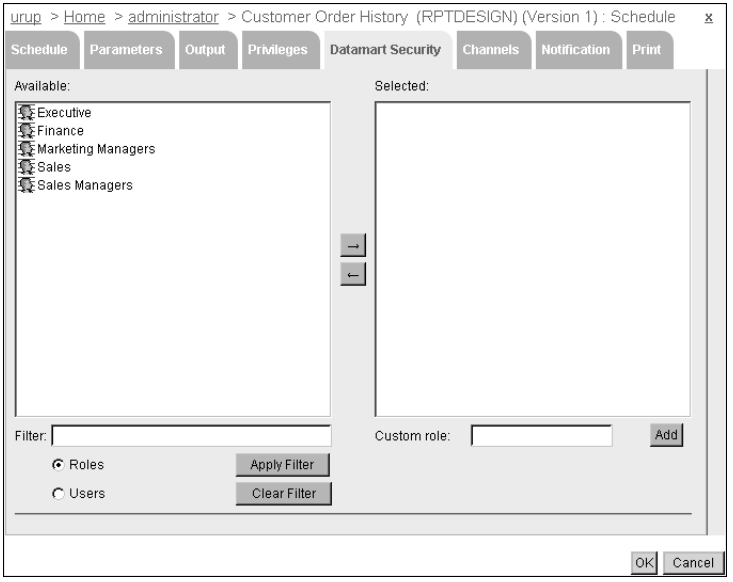

Figure 5-26 Selecting roles or users for which to filter job output

3 Optionally, enter a string in Custom role. Select Add to add the string to Selected.

Setting channel options

In Management Console, you can distribute an output document to roles and users by sending a job notice to one or more channels. For a job that runs successfully, the job notice contains the document. A user who has read privilege to a channel containing the job notice can access the notice. The administrator must subscribe the user to the channel containing the notice for the user to access the notice in Information Console.

How to set channel options

On Schedule—Channels, perform the following tasks:

1 Select a channel on which to view a job notice by moving the channel from Available to Selected, as shown in Figure 5-27. Channels displays only those channels to which the user who initiates the run request has write access.

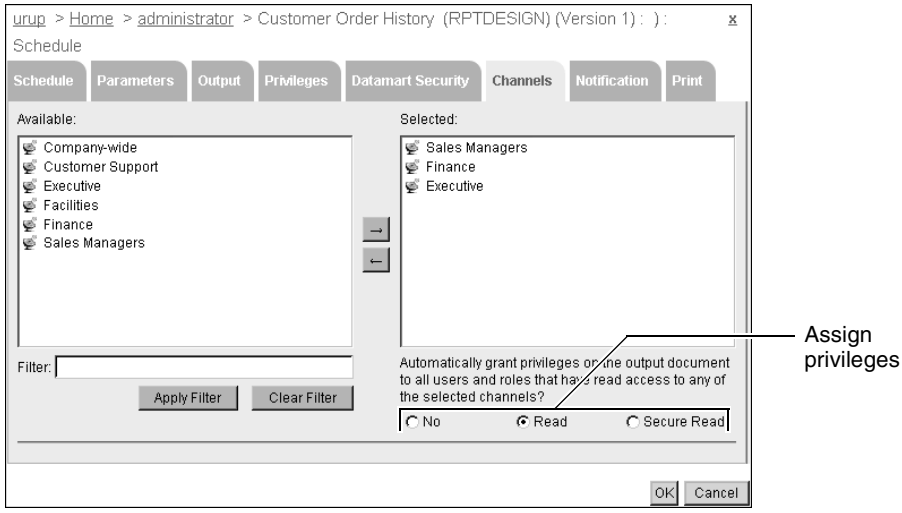

Figure 5-27 Selecting channels on which to view a job notice

2 Grant viewing privileges to all users and roles that have read access to any channel in Selected by selecting Read or Secure Read.

Notifying users about a job

When scheduling a job, in addition to using channels to notify users of job completion, you can also use notification groups for this purpose.

How to inform users of job completion using notification groups

On Schedule—Notification, perform the following tasks:

1 Select Groups or Users to view the notification groups and users from which to select in Available. Use Filter to see subsets of groups or users in Available.

2 Move selected groups or users from Available to Selected, as shown in Figure 5-28. iServer sends notification of job completion to the members of the groups and to the individual users that you select.

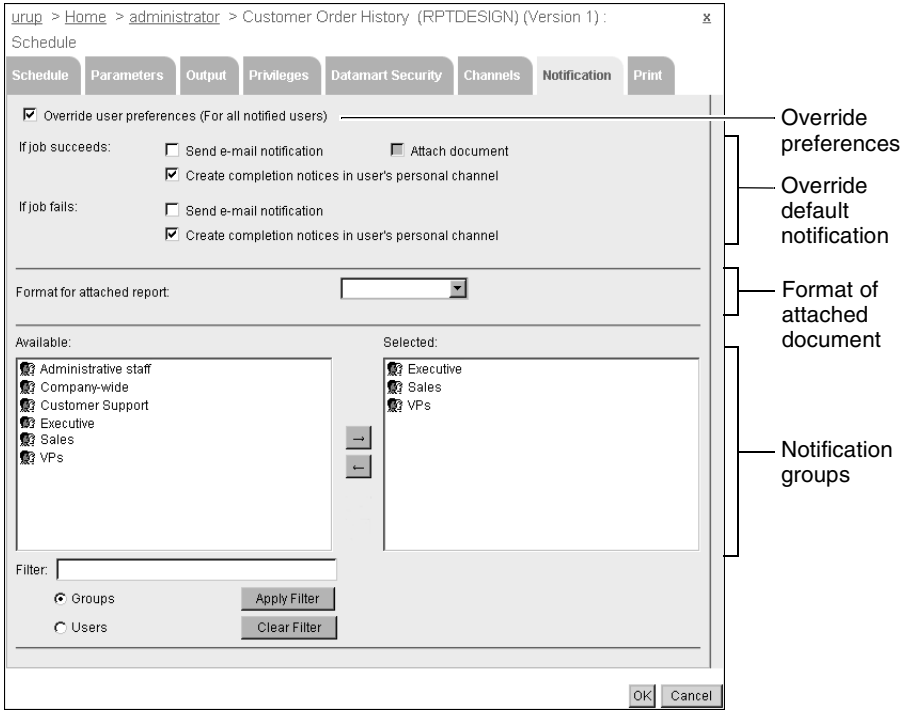

Figure 5-28 Selecting groups and users to notify of job completion

3 You can specify the means by which users receive job completion notification by selecting Override user preferences. Doing so overrides the settings that a user specifies in Personal Settings—Jobs for jobs that succeed and for jobs that fail. For either type of job, you can make the following selections:

- Send e-mail notification

  The user receives notification of job completion by e-mail. You can select Attach document to send the document as an attachment to the e-mail message. The user must have read privilege on the document. If the user does not have read privilege, only the location of the document appears in the e-mail. If you select Attach document, you must select a value for Format for attached report if a value does not appear there. Format for attached report is blank if you accept the default value for Document format on Schedule—Output.

- Create completion notices in the user's personal channel

  iServer sends a job completion notice to the user's personal channel. If the job succeeds, the notice contains the output document. In Schedule—Privileges, you must give the user Secure Read or Read privilege on the document to enable the user to view it.

Printing a document

Use Schedule—Print to control how iServer prints the output document after generating it. If you want to print the document, either by sending it to an iServer printer or printing it to a file on the server, you must first select Print the output document on the server. This setting enables the other options on Print. In Override default settings, accept the default values, or choose to override the default settings for any of the print options.

Figure 5-29 shows Schedule—Print as it appears when choosing to print a BIRT document. The print format: Postscript section contains a number of options, including Page Range, Page Style, and Chart DPI. When choosing to print Actuate Report Executable (.rox) output, an option with which to select a page range appears in place of Print format: Postscript, as shown in Figure 5-30.

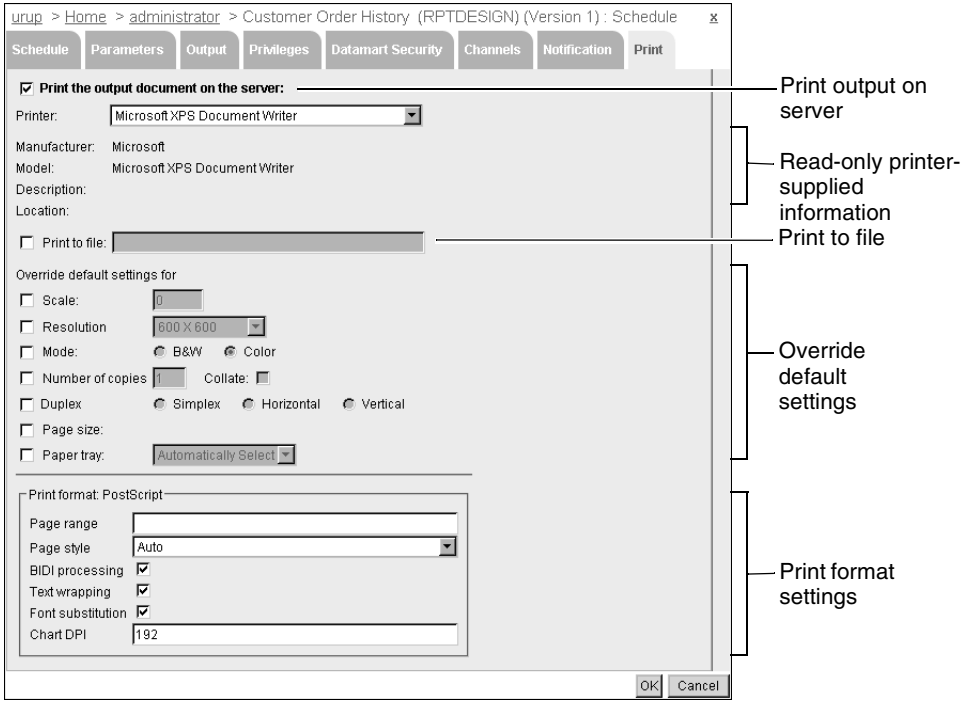

Figure 5-29 Selecting options on Schedule—Print for printing a BIRT document

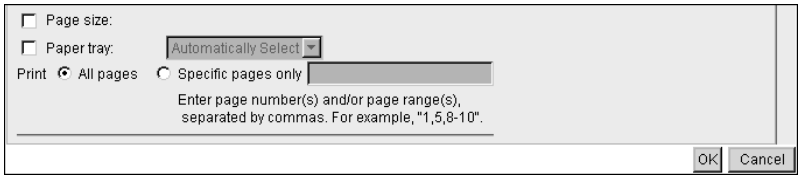

Figure 5-30 The bottom of Schedule—Print when printing the output of a ROX

Table 5-7 lists the various print options on Schedule—Print.

Table 5-7 Schedule—Print properties

Property	Description
Print the output document on the server	Prints the output document.
Printer	Selects a printer. The initial value is the user's default printer.
Manufacturer Model Description Location	The following read-only text about the printer, if available: ■ The manufacturer's name ■ The printer model name ■ A description of the printer ■ The location of the printer
Print to file	Creates a PostScript (.ps) file. Provide a file name.
Scale	The scale at which to print the output, expressed as a percentage.
Resolution	Resolutions at which to print the output, if supported.
Mode	Black-and-white or color.
Number of copies Collate	The number of copies to print, and whether to collate the copies.
Duplex	Single-sided or double-sided, and specifies whether double-sided printing is top-to-top or side-to-side.
Page size	Pick from an extensive list of standard paper sizes.
Paper tray	Specify the paper source.
Page range (BIRT design or document only)	Selects all pages or selected pages by number or by range, or both.
Page style (BIRT design or document only)	Sets the size to either the actual size, fit to page width, or fit to whole page.

Table 5-7 Schedule—Print properties

Property	Description
BIDI processing (BIRT design or document only)	Selected suppresses bi-directional processing of data.
Text wrapping (BIRT design or document only)	Selected wraps text. Deselected displays on one continuous line.
Font substitution (BIRT design or document only)	Selected substitutes fonts on the user's computer in lieu of the fonts specified by the design designer. Deselected prevents font substitution.
Chart DPI (BIRT design or document only)	Selects dots per inch, which determines the resolution of images and print in the document
Print (ROX only)	Specify to print all pages, or alternatively, specific pages, a range of pages, or both.

How to set print options and print a document

To print a document, choose Schedule—Print, and select Print the output document on the server. Select the printer to use and specify standard print options, such as scale, number of copies, and page range to print.

When you finish specifying the schedule and the parameters, output, privileges, and channels associated with scheduling the job, choose OK.

Understanding service requirements

Running jobs in an Encyclopedia volume requires the following iServer services, which the installation program configures by default:

- View and Factory services for running designs unscheduled
- The Factory service for running scheduled jobs
- A web service based on a custom web service event for scheduling jobs

iServer must have access to a printer to print the output of a scheduled job.

The install program configures access to printers in Windows, but not in UNIX. You reconfigure some iServer services, such as the View and Factory services, using Configuration Console.

Troubleshooting problems

Missing file dependencies and insufficient privileges are common causes of problems with viewing documents and running designs. For example, if you upload an Actuate report document that does not embed its report executable,

and does not have a related report executable in the Encyclopedia volume, the browser displays an error message when you try to view the report document, as shown in Figure 5-31.

Figure 5-31 Error message indicating dependency problem

If a parameter values file (.rov) does not have a dependency set to a design file of the same name, iServer displays the error message shown in Figure 5-32 if you try to schedule a job to run the ROV.

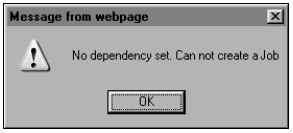

Figure 5-32 Error message when running an ROV file with a missing dependency

Solving a dependency problem

The procedure in this section describes how to set a dependency between files to avoid a dependency problem.

How to set a dependency on an Actuate report executable file

1 On Files and Folders, point to the arrow next to the report document file name and choose Properties, as shown in Figure 5-33.

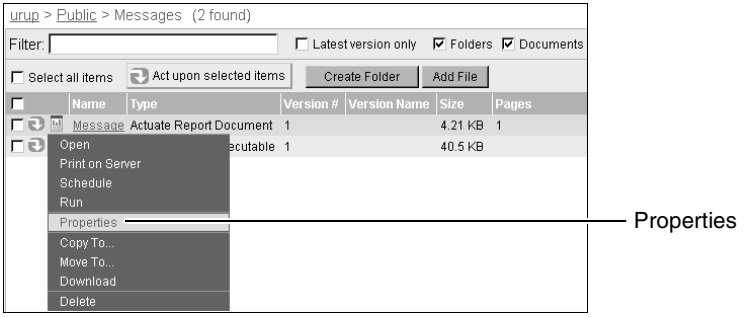

Figure 5-33 Choosing properties for a report document

On Properties, choose Dependencies.

2 On Dependencies, choose Add.

3 To make the report document dependent on the report executable, on File Browser, select the report executable and choose OK.

Dependencies appears with the added dependency, as shown in Figure 5-34.

Figure 5-34 Adding a dependency on an executable to a document

4 On Properties, choose OK.

Solving a privilege problem

To avoid an access problem when a user runs a design, the administrator must assign the following privileges and license options to the user:

- Execute and read privilege on the design
- The BIRT option for running a BIRT design, the e.Report (Actuate Basic Report) option for running an Actuate Report Executable (.rox).
- To enable a user to run a parameter values file (.rov), you must assign the user the following privileges:
  - Read and execute privileges on the design from which a user creates the ROV or on which the ROV depends
  - Read privilege on the ROV
- Write privilege on the folder to which iServer writes the document
- Write privilege on the channel to which the user submitting a job sends the job completion notice

The job submitter and the administrator can cancel a job. Users can get or delete information about a job the user submits from Jobs.

Only the administrator can cancel and get the information about a job of another user.

Bursting a document

Unscheduled run requests do not support document bursting. A design that uses bursting generates other documents, and iServer cannot determine which document to display. An execution-failed error message appears. Schedule a job to run such a design.

Using a date-and-time expression in a document or version name

When you submit a run or schedule request, you can specify a document name and a version name for the generated document. You can also incorporate a date-and-time expression in the name, so when you schedule a design to run on a recurring basis, the date-and-time expression creates unique document or version names.

For example, to display a document called Sales to date using the document generation date as a part of the document name, use the following expression:

```
Sales to date {mm-dd-yy}
```

On February 28, 2010, the name appears as:

```
Sales to date 02-28-10
```

You can create date-and-time expressions by using the predefined date-and-time formats in the locale map of Management Console or Information Console. Alternatively, you can create your own date-and-time formats.

About the locale maps

Add your own custom date-and-time formats to the following locale maps for iServer, Management Console, and Information Console:

- AC_SERVER_HOME\etc
- AC_SERVER_HOME\servletcontainer\mgmtconsole\WEB-INF
- AC_SERVER_HOME\servletcontainer\iportal\WEB-INF

iServer uses its own version of localemap.xml in determining the formatting that appears in an Actuate Basic report document.

Management and Information Console use their own versions of localemap.xml in determining the formatting that appears in their respective user interfaces, such as the date and time format.

About predefined date-and-time formats

You can include predefined date-and-time formats in a file name by using a keyword. Exact order and output depends on the locale. Table 5-8 lists the predefined date-and-time format keywords and the expression to which each keyword evaluates in a document. Examples and results that have a file-name

extension are document names. Examples and results that do not have a file-name extension are version names. The results are for the English (US) locale.

Table 5-8 Predefined date-and-time format keywords and expressions

Keyword	Description	Example	Result
General Date	Returns a date and time in the Short Date Long Time format.	{General Date}	01/23/2006 8:53:03 PM
Long Date	Returns a long date.	{Long Date}	Monday, January 23, 2006
Medium Date	Returns a date with the month name abbreviated to three letters: dd-mmm-yy.	{Medium Date}. <document extension>	23-Jan-06. <document extension>
Short Date	Returns a short date.	{Short Date}. <document extension>	01-23-2006. <document extension>
Long Time	Returns the time in a long format.	{Long Time}	8:45:00 PM
Medium Time	Returns hours and minutes in a 12-hour format, including AM/PM designation (hh:nn AM/PM).	{Medium Time}	8:45 PM
Short Time	Returns hours and minutes in 24-hour format (hh:nn).	{Short Time}	20:45

About a file name in an expression

Commas and colons in a date-and-time expression can create unexpected results in file names. For this reason, General Date, Long Date, Long Time, Medium Time, and Short Time are not recommended for use in a file name.

Creating a custom date format

You can create custom date formats. The exact output depends on the locale. iServer formats dates that appear in the Management Console user interface according to specifications in the locale map that Management Console uses.

If you update localemap.xml, you must restart the cluster nodes for the changes to take effect. You must also ensure that localemap.xml uses the correct encoding and that you store localemap.xml in the correct locations.

A locale definition in localemap.xml does not necessarily specify a value for every field. For a field with no specified value, iServer uses the default locale's value meaning for that field. If no default locale exists in the file, iServer uses a hard-coded value from the C locale.

In a cluster, the same file must reside on every iServer machine to achieve consistency among nodes.

Table 5-9 lists the date format symbols that you can use to construct a custom date format and the expression to which each variable evaluates in a document. Examples and results that have a file-name extension are document names. Examples and results without a file-name extension are version names. The results are for the English (US) locale.

Table 5-9 Date format variables

Symbol	Description	Example	Result
d	Returns day of the month without a leading zero (1-31)	Day{d}. <document extension>	Day3.<document extension>
dd	Returns day of the month with a leading zero (01-31)	Day{dd}. <document extension>	Day03. <document extension>
ddd	Returns the three-letter abbreviation for the day of the week	{ddd}.<document extension>	Tue.<document extension>
dddd	Returns the full name of the day of the week	{dddd}	Tuesday
ddddd	Returns the short date	{ddddd}	01/23/2006
dddddd	Returns the long date	{dddddd}. <document extension>	Monday, January 23, 2006. <document extension>
w	Returns the day of the week as a number, where Sunday = 1 and Saturday = 7	Weekday {w}. <document extension>	Weekday 3. <document extension>
ww	Returns the week of the year (1-53)	Week {ww}. <document extension>	Week 4. <document extension>
m	Returns the number of the month without the leading zero (1-12)	Month {m}. <document extension>	Month1. <document extension>

Table 5-9 Date format variables

Symbol	Description	Example	Result
mm	Returns the number of the month with the leading zero	Month {mm}. <document extension>	Month 01. <document extension>
mmm	Returns the three-letter abbreviation for the month's name	{mmm}. <document extension>	Jan.<document extension>
mmmm	Returns the full name of the month	{mmmm}. <document extension>	January. <document extension>
q	Returns the number of the quarter (1-4)	Quarter {q}. <document extension>	Quarter 1. <document extension>
y	Returns the number of the day of the year (1-365)	Day {y}. <document extension>	Day 23. <document extension>
yy	Returns the last two digits of the year (00-99)	Year {yy}. <document extension>	Year 01. <document extension>
yyy or yyyy	Returns all four digits of the year (1000-9999)	Year {yyy}. <document extension>	Year 2006. <document extension>
c	Returns the date variant as dddd	for {dddd}	for 01/23/2006 or for 01-23-2006

A syntax error can occur if you use certain unescaped literal characters or strings in a date expression that also uses a user-defined date-and-time format. For example, the following expression produces a syntax error described by the message in quotation marks:

```
Sales Report for MMM company as of {Date - mm/dd/yy}

"Bad format specification in token - {Date - mm/dd/yy}."
```

Creating a custom time format

You can create custom time formats. The exact output depends on the locale. iServer formats times according to specifications in the locale map for Management Console.

Table 5-10 lists the time format symbols that you use to construct a custom time format and the expression to which each variable evaluates in a document. Examples and results that have a document file-name extension are document

names. Examples and results without a document file-name extension are version names. The results are for the English (US) locale.

Table 5-10 Time format variables

Symbol	Description	Example	Result
h	Returns the hour of the day without the leading zero (0-23).	Hour {h}.<document extension>	Hour 9.roi
hh	Returns the hour of the day with the leading zero (00-23).	Hour {hh}.<document extension>	Hour 09.roi
n	Returns the minute without the leading zero (0-59).	Minute {n}.<document extension>	Minute 5.roi
nn	Returns the minute with the leading zero (00-59).	Minute {nn}.<document extension>	Minute 05.roi
s	Returns the second without the leading zero (0-59).	Second {s}.<document extension>	Second 1.roi
ss	Returns the second with the leading zero (00-59).	Second {ss}.<document extension>	Second 01.roi
tttt	This setting uses formats that are in the Management Console's locale map.	{tttt}	8:45:00 PM
AM/PM	Returns AM or am for any hour before noon and PM or pm for any hour after noon. This variable is case-sensitive.	{hh:nn:ss am /pm}	08:45:03 pm
A/P or a/p	Returns A or a for any hour before noon and P or p for any hour after noon. This variable is case-sensitive.	{h:n:s a/p}	8:45:3 p
AMPM	The default format is AMPM. This setting uses formats that are in the Management Console locale map.	{h:n:s AMPM}	8:45:3 PM

iServer returns times in 24-hour format unless you use an a.m. or p.m. format symbol. The symbol for minute is n. The symbol for month is m.

Monitoring job status

To obtain information about scheduled jobs, or those that already ran, choose Jobs from the side menu. Jobs is where you track jobs. For the administrator, all jobs are visible. For a user, only a job that the user scheduled is visible.

iServer groups job processing into five phases, represented by a set of Jobs properties. As a job progresses from one phase to another, the job name moves to the next property list. Table 5-11 describes these Jobs properties.

Table 5-11 Jobs properties

Jobs property	Description
Schedules	Jobs that will run at a later date
Waiting for Event	Jobs that will run after a system event
Pending	Jobs that are in the process queue
Running	Jobs that are running
Completed	Jobs that have run

iServer sends a job completion notice to Jobs—Completed after a scheduled job runs. A user or the administrator selects whether iServer sends a notice to a user's personal channel. If the job is successful, iServer includes a link to the output document in the completion notice, as shown in Figure 5-35. If the user deletes the output document from the folder to which the scheduled job wrote the document, iServer also deletes the link to the document from the completion notice on Jobs—Completed, but iServer does not delete any other part of the completion notice.

Figure 5-35 Viewing Jobs—Completed

iServer creates job completion notices for jobs that succeed and for jobs that fail. For each type of notice, Management Console provides property settings that support whether iServer sends a notice to a user and when iServer deletes the

notice. For every property setting pertaining to jobs that succeed, there is an identical, but separate, property setting for jobs that fail.

Setting job completion notice properties

In Management Console, a user or the administrator sets job completion notice properties in the following locations:

- On Users—Properties—Jobs, a user or the administrator specifies whether to notify a user about a completed job by sending a job completion notice to the user's personal channel, as shown in Figure 5-36. Selecting Place a job completion notice in the user's Personal Channel enables the following options, which support setting the policy for deleting job completion notices from the user's personal channel:
  - Delete notice according to volume settings
    iServer deletes the notice after the time that the job completion notice deletion policy for the volume specifies.
  - Delete notice after *n* days *n* hours
    iServer deletes the notice after the number of days and hours you specify.
  - Do not automatically delete notice
    iServer does not delete the notice from the user's personal channel.

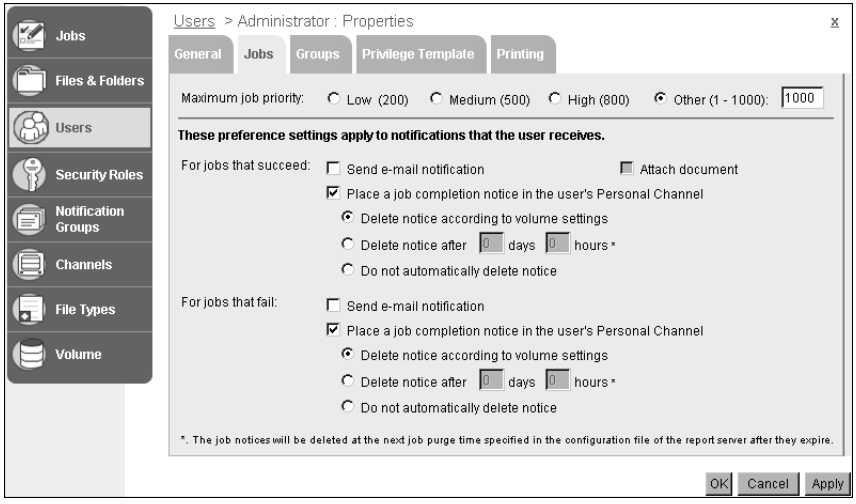

Figure 5-36 Setting completion notice properties on Users—Properties—Jobs

- On Volume-Properties-Archiving and Purging, the administrator sets the job completion notice deletion policy for the volume by selecting Purge success notices after *n* days *n* hours, or Purge failure notices after *n* days *n* hours, or both properties, then specifying the days and hours, as shown in Figure 5-37.

iServer does not purge notices if you specify 0 days 0 hours or if you do not select the property.

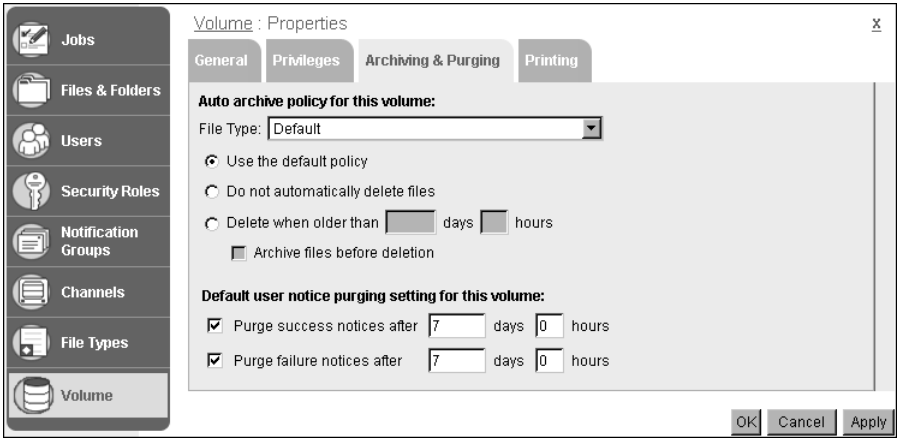

Figure 5-37 Volume—Properties—Archiving and Purging

As shown in Figure 5-38, after logging in to Configuration Console and choosing Advanced view, the administrator can set the job completion notice expiration properties by choosing System Volumes—Properties—Advanced—Archiving and Purging.

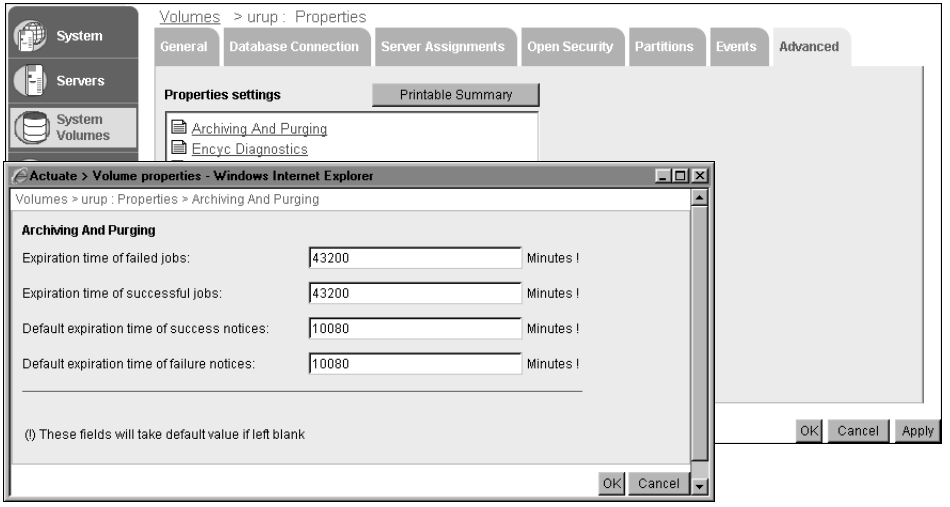

Figure 5-38 Setting properties on Archiving and Purging in Configuration Console

The following job completion notice expiration properties are available:

- Expiration time of failed and successful jobs

When no job completion notice for a particular job exists on any personal channel, iServer deletes the notice for that job from Jobs—Completed after the notice reaches this age.

- Default expiration time of failure and success notices

  The default value for the volume specifying the age that a job completion notice must reach before iServer can delete the notice from a user's personal channel. These are the same two properties as Purge success and Purge failure notices after *n* days *n* hours, in Management Console, Volume—Properties—Archiving and Purging. Setting these properties in one console sets the properties in the other console.

The default time for Expiration time of failed and successful jobs is 43200 minutes, or 30 days. The default time for Default expiration time of failure and success notices is 0 minutes.

In notifying another user when scheduling a job, if a user chooses Schedule—Notification, then selects Override user preferences and Create completion notices in user's personal channel, iServer deletes the notice according to the notified user's existing deletion policy.

iServer deletes job completion notices from a user's personal channel and from Jobs—Completed at the time the Encyclopedia volume general property Schedule for purging notices specifies, as shown in Figure 5-39. By default, this time is 2:15 A.M.

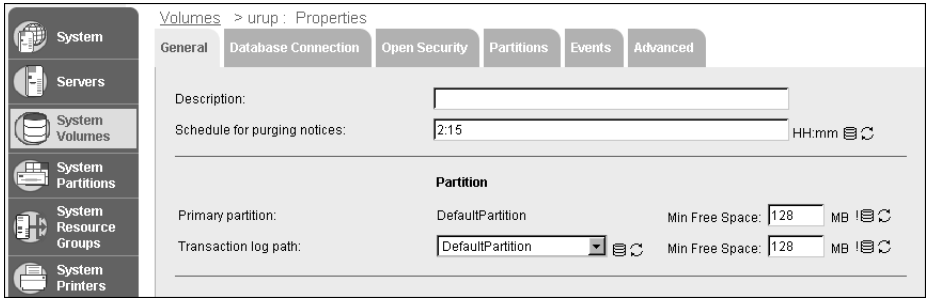

Figure 5-39 Setting Schedule for purging notices in Configuration Console

iServer deletes a job completion notice from a user's personal channel according to the deletion policy in effect when iServer ran the job. A user typically views a document and a job completion notice in Information Console. iServer cannot delete the job completion notice from Jobs—Completed in Management Console while the notice exists in a user's personal channel.

For example, if the user deletion policy is Delete notice after 2 days 0 hours, iServer deletes the notice from the user's channel after the time period expires. If another user deletion policy for the same job is 3 days 0 hours, iServer deletes that notice after that time period expires. iServer does not delete the notice from Jobs—Completed until all these personal channel job notices are deleted.

If the deletion policy for a user is Do not automatically delete, iServer does not delete the notice from the user's personal channel or from Jobs—Completed. iServer deletes the notice from Jobs—Completed after the user deletes the notice from the user's personal channel. If no personal channel contains a notice, iServer deletes the Jobs—Completed notice after the time specified by Expiration time of jobs of this type expires.

Getting detailed information about a job

A Jobs property displays basic information about that job phase. Table 5-12 lists the default information that appears on each property listing. On Options, you can modify these column settings.

Table 5-12 Default columns on Jobs properties

Jobs Property	Default column settings
Schedules	Job name Owner of the job Date and time of the next run Job priority
Waiting for Event	Job name Executable file name Owner of the job Job priority Event name Event status Event type Event parameter
Pending	Job name Executable file name Owner of the job Job priority
Running	Job name Executable file name Owner of the job Date and time the job submitted Date and time the job started

(continues)

Table 5-12 Default columns on Jobs properties (continued)

Jobs Property	Default column settings
Completed	Job name Document name Owner of the job Date and time iServer finished generating the document Number of pages in the document

On Jobs—Waiting for Event, the Event status field detects an event that meets the specified criteria to run a design.

Table 5-13 describes the possible event states.

Table 5-13 Event states

Status	Definition
Uninitialized	iServer did not start monitoring the system.
Polling	iServer is monitoring the system for matching event criteria and has not found matching criteria.
Satisfied	iServer found matching event criteria and ran the job.
Expired	iServer did not find matching event criteria within the polling interval, or a user cancelled the job.

iServer maintains status information for scheduled jobs, but not documents that iServer generates unscheduled.

How to view job details

To see more details about a job, choose a job name or point to the arrow next to a job name, then choose Details, as shown in Figure 5-40.

Figure 5-40 Getting detailed information about a job

Details—Summary displays by default. Summary lists basic information about the job, the executable file, and the output document, as shown in Figure 5-41.

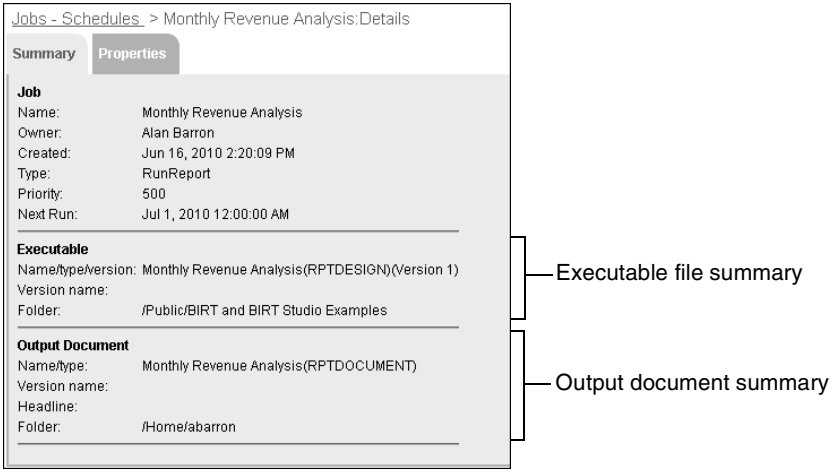

Figure 5-41 Viewing the Details—Summary page

To display additional job details, choose Properties. Figure 5-42 shows a partial view of Details—Properties.

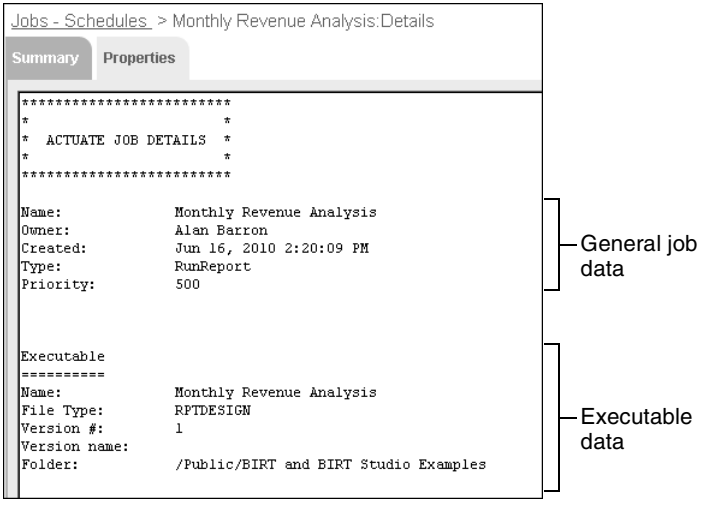

Figure 5-42 Viewing Details—Properties

Properties describes the following data for a job schedule:

- General job data, such as job name, owner, priority
- Executable file data, including file location, file type, version number

- Scheduling information, including job name, priority, retry policy
- Parameter data, including any parameters and their values
- Output settings, including output location, versioning, and archiving settings
- Privilege settings, including users and security roles having access to the output document
- Channel settings: channels to receive a job completion notice
- Notification settings, including users and security roles receiving job completion notices
- Printer settings

If you select a job from Jobs—Completed, you can view Details—Status. Figure 5-43 shows a partial view of Details—Status.

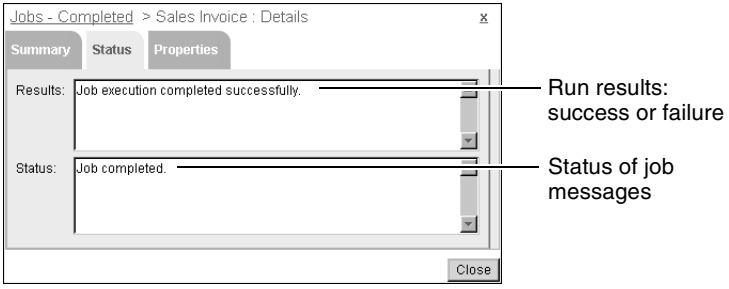

Figure 5-43 Viewing Details—Status

Editing a scheduled job

You can change the settings for any scheduled job before iServer processes it.

How to edit a scheduled job

1 Choose Jobs from the side menu, and on Jobs—Schedules, point to the arrow next to the job name. Choose Properties, as shown in Figure 5-44.

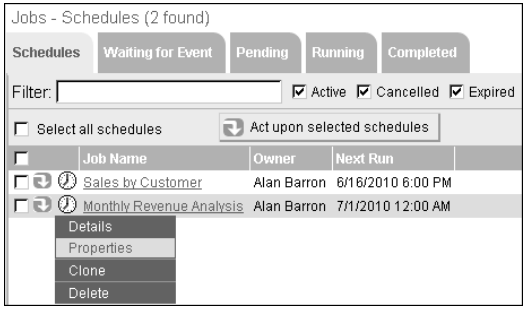

Figure 5-44 Accessing a job's Properties page

2 On Properties, make the necessary changes, then choose OK.

Cancelling a scheduled job

You can cancel or delete a job before iServer processes it. You cannot recover a deleted job. After iServer processes a job, iServer removes the job from Jobs—Schedules.

How to cancel a scheduled job

On Job Schedules—Schedules, point to the arrow next to the job you want to cancel, then choose Delete, as shown in Figure 5-45.

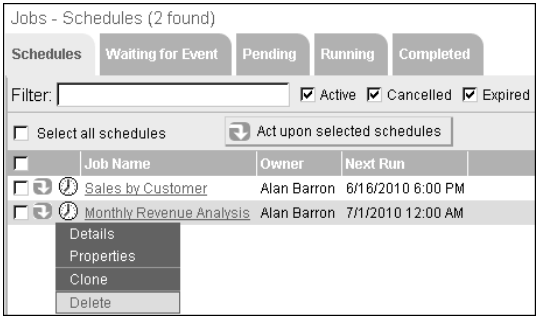

Figure 5-45 Deleting a scheduled job

You can also cancel jobs from Waiting for Event, Pending, and Running by pointing to the arrow next to the job and choosing Cancel.

When prompted, choose OK to confirm the deletion.

Deleting a job or job completion notice

When iServer finishes processing a job, it dispatches any requested completion notices, and the job appears on Jobs—Completed. You cannot recover a job completion notice after deleting it.

How to delete a job from Jobs—Completed

On Jobs—Completed, point to the arrow next to the job to delete, then choose Delete. When prompted, choose OK to confirm the deletion.

How to delete a job notice from your personal channel

1 Choose Channels from the side menu.

On Channels, choose Personal Channel.

2 On Channels—Personal Channel, point to the arrow next to the job notice to delete, then choose Delete. When prompted, choose OK to confirm the deletion.

Chapter

6

Managing channels and notification groups

This chapter contains the following topics:

- About channels
- Creating and managing channels
- Viewing a document
- Working with notification groups

About channels

A channel is a service to which users and security roles subscribe to access documents on an ongoing basis. Channels use push technology—also called push distribution or publish-subscribe—to deliver job completion notices and documents from a central server across the internet to users. In Management Console, an administrator manages channels typically to provide users access to, and control distribution of, particular types of documents.

Managing channels

An administrator uses Channels, shown in Figure 6-1, to perform the following tasks:

- Create, delete, and modify channels.
- Provide or remove user access to channels.
- Display a list of subscribers to a channel.
- View a document.

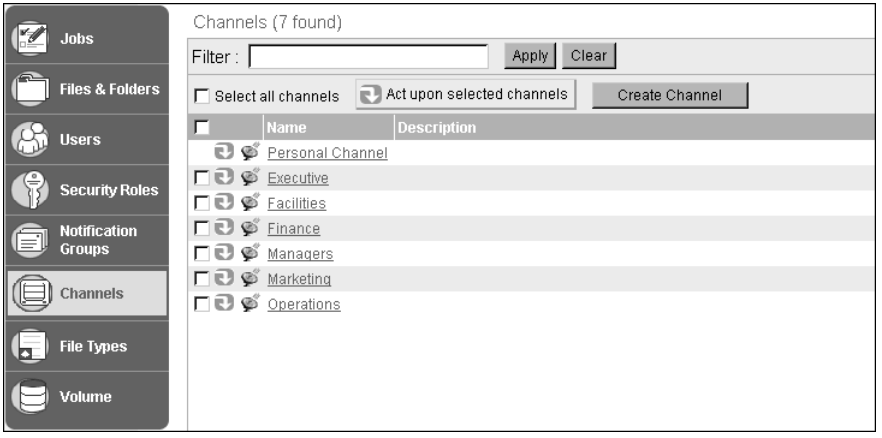

Figure 6-1 Viewing Channels

Subscribing to channels

An administrator provides and removes access to channels, and a user typically subscribes to, and unsubscribes from, a channel using Information Console. An administrator also can subscribe a user to, and unsubscribe a user from, a channel using Users in Management Console.

About the personal channel

Every user has a subscription to a personal channel. A user can subscribe to additional channels, if the user has the privileges to access additional channels. A user cannot unsubscribe from a personal channel, but a user can delete job notices from his personal channel. An administrator sets options on Users—Properties—Jobs to control whether iServer sends job completion notices to a user's personal channel by default, and if so, under what conditions iServer deletes notices. The user can also set these options, on Personal Settings—Jobs. A user scheduling a job can also control whether iServer sends a job completion notice for that job. If the user decides to send a notice, it appears in the user's personal channel and any other channels the user specifies when setting up the job.

Creating and managing channels

Only an administrator can create, modify, or delete channels. An administrator can view a list of current subscribers to any channel, although this list shows only those users who explicitly subscribe to the channel, not the users who have access through security role membership.

An administrator accesses all channels in the Encyclopedia volume through Management Console, and defines which security roles and users can access particular channels. For example, you can create a Sales channel that makes all sales documents available to marketing managers and finance managers. You create a security role, to which you assign the marketing and finance managers, then give read privilege on the Sales channel to that security role.

Security roles also represent other groups of users at the company, such as operations managers, facilities managers, and the legal department. By not subscribing these roles to the Sales channel, the administrator limits the distribution of sales documents.

You can also create a channel accessible to everyone. You create a channel, then give read privilege on it to the system-defined All role. Select from the following privileges when assigning privileges on a channel to a user or security role:

- Read

  A user can view the channel contents. To view a document through a channel, a user must have read privilege on the document.

- Write

  A user can direct the job completion notice and output of a scheduled job to the channel.

You create a new channel by choosing Create Channel on Channels. Table 6-1 describes the channel properties that you set on New Channel.

Table 6-1 New channel properties

Property	Description
Name	The channel name can be any length, but it must be unique.
Description	A description of the channel.
Auto delete after	The length of time a document is available in the channel before iServer deletes the job completion notice from the channel. The default value is 14 days.
Small (16x16) icon URL	The full URL of the small image file to represent the channel. If you do not set this value, the user interface uses a default 16x16 image to represent the channel.
Large (32x32) icon URL	The full URL of the large image file to represent the channel. If you do not set this value, the user interface uses a default 16x16 image to represent the channel.

How to create a channel

1. On Channels, choose Create Channel.
2. On New Channel—General, shown in Figure 6-2, specify a value for Name, and for Auto delete after: *n* days, where *n* is a number you specify.

   iServer requires these properties.

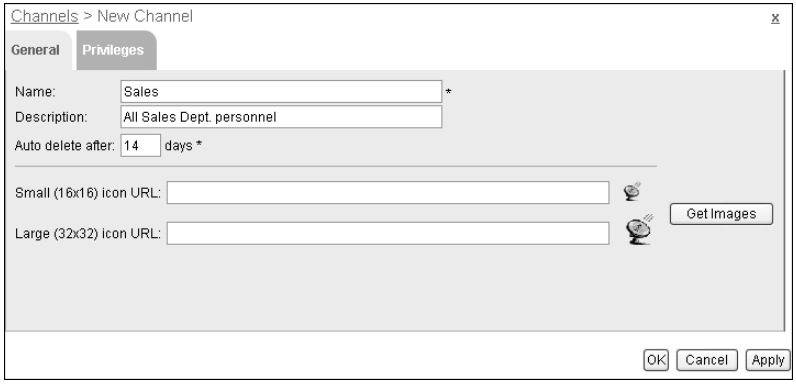

Figure 6-2 Specifying values for properties on New Channel—General

If you specify an icon URL for the channel, choose Get Images to refresh the channel icon.

Choose Privileges.

3 On Privileges, perform the following tasks:

1 Select Roles or Users to view the list of security roles or users from which to select in Available.

2 Move roles or users from Available to Selected.

3 Select a user or role in Selected and assign privileges on the channel by selecting Read, Write, or both, as shown in Figure 6-3.

Choose OK.

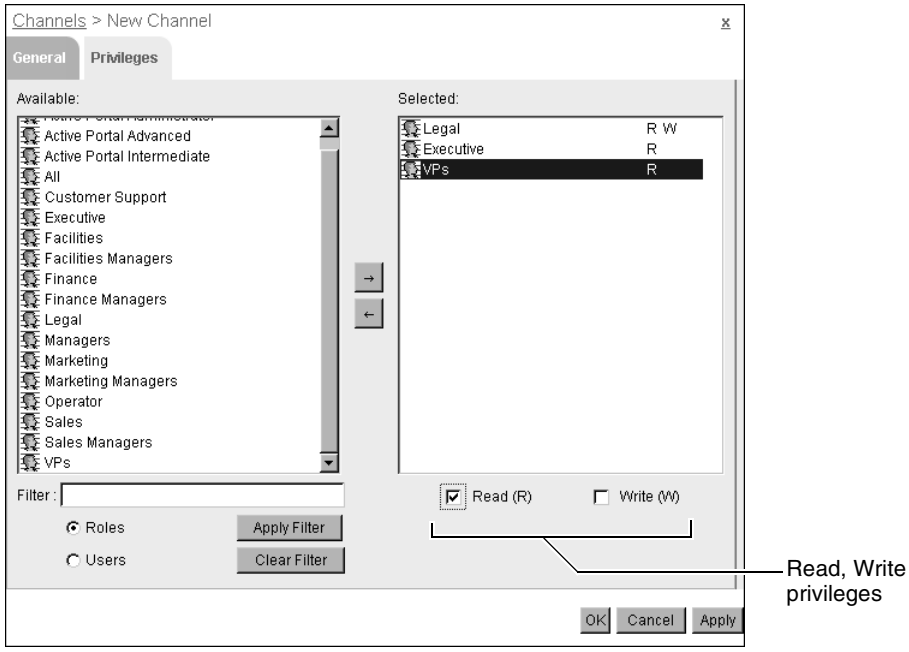

Figure 6-3 Assigning privileges on a new channel

How to update basic settings for one or more channels

1 On Channels, select channels to update as follows:

- To select a single channel, point to the arrow next to the channel name whose basic settings you want to update, and choose Properties, as shown in Figure 6-4.
- To select multiple channels, select the boxes next to the channel names whose basic settings you want to update. Alternatively, to select all

channels on the current page, select the box next to Name. To select all channels in the Encyclopedia volume, select Select all channels.

Point to Act upon selected channels, and choose Properties.

2 On Properties—General, modify the following properties:

- Name (for single channels only)
- Description
- Auto-delete policy
- Channel icon URLs

Choose OK.

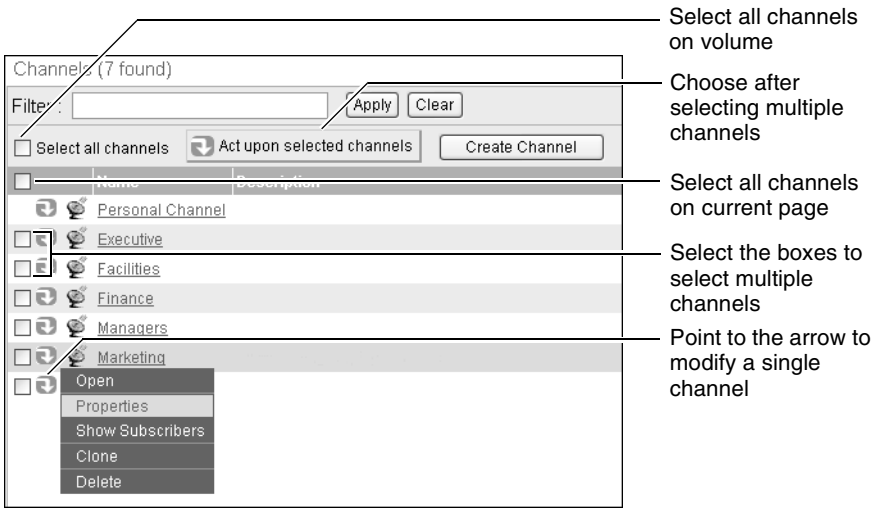

Figure 6-4 Accessing Channels—Properties

How to modify privileges for a single channel

1 On Channels, point to the arrow next to the channel name, and choose Properties, as shown in Figure 6-4. On Properties, choose Privileges

2 On Privileges, add privileges for users or security roles similar to the way you assign privileges on a new channel. Remove privileges by moving user names and roles from Selected to Available. Choose OK.

How to modify privileges for multiple channels

1 On Channels, select the boxes next to the channel names whose privileges you want to modify, as shown in Figure 6-4. Alternatively, to select all channels on the current page, select the box next to Name. To select all channels in the Encyclopedia volume, select Select all channels.

Point to Act upon selected channels, and choose Properties

On Properties, choose Privileges.

2 On Privileges, perform the following tasks, as shown in Figure 6-5:

- View a list of roles or users in Available.
  Select Roles or Users.
- Remove privileges on the channels.
  Move roles or users from Available to Remove these privileges. iServer assigns both Read and Write privileges to a role or user you move to Remove these privileges.

  To select a privilege that you want a role or user to keep, select the role or user in Remove these privileges, then deselect the privilege.
- Remove all privileges on the channels.
  Select Remove all. Selecting Remove all does not remove privileges you assign in Add these privileges.
- Assign privileges on the channels.
  Move roles or users from Available to Add these privileges.

  In Add these privileges, select one or more roles or users, then select Read, Write, or both.

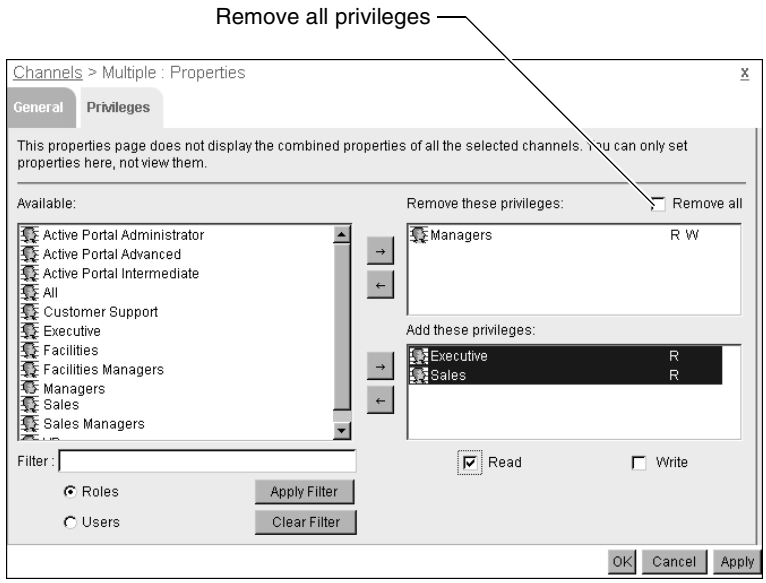

Figure 6-5 Removing and adding privileges on multiple channels

Choose OK.

How to clone a channel

You can create a copy of a channel by cloning an existing channel.

1 On Channels, point to the arrow next to the channel name and choose Clone, as shown in Figure 6-6.

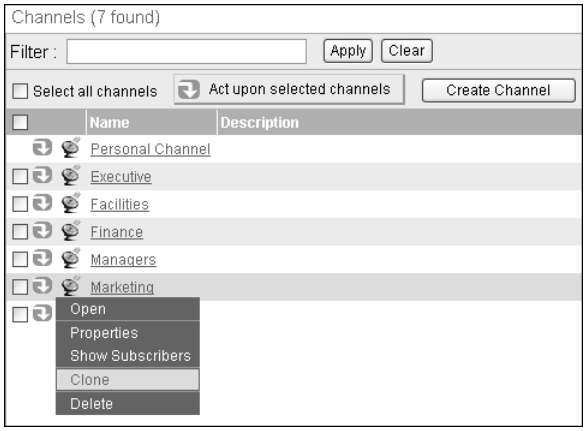

Figure 6-6 Choosing to clone a channel

2 On New Channel—General, change the cloned channel name. Optionally, add a description, specify the number of days for auto delete, and specify the URL for a small or large icon.

Modify any other properties as needed, then choose OK.

How to delete one or more channels

1 On Channels, shown in Figure 6-7, you can delete one or more channels as follows:

- To delete a single channel, point to the arrow next to the channel name, and choose Delete.
- To delete multiple channels at the same time, select the channels you want to delete. Alternatively, to select all channels on the current page, select the box next to Name. To select all channels in the Encyclopedia volume, select Select all channels.

  Point to Act upon selected roles, and choose Delete.

2 Confirm the deletion.

How to view a channel's subscriber list

1 On Channels, point to the arrow next to the channel name, and choose Show Subscribers, as shown in Figure 6-7.

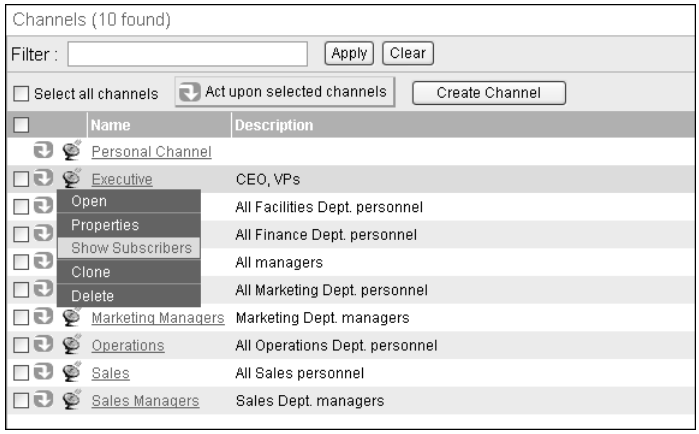

Figure 6-7 Choosing to show subscribers to a channel

Channels—Subscribers displays a list of current subscribers to the specified channel, as shown in Figure 6-8. You cannot add or remove subscribers on Subscribers.

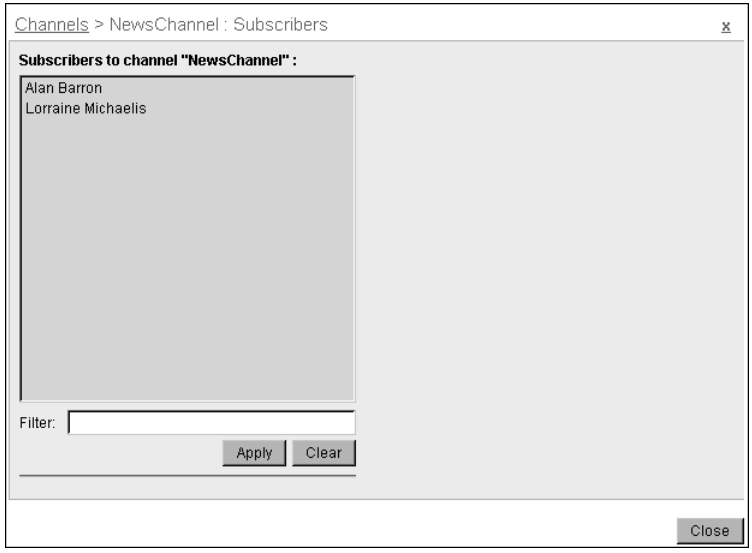

Figure 6-8 Viewing the list of channel subscribers

2 To return to Channels, choose Close.

How to specify a channel icon

You can specify an icon that both iServer and Information Console display next to the name of a channel, as shown in Figure 6-9.

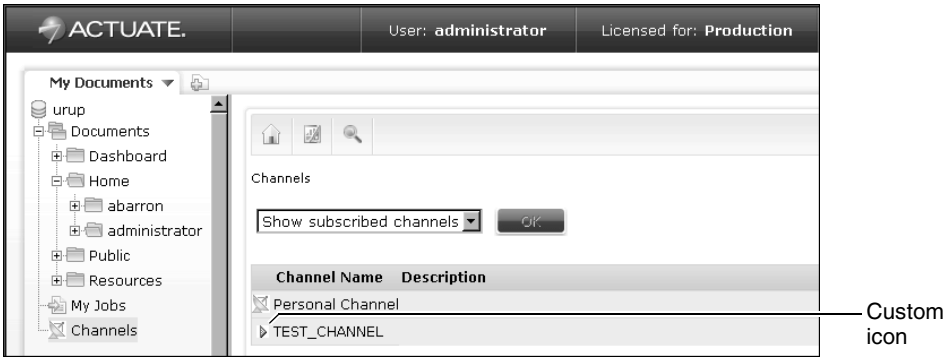

Figure 6-9 Custom channel icon

1 Place the icon image in <AC_SERVER_HOME>/servletcontainer /mgmtconsole/images/channels. Alternatively, place the icon on a web server.

2 From the side menu of Management Console, choose Channels.

3 To create a new channel, choose Create Channel.

To modify an existing channel, on Channels, point to the icon next to the channel, and choose Properties.

4 In Channels—Properties, in Small icon URL, type the URL of the icon. For example, use the following URL as shown in Figure 6-10:

```
http://localhost:8900/acadmin/images/channels/img_plusred.gif
```

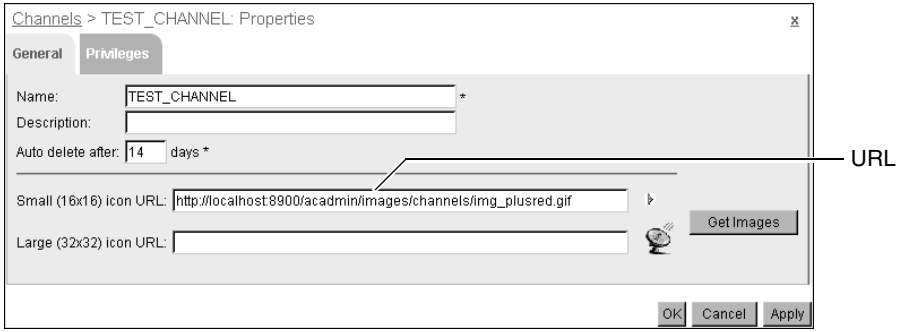

Figure 6-10 Specifying the URL to the icon

5 Choose Get Images, then OK.

Viewing a document

When iServer generates a document, iServer sends a completion notice to specified channels. A subscriber to a channel can view the document in a web browser by selecting the document name in the completion notice.

The web browser automatically uses the appropriate viewer for the type of document. Users typically view documents using Information Console.

How to view a document from a channel

1. On Channels, open the channel containing the job completion notice.
2. Either choose the document name or point to the arrow next to the job name, and choose Open Document, as shown in Figure 6-11.

Figure 6-11 Opening a document from a channel

The document opens in a separate browser window.

Working with notification groups

When a user schedules a job, the user has the option of choosing to notify other users about the completion of the job. Notification groups provide a convenient means of informing sets of users when jobs complete and documents are available. Each member of the group receives an e-mail or a job completion notice in his personal channel, as specified for each user. Notification groups streamline the notification process.

Only an administrator can create and manage notification groups. A user can view a list of groups of which the user is a member on Personal Settings—Groups in Management Console.

To complete the tasks in this section, use Notification Groups, as shown in Figure 6-12.

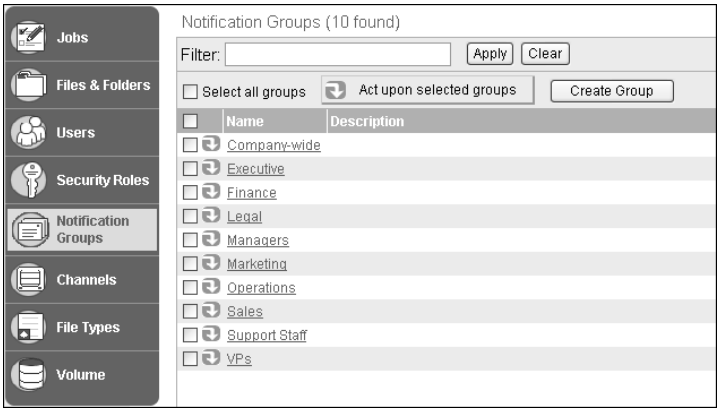

Figure 6-12 Viewing Notification Groups

How to create a notification group

1 On Notification Groups, choose Create Group.

2 On Notification Groups—New Notification Group, type the name of the group, as shown in Figure 6-13. Optionally, you can type a description.

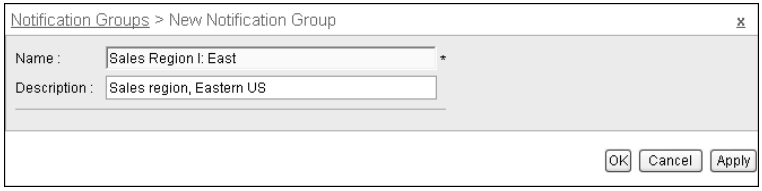

Figure 6-13 Creating a new notification group

Choose OK.

How to clone a notification group

You can create a copy of a notification group by cloning an existing notification group.

1 On Notification Groups, point to the arrow next to the group name, and choose Clone, as shown in Figure 6-14.

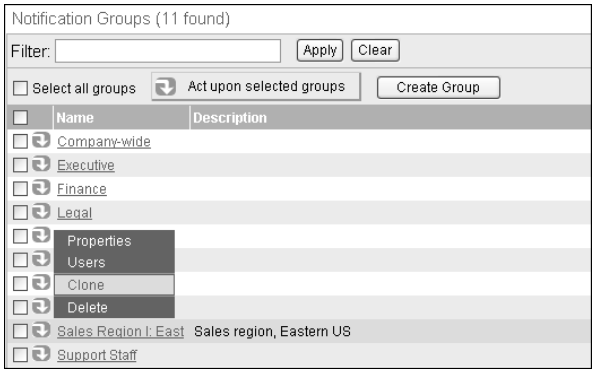

Figure 6-14 Choosing to clone a notification group

2 On New Notification Group, modify the cloned group name. Optionally, you can type a description.

Choose OK.

How to add and remove users from a single notification group

1 On Notification Groups, point to the arrow next to the notification group name, and choose Users, as shown in Figure 6-15.

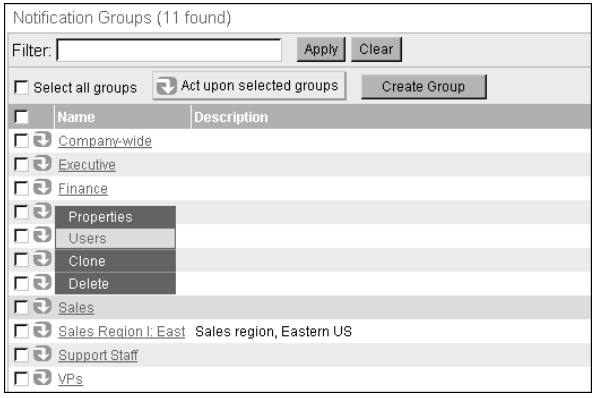

Figure 6-15 Choosing to add or remove users to or from a notification group

2 On Notification Groups—Users, you can add and remove members of the selected group, as shown in Figure 6-16.

Figure 6-16 Adding or removing users to or from a notification group

To add users:

1. Choose Add.
2. On Notification Groups—Users—Add, move the users you want to add to the group from Available to Add, as shown in Figure 6-17.

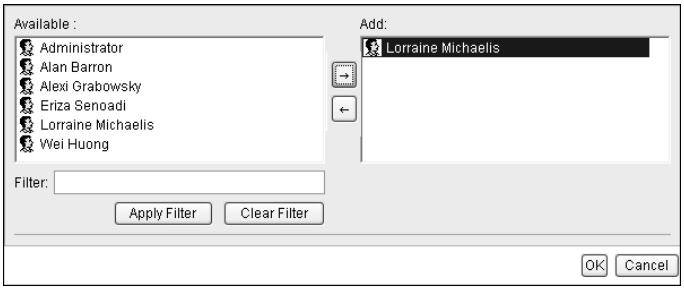

Figure 6-17 Adding users to a group

3. Choose OK.

To remove users:

1. Select the users whose membership you want to revoke, and choose Remove.
2. Confirm the removal.
3. Choose Close.

How to add and remove users from multiple notification groups

1. On Notification Groups, select the names of the groups from which you want to add or remove users. Figure 6-18 shows two groups selected. Alternatively, to select all groups on the current page, select the box next to Name. To select all the groups in the Encyclopedia volume, select Select all groups.

   Point to Act upon selected groups, and choose Users.

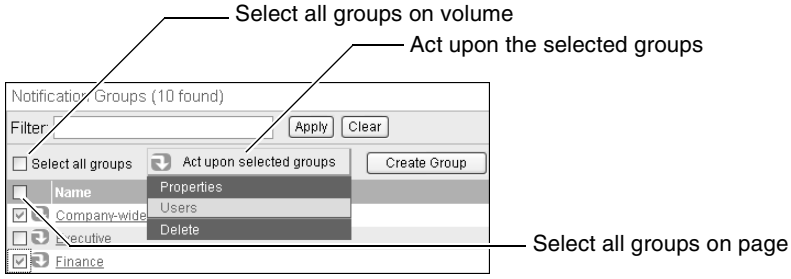

Figure 6-18 Choosing to add and remove users from multiple groups

2 On Notification Groups—Users, add users to notification groups or cancel group memberships as follows:

- To cancel membership in the selected groups, move users from Available to Remove these users.
- To add members to the selected groups, move users from Available to Add these users.
- To cancel all memberships in the selected notification groups, select Remove all.

  Selecting Remove all does not cancel membership in the selected groups for users you move from Available to Add these users.

  Figure 6-19 shows Notification Groups—Users.

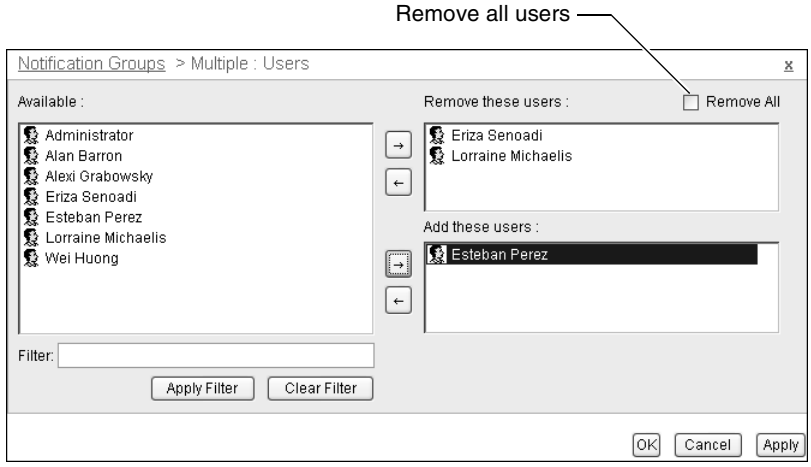

Figure 6-19 Adding and removing users to and from multiple groups

Choose OK.

How to rename a notification group

iServer tracks groups by ID, not membership. When you change the name of a notification group, its membership remains the same. Changing the notification group name does not affect group member notification.

1. To rename a notification group, point to the arrow next to the notification group name, and choose Properties.
2. On Notification Groups—Properties, type the new name of the group.

How to modify the description for multiple notification groups

Notification groups must have unique names. Groups can have the same description, and you can modify more than one description at a time.

1. On Notification Groups, select the names of the groups whose description you want to modify. To select all groups, choose Select all groups. To select all groups on the current page, select the box next to Name. Point to Act upon selected groups, and choose Properties.
2. On Notification Groups—Properties, type the new description as shown in Figure 6-20.

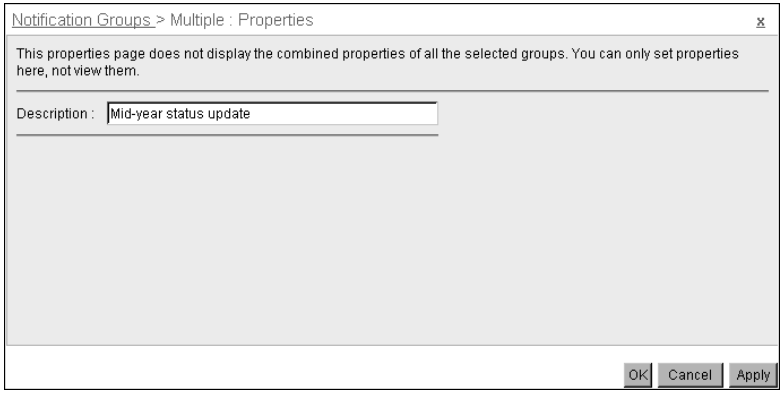

Figure 6-20 Properties for multiple notification groups

Choose OK.

How to delete one or more notification groups from the Encyclopedia volume

1. On Notification Groups:
   - To delete a single notification group, point to the arrow next to the notification group name, and choose Delete, as shown in Figure 6-21.
   - To delete more than one notification group, select the names of the groups to delete. To select all groups on the current page, select the box next to Name. Point to Act upon selected groups, and choose Delete, as shown in Figure 6-21.

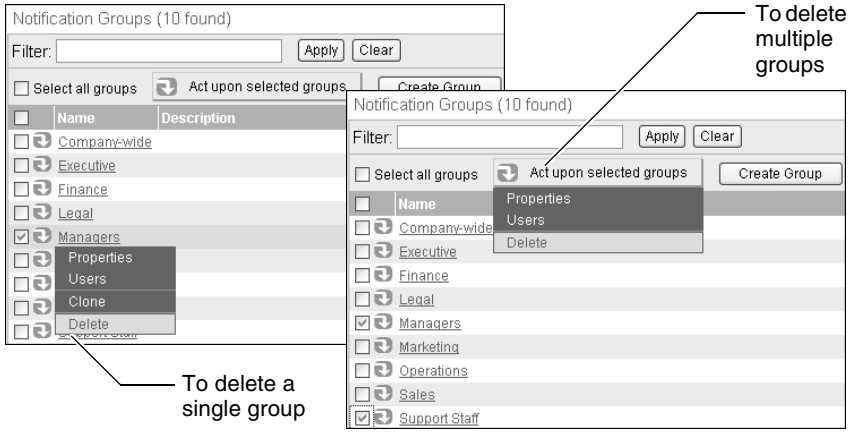

Figure 6-21 Deleting a group

2 Confirm the deletion.

Chapter

7

Working with file types

This chapter contains the following topics:

- About file types and volume management
- Working with Actuate Query
- Managing Actuate Analytics files
- Managing spreadsheet designs

About file types and volume management

You can view properties of the different file types from File Types. Each file type has properties you can view.

How to view the property values of a file type

On File Types, point to the arrow next to the file type, and choose Properties, as shown in Figure 7-1.

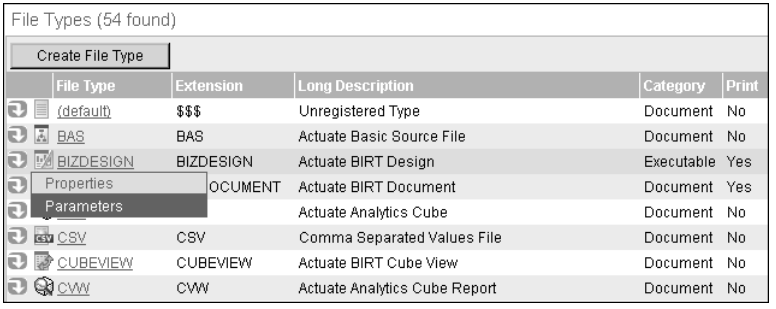

Figure 7-1 Viewing the property values of a file type

On File Types—Properties, you can view the definition of the selected file type.

Working with Actuate Query

When you license and enable Actuate Query Option for BIRT iServer System, you can use information objects in an Encyclopedia volume to retrieve and display data from data sources. Actuate information objects contain database connection and data column information. Actuate Query supports the following file types, as shown in Table 7-1:

- Actuate Basic information object (.dox) files
- information object (.iob) files
- data source map (.sma) files

To run an information object IOB that connects to more than one data source, you must license the Data Integration Option.

When you use Actuate Query with an information object IOB or data source map SMA to retrieve data from data sources, iServer uses the following files:

- An ODA driver to retrieve data from data sources
- An information object template file, a DOX, to format data that the information object retrieves

Table 7-1 Actuate Query process files

File	File type
Information object ODA driver	ROX or DOX
Actuate query template data object executable file, AQTemplate<release ID>.dox	DOX
Data object instance, saved from query data	DOI
Report object design, AQTemplate.rod	ROD

About the information object ODA driver

iServer uses the Integration service (AIS) ODA driver to connect to data sources when you use an information object. iServer also uses the ODA driver when you run designs that use an information object as a data source.

When running an information object, a Factory process uses the ODA driver to communicate with the Integration Service.

A design developer uses the ODA driver to create an Actuate Basic executable file, either a report object executable (.rox) file or a data object executable (.dox) file. This executable file uses an information object as a data source.

About the Actuate Query template file

iServer uses the Actuate Query template data object executable (.dox) file to format and display data that is retrieved using an information object with Actuate Query. If you save the query data as a data object instance (.doi) file, iServer creates a dependency between the DOI and the template file.

A developer can customize the query template. The DOX name is AQTemplate<release ID>.dox, where <release ID> is the release identifier, such as 90A060712.

The template file is a special DOX that is used only with IOB and SMA files. You cannot run the DOX file using Actuate e.Report Designer Professional, nor can you run it from an Encyclopedia volume.

About the Actuate Query template report design

The Actuate Query template report design called AQTemplate.rod ships with Actuate e.Report Designer Professional. An Actuate Basic design developer can customize this design to create an Actuate Query template data object executable (.dox) file. For example, a developer can change the design's default font, which is Arial Unicode MS, if the developer needs to change the font to display characters in some languages. The template's design contains a connection and data source components for use with information objects and the Integration

service (AIS). Do not change the connection and data source classes in AQTemplate.rod.

Using a customized Actuate Query template

After you create a customized template data object executable (.dox) file, you can upload the template to an Encyclopedia volume and configure iServer to use the template by completing one of the following actions:

- Use the advanced view of Configuration Console to specify the template file as the value for the Volume Actuate Query template file parameter. The parameter is on Volumes—Properties—Advanced—Actuate Query Generation for the Encyclopedia volume. The DOX that you specify becomes the default template file for all new queries that use an IOB or SMA.
- Use IDAPI to create an Actuate Query and specify the DOX as the template file. You can specify the template file in a GetQuery( ), CreateQuery( ), or ExecuteQuery( ).

Managing Actuate Analytics files

With an Actuate iServer System license file that enables the Actuate Analytics Option, iServer supports running or scheduling an Analytics cube profile to generate multidimensional data cubes for analysis. iServer retrieves data, structures the data in an Analytics cube, and adds the cube to the Encyclopedia volume.

You analyze the cube data using the Analytics Cube Viewer, which is distributed as a component of Information Console and Management Console. When you analyze a cube, you can aggregate or categorize data, summarize data, and create graphs that are based on the data. You can save your analysis of the data as a cube view in the Encyclopedia volume. On an Encyclopedia volume, you can save a maximum of 30 cube report (.cvw) files for each cube (.cb4) file.

You can store and manage multiple views.

When you enable the Analytics Option, you can perform the following tasks:

- Run and schedule cube profiles in an Encyclopedia volume.
- Generate a transient or persistent cube in an Encyclopedia volume.
- Create a new cube view and save the view in an Encyclopedia volume.

If you do not enable the Analytics Option:

- You can upload a cube profile, a cube, or a cube view to the Encyclopedia volume.
- You can view or access existing cubes in the Encyclopedia volume.

- You cannot run or schedule cube generation. Scheduled jobs run and fail.

About Analytics file types

Table 7-2 describes the Encyclopedia volume file types for Analytics cube profiles, cubes, cube views, and Microsoft Analysis Service Access parameters.

Table 7-2 Analytics file types

File type	Description
DP4	A cube design profile is a binary file that contains information about the data source connection, the data to retrieve, and how to organize the data as a multidimensional cube. This is an executable file type.
CB4	A cube data file, generated from a profile. This is a document file type.
CVW	A cube view for a specific cube. This is a document file type. A cube view is dependent on the cube profile that generates the cube view.
ODP	Microsoft Analysis Services OLAP cube access parameters for a Microsoft SQL database. This file contains parameters that identify and access the cube that Microsoft Analysis Services stores and manages. This is a document file type.

About Analytics data source support

iServer supports the following types of data source access:

- ODBC data sources
- Text files
- XML files
- Executable files

For information about support for JDBC database drivers for Analytics and Cube Designer, see the Supported Products and Obsolescence Policy at the following URL:

http://support.actuate.com/documentation/spm

About the Analytics default data source

By default, iServer looks for a text file or XML data source in the iServer drivers directory. On a Windows system, the default directory is:

```
\Program Files\Actuate10\iServer\drivers
```

On a UNIX system, the default directory is AC_SERVER_HOME/drivers.

About connection information in an external file

Analytics supports specifying data source connection information in an external file for the following types of connections:

- ODBC
- Paths to the XML Data File and XML Data File Descriptor

A cube designer must configure the cube to use connection information from an external file. You specify the connection configuration file's location using the Configuration file for connections parameter that you set in Configuration Console. If a cube uses data source information from the configuration file, cube data generation fails if the configuration file does not contain the correct connection information.

Accessing a Microsoft Analysis Services data cube

Analytics Option supports viewing and manipulating data from a multidimensional data cube in an MS SQL database with Microsoft Analysis Services. Access to data cubes in a Microsoft SQL database with Microsoft Analysis Services is available only when iServer runs on Windows.

You can view and manipulate cube data using Cube Viewer. To access data from a multidimensional cube in an MS SQL database using Cube Viewer, create an ODP parameter file in an Encyclopedia volume. When you use Cube Viewer with the ODP parameter file, iServer retrieves data from the cube that is specified in the ODP parameters.

Table 7-3 lists the parameters for the Microsoft Analysis Services (.odp) file type.

Table 7-3 Microsoft Analysis Services file type parameters

Display name	Parameter name	Description
Microsoft Analysis Service Cube Name	cubename	Name of the cube in the Microsoft SQL Server that the Microsoft Analysis Service manages. Required.
Data Source Name	datasourcename	Microsoft SQL Server database name. Required.
Data Source Provider Name	datasourceprovider	Name of the Microsoft SQL Server database. Default value is MSOLAP. Required.
Description	description	Description of the cube. The text appears in the About box of Actuate Cube Viewer. Optional.

Table 7-3 Microsoft Analysis Services file type parameters

Display name	Parameter name	Description
OLAP Server Name	olapserver	Name of the OLAP server that connects to the Microsoft SQL Server database. Required.
Username for ODBO Data Source	userid	The user ID to use to log in to the Microsoft SQL Server. Optional.

How to create an ODP parameter file

1. On File Types, point to the arrow next to the ODP file type parameter, and choose Parameters.
2. On File Types—Parameters, choose Save File To Server.
3. Complete Create Parameter Values File as shown in Figure 7-2:
   - Type the Encyclopedia volume file name and the folder that contains the ODP file.
   - If the parameter values file already exists, you can choose to:
     - Replace the latest version with a new one.
     - Create a new version and keep the previous version.
     - Specify how many earlier versions to retain.
   - Type the parameters to access the multidimensional data cube in an MS SQL database.

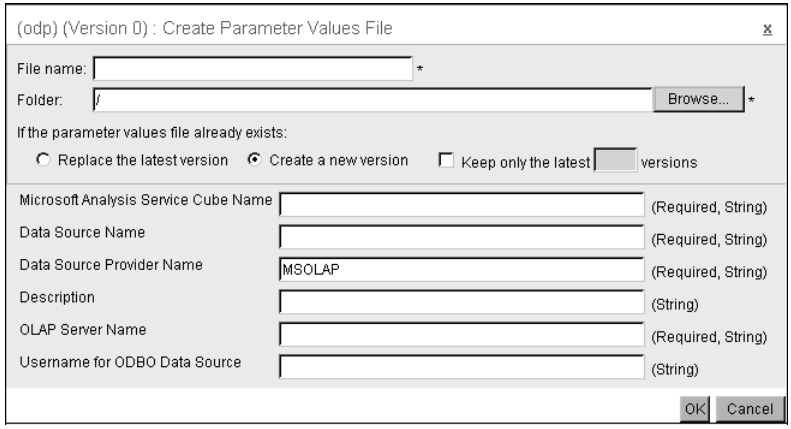

Figure 7-2 Create Parameter Values File

Choose OK.

Managing spreadsheet designs

With an iServer System license file that enables the BIRT Spreadsheet Option, you can run or schedule spreadsheet designs created using BIRT Spreadsheet Designer.

Using BIRT Spreadsheet Designer, a design developer creates a spreadsheet design that can:

- Connect external data to a worksheet range.
- Manipulate and format the data.

In BIRT Spreadsheet Designer, the developer:

- Creates the workbook (.sod) file
- Optionally, references files such as a VBA template in an Excel workbook

Understanding how iServer handles spreadsheet files

When you publish a spreadsheet design to an Encyclopedia volume using BIRT Spreadsheet Designer, iServer assigns the SOX file type to the spreadsheet design.

When you use BIRT Spreadsheet Designer to publish a workbook to an Encyclopedia volume, BIRT Spreadsheet Designer adds the spreadsheet design and files referenced by the design, such as callback classes or VBA templates, to the Encyclopedia volume.

When you upload a workbook to an Encyclopedia volume using Management Console instead of using BIRT Spreadsheet Designer, files referenced by the spreadsheet design are not uploaded. Management Console assigns the SOX file type to the workbook file.

When you run the spreadsheet design with the BIRT Spreadsheet Option enabled, iServer performs the following actions in this order:

- Reads in the workbook that the design developer created in BIRT Spreadsheet Designer
- Sets the parameters that are attached to the workbook
- Executes the callback class, if one exists
- Refreshes the data from data sources, such as databases, XML files, and text files in the workbook
- Applies the VBA from the template, if one exists
- Saves the document, either as an Excel file, which is viewable from the Encyclopedia volume, or as a spreadsheet object instance file (SOI), which users can use to open personalized or secure Excel views of the document

Specifying spreadsheet design connection properties

There is no default location for the connection configuration file. To use a connection configuration file, you create the file and then specify its name and location using the ConnConfigFile parameter in Management Console.

Setting parameters for spreadsheet designs

The BIRT Spreadsheet Factory process generates spreadsheet designs. When you manage spreadsheet designs in iServer, you can encounter run-time errors due to environment settings. If so, review Table 7-4 to select a parameter that can correct the problem. To ensure that iServer always uses these settings, you must specify these parameters with both BIRT Spreadsheet SOX and SOI file types. To duplicate these settings on another file type, you can set the parameters for one file type, choose to export the parameters to a ROP file, and import the ROP file to the other file type.

Table 7-4 BIRT Spreadsheet design parameters

To perform this task…	Use this parameter…
Resolve the message Unable to connect to Java helper.	AC_ JDRV_LAUNCH_WAIT Supply an integer that indicates the number of seconds to wait before timing out. If you receive this message or the system is too busy, increase the launch time-out value beyond the default setting of 10 seconds to provide more time for the BIRT Spreadsheet factory to start.
Resolve the message Couldn't find Java runtime environment by setting the parameter in Configuration Console.	AC_JRE_HOME Provide a string as the full path to set the Java Runtime (JRE) installation directory. If you set the JRE_HOME environment variable on UNIX, this parameter is optional. If JRE_HOME appears in BIRT iServer registry keys on Windows, this parameter is optional. iServer uses the value in the Windows Registry.
Tune the performance of the Java Virtual Machine by setting the parameter in Configuration Console.	AC_JVM_PARAMETERS Provide a string for parameters to pass to the Java Virtual Machine (JVM) when starting the JVM. There is no default value. The options you set for this parameter vary by platform. For example, to see a list of options for the Sun Windows JVM, see the following URL: `http://java.sun.com/j2se/1.3/docs /tooldocs/win32/java.html#options`

(continues)

Table 7-4 BIRT Spreadsheet design parameters (continued)

To perform this task…	Use this parameter…
Tune the performance of the Java Virtual Machine by setting the parameter in Configuration Console. *(continued)*	In the Sun Windows JVM, you can set the maximum heap size using the -Xmx parameter and the minimum heap size using -Xms. Adapt the JVM options as your system requires. For example, you can change the maximum heap size to ensure that the JVM has enough memory to run the largest design. Ensure that the iServer machine has enough free memory to accommodate the maximum heap size. Do not set it to more than 256 MB. If iServer uses a running JVM to generate a spreadsheet document, AC_JVM_PARAMETERS values have no effect. The values are used only when starting the JVM.
Resolve a message similar to Driver or file not found by setting the parameter in Configuration Console.	AC_JDRV_CLASSPATH Supply a string for the location of the spreadsheet population class, database drivers, or alternate XML or XSL processors. Separate multiple entries in Windows using a semicolon (;) and in UNIX using a colon (:). BIRT Spreadsheet uses an internal class loader, not the system CLASSPATH.
Decrease the system resources used.	AC_ JDRV _TIMEOUT Provide an integer that indicates the number of seconds to wait after the last completed document request runs before timing out. Use this parameter to consume fewer resources. Using this parameter may result in a longer initial document generation time. Changes to this parameter take effect only when you restart iServer. The default value (-1) keeps the BIRT Spreadsheet Factory up and does not exit. If you use a value of 0, the BIRT Spreadsheet Factory process exits immediately after it completes each document request.
Set the debugging options.	AC_JDRV_LOG_LEVEL You can change the debugging level by supplying one of the following integers for the logging level: ■ 1 logs errors. ■ 2 logs warnings. ■ 3 logs status information (the default setting). ■ 4 logs debug messages.

Table 7-4 BIRT Spreadsheet design parameters (continued)

To perform this task…	Use this parameter…
Control spreadsheet document DPI.	AC_SS_DPI Add AC_SS_DPI as a file type parameter to specify the DPI for all spreadsheet documents. To specify the DPI for a document, add AC_SS_DPI as a design parameter. BIRT Spreadsheet Designer creates the AC_SS_DESIGNDPI parameter as a hidden design parameter when deploying a spreadsheet design to an Encyclopedia volume. AC_SS_DESIGNDPI specifies design DPI if you do not specify AC_SS_DPI.
Control caching of spreadsheet books.	AC_SS_BOOKCACHESIZE Specify the number of spreadsheet books cached. The default is 8 books. A value of 0 disables caching. For improved performance, iServer stores generated spreadsheet documents in a cache to access and run them again if necessary.
Control creation of a graphics port by setting the parameter in Configuration Console.	AC_RUNNING_HEADLESS When running a spreadsheet design, iServer creates a graphics port. Use AC_RUNNING_HEADLESS to control the creation of the graphics port. The value is either yes or no. The default value is no, create a graphics port. Set this value to yes to disable the creation of a graphics port. On systems without a graphics card or graphics port, set this value to yes. For better performance, set this value to yes if the spreadsheet design does not use the Adjust column width property on any of the design ranges.
Control where iServer searches for data source connection information.	AC_SS_CONNECTION_OVERRIDE To not use the connection information in the spreadsheet design, create the string parameter AC_SS_CONNECTION_OVERRIDE, and set the value to OFF. The default value is ON.

If a port conflict exists, and another process listens on the port to which the BIRT Spreadsheet Factory process is assigned, unpredictable results can occur, such as error messages from the conflicting process or spreadsheet designs that do not complete because the port is not available.

Chapter

8

Managing volume-level operations

This chapter contains the following topics:

- Working at the volume level
- Archiving files and removing empty folders
- Setting volume privileges
- Setting volume-level printer options
- Setting web browser defaults

Working at the volume level

To access the Volume pages of Management Console, choose Volume from the side menu, as shown in Figure 8-1.

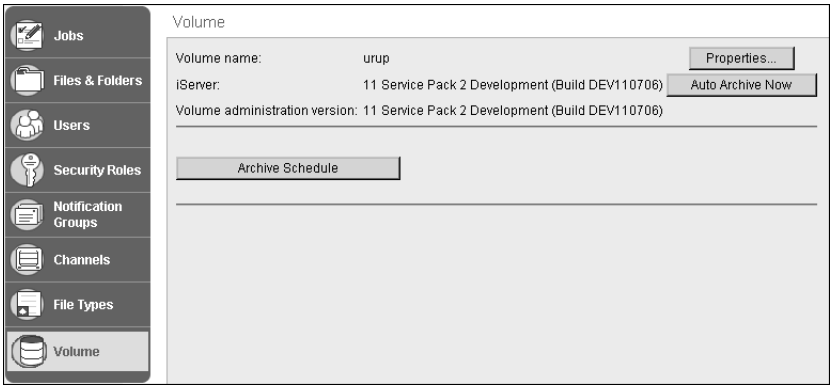

Figure 8-1 Viewing Volume

From Volume, you can:

- Access Volume—Properties.
- Initiate autoarchiving.
- Schedule an archiving cycle.

Using Volume—Properties, you can:

- Set a retry policy for failed jobs.
- Enable or disable browser caching of DHTML documents.
- Set security roles and user privileges on the Encyclopedia volume.
- Set an autoarchiving policy for the volume.
- Set a volume-level purge policy for job notices.
- Set volume-level printing properties.
- Establish a connection with an external cache for running information object jobs.

Figure 8-2 shows Volume—Properties—General as well as the other properties for Volume.

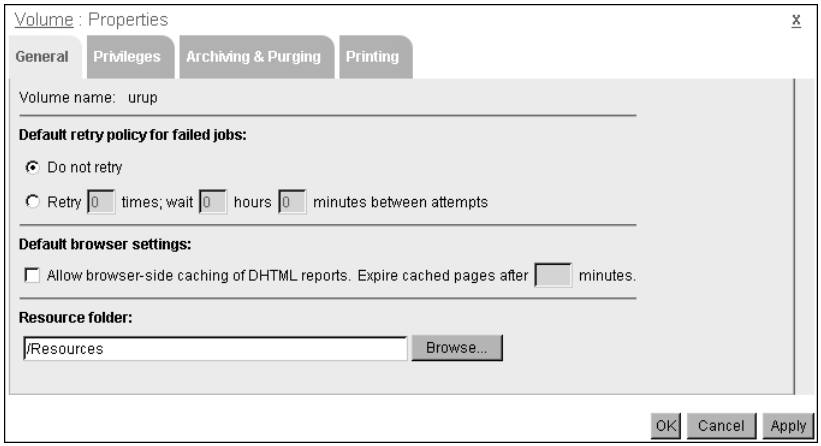

Figure 8-2 Volume—Properties—General

Many of the relationships in the Encyclopedia volume have recommended and hard limits. If you adhere to the recommended limits, the appearance, behavior, and performance of Management Console is acceptable. Your web browser imposes the hard limits. Table 8-1 shows the limits for the Encyclopedia volume.

Table 8-1 Limits for the Encyclopedia volume

Relationship	Recommended limit	Hard limit
Channels notified about a particular job	100	1000
Channels to which a particular user subscribes	15	150
Notification groups of which a particular user is a member	100	2000
Security roles of which a particular user is a member	100	2000
Security roles that are children of a particular security role	100	2000
Security roles that are parents of a particular security role	100	2000
Users and notification groups notified about a particular job	100	1000
Users and security roles in a single access control list (ACL) for a file, folder, or channel, including ACLs that jobs create	100	2000

(continues)

Table 8-1 Limits for the Encyclopedia volume (continued)

Relationship	Recommended limit	Hard limit
Users and security roles in a particular privilege template	100	2000
Users who are members of a particular notification group	Unlimited (greater than 1,000,000)	
Users who are members of a particular security role	Unlimited (greater than 1,000,000)	
Users who subscribe to a particular channel	Unlimited (greater than 1,000,000)	

Archiving files and removing empty folders

By performing the following Encyclopedia volume autoarchiving tasks, administrators and users specify the policy that iServer uses to delete files and empty folders, and archive files and folders in the Encyclopedia volume:

- Using Management Console, an administrator can set the autoarchive policy for the entire Encyclopedia volume and for specific folders and files.
- Using Configuration Console, an administrator can specify the archive service to use to archive files. You specify a single archive service for the Encyclopedia volume.
- A user can set the autoarchive policy for specific files and folders. A user must have read, write, and delete privileges on the file or folder. When submitting a job, a user can also set the autoarchive policy on the output document.

The following points are useful to know when setting autoarchive policy:

- The volume autoarchive policy is the default policy for every file and folder in the volume. If you change the policy for a file type, specific file, or folder, that policy supersedes the volume policy.
- If you specify a policy for a particular folder that differs from its parent folder policy, all the files and folders in that particular folder inherit its policy as the default policy.
- If you specify a policy for a particular file, that policy supersedes the policy the file inherits from its containing folder.
- If you do not specify a policy for a file type on Properties—Auto Archive for a folder, any file of that file type within the folder inherits the folder policy.
- The autoarchive process removes a folder if it is empty or if the following conditions are true:

- Every subfolder is empty.
- The age of every file in the folder has expired.

- If the administrator specifies a volume archive service provider in Configuration Console, iServer enables the Archive before deletion option on Properties—Auto Archive when a user selects or has already selected Delete when older than n days n hours or Delete after date <date> time <time>.

iServer determines whether to perform autoarchiving on an item by processing volume contents using the following order of precedence and evaluating:

- The policy on an individual file or empty folder
- The policy for the specific file type or folder, from the containing folder's File Type list
- The containing folder's default policy
- The policy for the specific file type or folder, from the File Type list of the folder containing the folder
- The policy for the specific file type or folder, from the File Type list of folders that are higher in the hierarchy
- The policy for the Encyclopedia volume

To see an item's autoarchive policy, from Files and Folders, point to the arrow next to the item and choose Properties. On Properties, choose Auto Archive. On Auto Archive, choose View Policy.

By default, iServer performs an autoarchive sweep once daily. You can specify when and how many times to perform an autoarchive sweep in a day.

When iServer performs autoarchiving, it starts from the Encyclopedia volume's root folder. For each file whose age has expired, iServer deletes the file. If the Archive files before deletion option is selected, iServer calls the archive application for the Encyclopedia volume, then deletes the file if the archive process succeeds. If the archive process fails, iServer does not delete the file.

Using autoarchiving applications

In Configuration Console, an administrator can specify a volume archive service provider, or archive application, that the system uses to archive files before deleting them. The archive application is software that is the interface between iServer and an external archiving tool.

You can use an archive application that calls the online archive SOAP-based API. iServer ships with a configurable, Java-based Encyclopedia volume autoarchive application that uses the SOAP-based autoarchive API. Using the application requires an BIRT iServer System license with the Online Archive option enabled.

When iServer performs autoarchiving, it loads the archive application. If a file autoarchive policy specifies deletion and includes the Archive files before deletion option, iServer exports the file to the external archiving tool.

iServer read-locks the file during the archive process so no other process can delete or change the file during archiving. After the archive service signals that the archive process succeeded, iServer deletes the file. If the archiving fails, iServer does not delete the file.

Setting the volume's autoarchiving and purging rules

On Volume—Properties—Archiving and Purging, shown in Figure 8-3, the administrator can set the autoarchive policy for all the files and empty folders in the Encyclopedia volume or for a specific file type.

The default policy for the volume is Do not automatically delete this file and Do not archive the file before deletion. Use File Type to set the autoarchive policy for a file type. The policy you set for that file type is the default policy for every file of that type on the volume. When you select a file type in File Type, iServer displays the current autoarchive settings for the file type you select.

You can modify settings for one file type after another before choosing OK to implement those changes. iServer retains the values you set for multiple file types and applies the values when you choose OK.

Figure 8-3 shows settings for an autoarchive policy on Volume—Properties—Archiving and Purging.

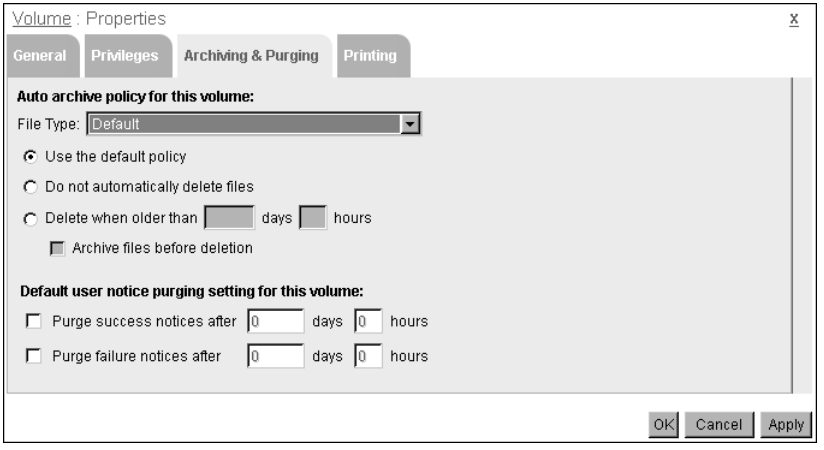

Figure 8-3 Viewing Volume—Properties—Archiving and Purging

Volume—Properties—Archiving and Purging also displays the settings for the volume's default purging policy. Using the options described in Table 8-2, the administrator sets the volume default policy specifying how long a job

completion notice remains on a user's personal channel before iServer can delete the notice.

Table 8-2 Purge settings

Property	Description
Purge success notices after *n* days *n* hours	Enable deleting job completion notices for jobs that succeed. Set the time after which iServer can delete the notice.
Purge failure notices after *n* days *n* hours	Enable deleting job completion notices for jobs that fail. Set the time after which iServer can delete the notice.

The administrator can view or change the job completion notice purge settings for a user by choosing Users from the Management Console side menu, pointing to the arrow next to a user and choosing Properties, then choosing Jobs. A user can do this also, by choosing Personal Settings from the Management Console side menu and choosing Jobs. A user's own job completion notice purge policy supersedes the volume-level policy.

How to set the Encyclopedia volume's autoarchive policy

1. On Volume, choose Properties.
2. On Properties, choose Archiving and Purging.
3. On Archiving and Purging, specify the autoarchive policy for the Encyclopedia volume. If you do not specify an autoarchive policy for a file type, the Encyclopedia volume uses the default autoarchive policy.
4. When you finish, choose OK.

Scheduling and initiating an autoarchiving cycle

From Volume, you can start, stop, and schedule archive sweeps.

How to start an autoarchiving cycle

On Volume, choose Auto Archive Now, and confirm, as shown in Figure 8-1.

How to stop an autoarchiving cycle

When iServer is running an archive sweep on an Encyclopedia volume, you can stop the process from Volume, using Stop Archive Thread, as shown in Figure 8-4.

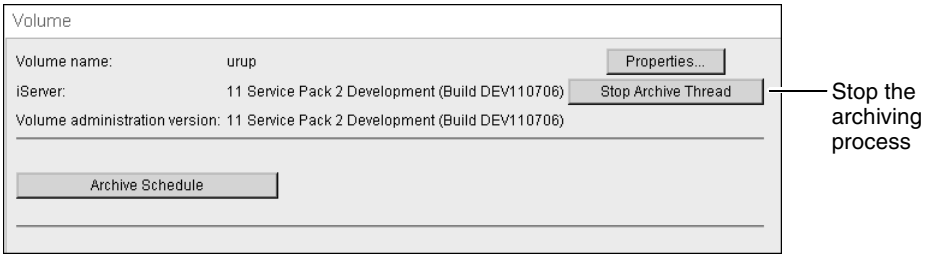

Figure 8-4 Stopping an autoarchive sweep

How to schedule an autoarchiving cycle

Choose Archive Schedule, as shown in Figure 8-4, to schedule regular archive sweeps. You can specify the time zone, frequency, date, and time. You can even exclude specific dates from the pattern that you create. You specify duration using the Start and End dates in Archive Schedule.

Setting web browser defaults

An administrator can enable or disable DHTML document caching by a web browser, as shown in Figure 8-5. Selecting Allow browser-side caching of DHTML documents in Volume—Properties supports a user's browser storing a document in DHTML format on the user's local machine. Normally, iServer does not store DHTML files. You can specify the length of time before the cached pages expire on Volume—Properties—General.

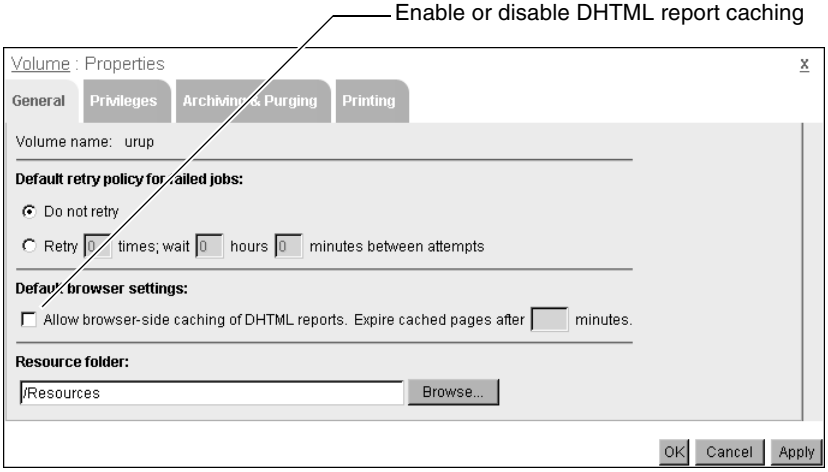

Figure 8-5 Enabling or disabling DHTML report caching

Setting volume privileges

By default, the All security role has visible, read, execute, and write privileges on the root folder. An administrator can view and change the root folder's properties on Volume.

How to view privileges on the Encyclopedia volume's root folder

1 On Volume, choose Properties.

On Properties, choose Privileges.

2 On Privileges, you can view the current privilege settings.

Figure 8-6 shows the default setting.

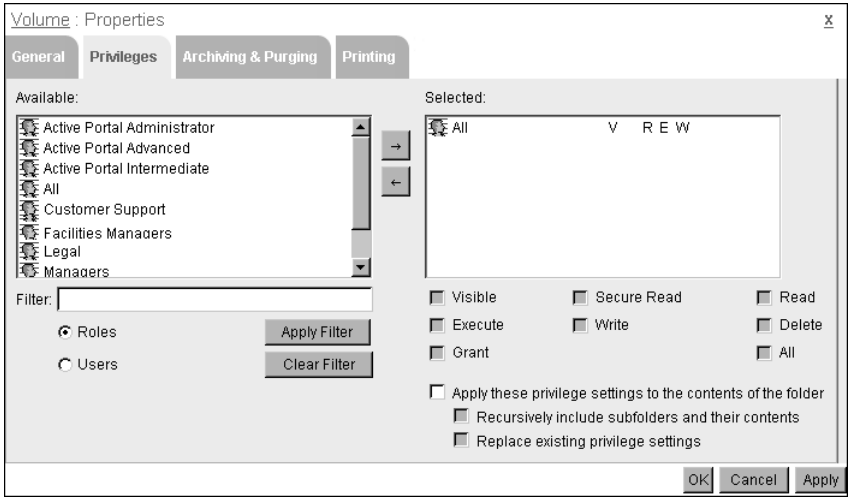

Figure 8-6 Viewing Volume—Properties—Privileges

You can also modify the current privilege settings from Privileges.

When you finish, choose OK.

Setting volume-level printer options

The Encyclopedia volume recognizes and supports printers that are set up for iServer. You do not have to install printers specifically for the Encyclopedia volume. You do, however, customize printer settings for each printer that is available to the Encyclopedia volume.

Only a volume administrator can set printer options at the Encyclopedia volume level. Users can accept values for these printer properties as defaults, set their own, or set them on individual print jobs.

Table 8-3 describes these properties.

Table 8-3 Volume-level printer properties

Property	Description
Scale	The scale at which to print the output, expressed as a percentage.
Resolution	The resolution at which to print the output.
Mode	Black and white or color.
Number of copies	The number of copies to print.
Collate	Collate the copies.
Duplex	Select ■ Simplex (one-sided) ■ Horizontal (double-sided, side by side) ■ Vertical (double-sided, top to top)
Page size	An extensive drop-down list of standard international formats.

Some printers do not support all these options.

When a user prints a document, iServer adheres to printing specifications from three sources, in the following order of precedence:

- Printer property values set for the current print job.
- Printer property values that are the user's default settings. The Encyclopedia volume administrator or the user can set these values.
- Printer property values that are set at the Encyclopedia volume level by the Encyclopedia volume administrator.

For a print request when scheduling a job, iServer uses the page size that the user explicitly selects either on Schedule—Printing, or on Personal Settings—Printing. If the user does not select a page size, iServer uses the page size that the scheduled design or document specifies. iServer does not use the Encyclopedia volume default setting.

Figure 8-7 shows how iServer determines which printer properties to use for a print job.

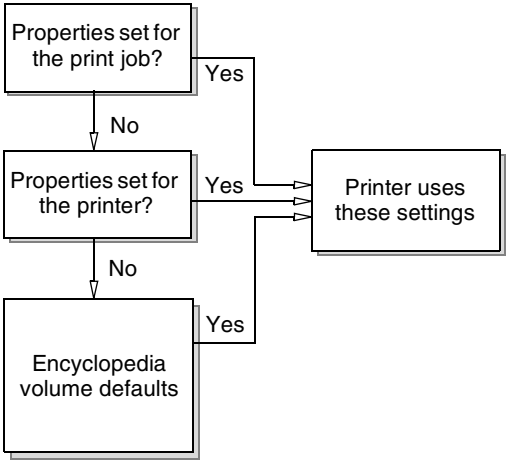

Figure 8-7 Precedence for printer properties

Using Volume—Properties—Printing, an administrator can set property values for any iServer printer and specify the default printer for an Encyclopedia volume.

How to set Encyclopedia volume-level printer properties

1 On Volume, choose Properties.

On Properties, choose Printing.

2 On Printing, specify a default printer and printer settings for the Encyclopedia volume, as shown in Figure 8-8.

If available, iServer displays the following information from the printer and operating system:

- Manufacturer
- Model
- Description
- Location

When you finish setting the properties for a printer, you can set properties for a different printer by selecting it from the Printer drop-down list. You do not need to choose OK between printer selections.

When you have specified settings for all printers, choose OK.

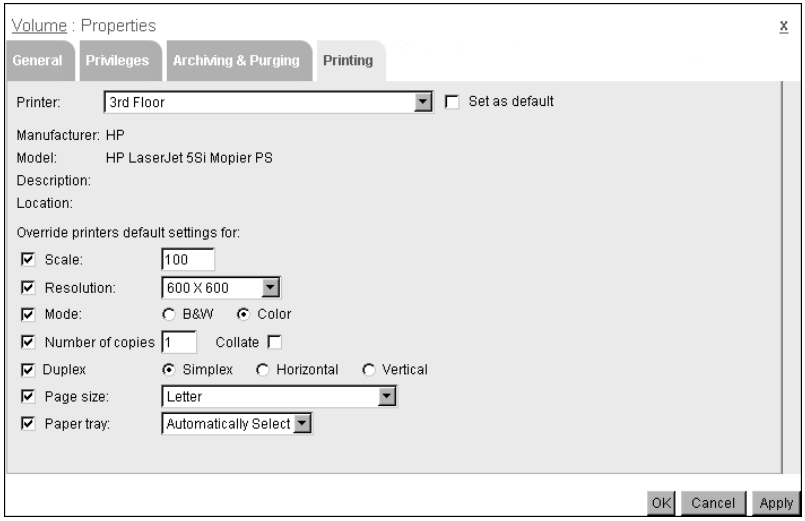

Figure 8-8 Setting print properties on Volume—Properties—Printing

Chapter

9

Managing Encyclopedia volume security

This chapter contains the following topics:

- About Encyclopedia volume security
- Planning how to assign privileges
- Setting privileges to access an information object
- Using page-level security
- Using information object pass-through security
- About Open Security
- About RSSE
- Using Management Console with Open Security
- Using RSSE with page-level or SmartSheet security

About Encyclopedia volume security

An administrator protects the Encyclopedia volume against unauthorized use by password-protecting user accounts, sharing files, and assigning privileges to users and groups of users to access files, folders, and channels.

Using Management Console, an administrator assigns privileges, such as Execute, to users either directly or through security roles, as shown in Figure 9-1.

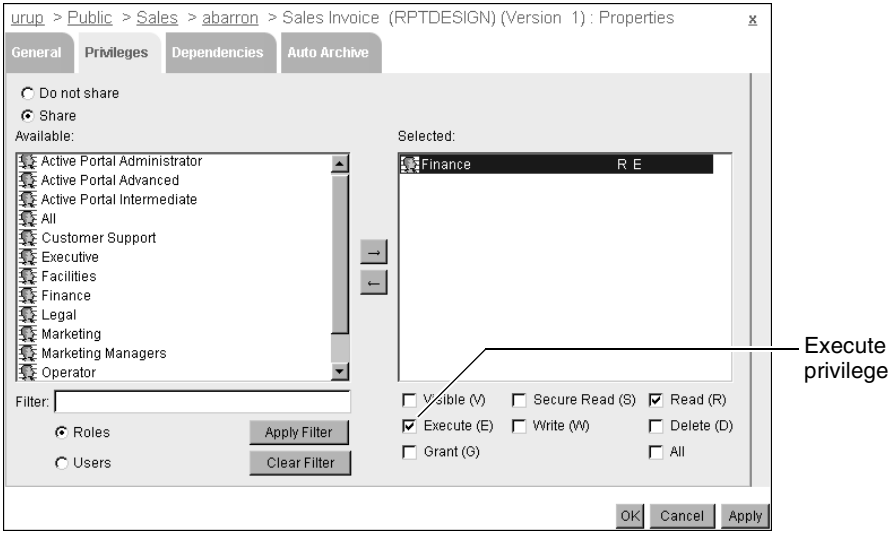

Figure 9-1 Assigning a privilege to a security role

A security role is a name for a set of privilege levels. You use a security role to assign privileges to a group of users.

About the types of privileges

Users can have the following types of privileges to access files in an Encyclopedia volume:

- Delete
  The ability to remove items from the Encyclopedia volume.
- Execute
  The ability to run items from the Encyclopedia volume.
- Grant
  The ability to extend privileges for a specific item in the Encyclopedia volume to another user.

- Read
  The ability to open, work with, print, and download an item in the Encyclopedia volume.
- Secure read
  The ability to read only specific parts of a document in the Encyclopedia volume. To use Secure read, iServer must have BIRT or e.Report Page Level Security option, or BIRT SmartSheet Security option enabled.
- Trusted execute
  The ability to execute an information object without having execute privilege for the information object's underlying data sources. This privilege applies only to information object (.iob) files.
- Visible
  The ability to view items in the Encyclopedia volume.
- Write
  The ability to place an item in an Encyclopedia folder.

About Page-Level Security and SmartSheet options

You purchase a license to use Page-Level Security to restrict user access to specific pages of a BIRT or Actuate Basic document. Users or security roles that have the secure read privilege can read specific pages of a document protected by page-level security. The BIRT SmartSheet Security option provides page-level security for a spreadsheet document by restricting access to data, worksheets, or data range sections of the document based on user name or security role.

About accessing files and folders

All users can view the root folder of the Encyclopedia volume. A user must have the visible privilege to see items in the root folder. An administrator can specify a home folder for a user. When you log in to Management Console, you see your home folder. You have visible, read, and write privileges for your home folder.

By default, a user who creates a file or folder in the Encyclopedia volume owns the item and has full privileges to access it. A user with privilege to read a file can copy it and become the owner of the copy. If an administrator deletes a user, the administrator becomes the owner of all files and folders that the deleted user owned. An administrator always has full privileges on all items in the Encyclopedia volume.

Planning how to assign privileges

You need to understand the privileges required to run designs and perform other tasks, so you can devise an effective security strategy. Table 9-1 lists the privileges that a user needs to perform typical tasks with items in the Encyclopedia volume. You set the privileges on a particular item in the Encyclopedia volume, such as a design or folder. For example, to read future documents that a scheduled design generates on a regular basis, you give users or roles privilege to read the design. To read an existing document, you set the privilege on the document itself.

Table 9-1 Privileges to access files and folders

Tasks	Required privileges
Copying an item from one folder to another	Visible—item Visible—destination folder Write—destination folder
Creating a query definition (.dov) file	Visible—dependent files Read and execute—dependent files and information object
Deleting a folder	Visible—folder Delete—folder Delete—files in the folder
Deleting a file	Visible Delete
Downloading contents of a document	Visible—design or document Read—design or document
Downloading a document with restricted content	Visible—document Read and Execute—document
Moving an item	Visible—item Visible—destination and source folders Write—destination and source folders
Opening an Actuate search definition (.ros) file created by another user	Visible—the search definition file Read—the document file Read and execute—the executable file
Printing a document on an iServer printer	Visible Read

Table 9-1 Privileges to access files and folders

Tasks	Required privileges
Reading contents of a document	Visible—design or document Read—design or document
Reading restricted contents of a document	Visible—the document Secure read—the design or document
Running or scheduling a designto run	Visible—design Execute—design Read—design Delete—pre-existing document file if it is replaced
Running a document with restricted content	Visible—the document Read and Execute or Secure read—document Execute—design
Setting privileges to access an item	Visible Grant
Viewing a file or folder in a list of files or folders	Visible, Read, or Secure read
Viewing a cube	Read—the cube Read—the cube profile
Viewing the properties of an item	Visible, Read, or Secure read

Table 9-2 lists the privileges that a user needs to perform typical tasks in channels.

Table 9-2 Privileges to channels

Tasks	Required privileges
Reading a notice in a channel	Read or Secure read—document the notice contains
Sending a notice to a channel	Write
Subscribing to a channel	Read
Updating the contents of a channel	Write—channel
Viewing a channel	Read

Setting privileges to access an information object

If a user has trusted execute privilege to access an information object or data source map, iServer does not check the privileges of any data sources that the information object uses. If the user has only execute privilege, iServer checks the privileges of the underlying data sources before it runs the information object. Figure 9-2 shows an example of iServer checking privileges. MyObject uses the Source1 information object. Source1 uses Source2. If a user has execute privilege on MyObject and trusted execute privilege on Source1, iServer checks privileges on MyObject and Source1. iServer does not check privileges on Source2.

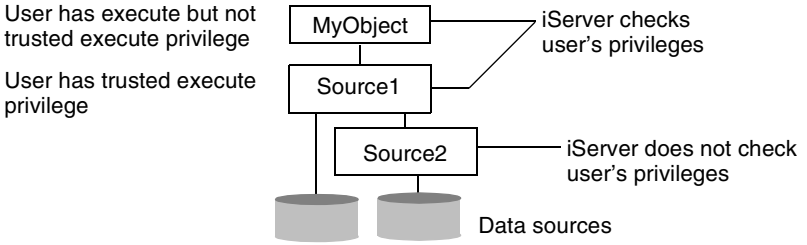

Figure 9-2 Using trusted execute privilege

In Files and Folders, the administrator can set the trusted privilege on Properties—Privileges for an information object, as shown in Figure 9-3. iServer removes the trusted execute privilege when you update or copy an object.

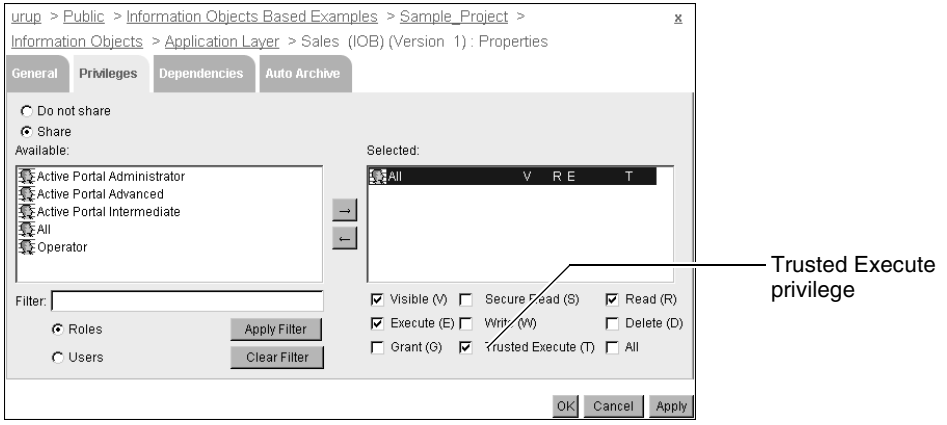

Figure 9-3 Assigning trusted execute privilege to a role

Using page-level security

BIRT Page Level Security option supports page-level security for BIRT designs (.rptdesign). e.Report Page Level Security option supports page-level security for Actuate Basic designs (.rox). Design developers create a design using security rules that determine which pages or parts of a document a user can view. The design defines a list of users and security roles that can access the document's groups and sections. In the design, the list can be a static list or an expression that generates a list based on information in the design. iServer uses this list to generate the access control list (ACL) for each document page.

Viewing reports using page-level security

When a user views a document that uses page-level security in an Encyclopedia volume, the View process retrieves the user's ACL from the volume. Then iServer compares the user's information with the ACL for each page in the document to determine which pages the user can view.

Enabling page-level security

To use page-level security in shared documents, administrators must assign the following privileges in addition to the visible privilege:

- To have limited read access, users or security roles must have secure read privilege on the design or document file.
- To run the design, users or security roles must have read and execute privileges. A user who generates a document file can also delete the document file if it replaces a previously generated one.
- To run the document, users or security roles must have read and execute privileges, or secure read and execute privileges on the document. They must also have execute privilege on the design.

If a user or security role has read privilege on a document that uses page-level security, users can view the entire document.

Using information object pass-through security

To connect to a data source, an information object uses a data connection definition (.dcd) file. The DCD specifies what security information, such as a user name and password, the information object uses to access data from the data source.

When creating a DCD, the data modeler uses Actuate Information Object Designer to specify the file's security policy as either proxy or pass-through.

- Using proxy security, the information object uses the security information specified in the DCD when it connects to a data source.
- Using pass-through security, the information object uses the security information provided by the volume administrator using Management Console.

Typically, you use pass-through security to avoid changing the name-value pairs set in the DCD by using Files and Folders in Management Console to specify alternate name-value pairs that override those in the DCD.

When associating using pass-through security with an Encyclopedia volume security role, the role must have only individual users as members. iServer does not support using nested roles with pass-through security.

How to configure an information object to use pass-through security

1 On Files and Folders, point to the arrow next to the name of a DCD, and choose Pass Through Security, as shown in Figure 9-4.

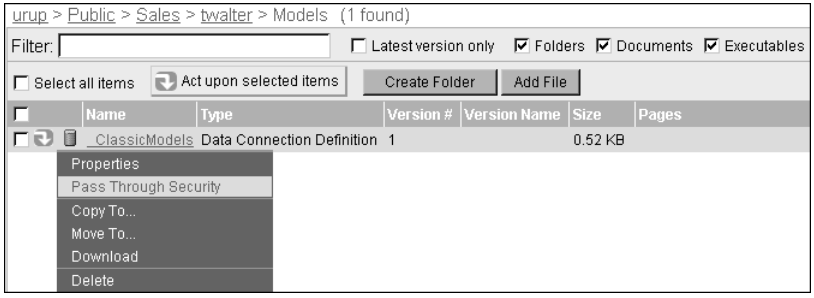

Figure 9-4 Configuring a DCD for pass-through security

2 To enable pass-through security for a user or role, on Files and Folders—Pass Through Security, select the user or role in Available, as shown in Figure 9-5.

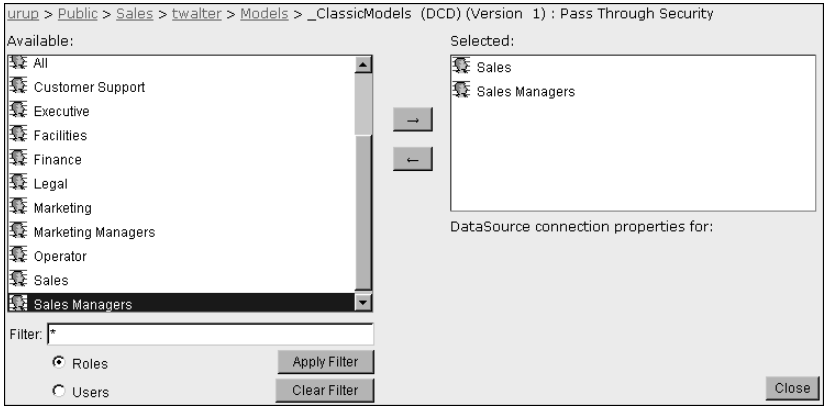

Figure 9-5 Specifying security roles or users

Choose the right arrow to move it to Selected.

3 To provide new values for DCD properties, select a user or role in Selected, as shown on the left in Figure 9-6. In this case, the Sales role is selected.

You specify any DCD property and value for it by choosing Add. Or, choose Add User Name and Password and specify values for the username and password properties only, as shown on the right in Figure 9-6.

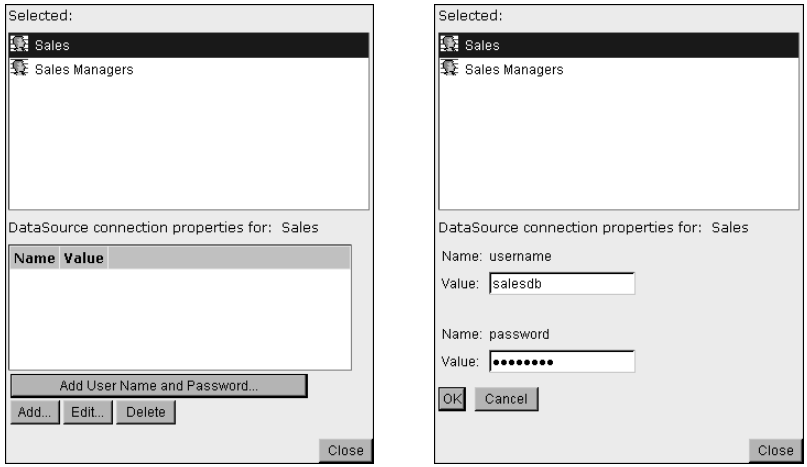

Figure 9-6 Setting data source connection properties

Choose OK.

4 If you need to modify the pass-through security settings, choose the role or user in Selected to display the pass-through properties and values.

Select the property and value to edit, then choose Edit, as shown in Figure 9-7.

Figure 9-7 Editing data source connection properties

Modify the value and choose OK.

5 To delete a pass-through property setting, choose the role or user in Selected to display the pass-through properties and values. Select the property and value to delete, then choose Delete.

About Open Security

Open Security is an Actuate Server Integration Technology that supports externalizing user registration and properties management to another system.

Using Open Security, developers use the Report Server Security Extension (RSSE) to create an interface to an external security source, such as a Lightweight Directory Access Protocol (LDAP) server. Using the interface, iServer retrieves information from the external security source to control access to the Encyclopedia volume. Developers create an interface to the Encyclopedia volume that performs various levels of security integration based on an external security source.

You need to understand the following terms associated with the application:

- Authentication
  The process of verifying user login information. A user sends the login information to authenticate the user's identity. For example, a password confirms that the user is entitled to use a particular user ID. More complex authentication mechanisms include a smart card that a user must run through a reader, a digital certificate, or biometric data such as a fingerprint.
- Authorization
  The process of determining whether an authenticated user is allowed to access a particular resource. For example, iServer determines whether a user has the right to access a particular item in an Encyclopedia volume.

About RSSE

Using the Java Report Server Security Extension (RSSE), a developer can create an application that controls security for an Encyclopedia volume. iServer can use internal security functionality or an RSSE application to use external security information. In either situation, iServer uses privileges to control access to Encyclopedia volume information.

Actuate provides a set of applications that use a Java RSSE service in \Actuate11 \ServerIntTech\Java Report Server Security Extension. This library shows how

you can create a driver within the Java RSSE framework. The directory contains subdirectories for three areas of RSSE functionality:

- External authentication
  You can authenticate users in the Encyclopedia volume based on an external, third-party security system. You can see a Java RSSE service implementing external authentication in \Actuate11\ServerIntTech\Java Report Server Security Extension\LDAP_Authentication_Example. For more information about this application, see readme.doc in that directory.

- External registration
  You can control access to Encyclopedia volume items based on information from an external security system. With this strategy, you externalize users, roles, groups, and user properties. You can see a Java RSSE service that implements external user registration in \Actuate11\ServerIntTech \Java Report Server Security Extension\LDAP. For more information about this application, see readme.doc in that directory.

- Changing access control lists (ACLs) to control access to reports that use page-level security
  By default, the Encyclopedia volume returns the user and all security roles to which the user belongs. You can control access to data in a report using page-level security based on information from an external third-party security system. When you use an external third-party security system, an application typically needs to translate the BIRT iServer list to an application-specific access control list. You can see this type of application using a Java RSSE service in \Actuate11\ServerIntTech\Java Report Server Security Extension\ Page_Security_Example. For more information about this application, see readme.doc in that directory.

For more information about RSSE, see the following resources:

- Chapter 10, Using Java Report Server Security Extension, in *Using BIRT iServer Integration Technology.*
- In the directory into which Server Integration Technology installs, see \Java Report Server Security Extension\LDAP\readme.txt. Server Integration Technology typically installs into Program Files\Actuate11\ServerIntTech on Windows platforms and AcServer/ServerIntTech on UNIX and Linux platforms.

Open Security levels

Open Security can be configured for one of several levels of use. Table 9-3 lists and describes all Open Security levels.

Table 9-3 Open Security levels

Level	Description
Open Security not used	The Encyclopedia volume stores information such asusers, security roles, notification groups, and privileges.
External user authentication	The Encyclopedia volume stores information such as users, security roles, and notification groups. At login, a Report Server Security Extension application authenticates users externally. A Report Server Security Extension application maps the user to an Actuate user. Complex credentials are supported.
External user properties	The Encyclopedia volume stores information such as users, security roles, and notification groups. Some or all user properties can be specified in an external security source. External or internal user authentication can be used.
External user registration	An external security source stores information such as users, security roles, and notification groups. All user properties are obtained externally. External user authentication must be used.

The Open Security application that ships with iServer uses the External user registration level. Use the External user properties level with the Open Security not used level or with the External user authentication level.

The following Open Security applications ship with iServer:

- External authentication

  The Open Security application uses security information from a Sun ONE Directory Server, an LDAP server, to control attempts to log in to the Encyclopedia volume. The LDAP server stores only authentication information, such as a user's login and password.

- External registration

  The Open Security application uses external registration, where all user information is stored in the LDAP server.

About external user authentication

Using a Report Server Security Extension (RSSE) application, iServer accesses an external security source to authenticate user credentials, such as a user name and password, when a user attempts to log in to the Encyclopedia volume. The security extension application evaluates the credentials and determines whether they are valid. If the application validates the credentials, it determines which Actuate user account should access the Encyclopedia volume.

At this Open Security level, Actuate user accounts and Actuate security roles are defined in the Encyclopedia volume. Each user must be defined in the Encyclopedia volume. Privileges are defined, using Actuate user names and security roles, for access to folders and other items, such as reports, jobs, and channels.

About external user properties

Using Open Security functionality, you can store any combination of the following Actuate user properties in an external security source:

- E-mail address
- Web viewing preference
- Home folder
- Privilege template
- Maximum job priority
- Security IDs for page-level security
- Notification preferences
- Channels to which a user subscribes

If a property is specified externally, the property's value in the Encyclopedia volume is ignored. You cannot use Management Console to update that property.

At this Open Security level, the following information is managed within the Encyclopedia volume:

- User name
- Security role membership
- Notification group membership
- Privilege rules, in the form of access control lists (ACLs) for folders and other items, such as reports, jobs, and channels

About external user registration

Using this level of Open Security functionality, an RSSE application obtains all user information from the external security source. The RSSE application determines whether the user credentials are valid and specifies the user's properties. You can use page-level security with this level of Open Security.

At this Open Security level, the Encyclopedia volume passes the user's login ID and credentials to the RSSE application. The application evaluates the credentials and determines whether the user can access the Encyclopedia volume and, if so, what the user properties are.

The external security source maintains the following user information:

- User name
- E-mail address
- Web viewing preference
- Home folder
- Privilege template
- Maximum job priority
- Security role membership
- Security IDs for page-level security
- Notification preference
- Notification group membership
- Channels to which the user subscribes

At this Open Security level, you do not specify or store the user in the Encyclopedia volume. If your security source contains user profiles having the appropriate user information, developers can create an RSSE application that uses this information. You do not have to duplicate the user information in the Encyclopedia volume.

You define privileges for files and folders using security roles or user names. Use Management Console to assign privileges.

At this Open Security level, the external security source provides the identities of users, security roles, and notification groups. The external security source provides a single, unique identity for each Encyclopedia volume user, security role, and notification group.

Master lists of users, security roles, and notification groups are not in the Encyclopedia volume. Instead, the Encyclopedia volume uses the RSSE application to retrieve lists of users, security roles, and notification groups and their properties.

The Encyclopedia volume stores ACLs for each folder and other items, such as reports and other files in the Encyclopedia volume, jobs, and channels. The ACLs contain the user and security role names from the RSSE and the privileges assigned to each user and security role.

About externally defined security roles

When using an RSSE application with externally defined Actuate security roles, the security roles cannot be nested. For example, if the security roles Supervisor and Manager are defined externally, the Supervisor security role cannot be a child of the Manager security role.

About the All security role and external registration

The All security role is a system security role to which all users belong. When using external registration, developers can create an RSSE application that enables or disables the All security role in the Encyclopedia volume.

About the anonymous user and external registration

When using external user registration, iServer does not support the special user with the name anonymous. If no Open Security is used, and the anonymous user is present with no assigned password in the Encyclopedia volume, the anonymous user is used as a default login for the Encyclopedia volume.

When using external user registration, a developer must set up the external security source and RSSE application to support connecting as anonymous. To do so, the RSSE application must accept a login with the user name anonymous and no password.

About the Administrator security role and external registration

The Administrator security role is a system security role with administrative privileges. A user belonging to the Administrator security role can access any item in the Encyclopedia volume. An administrator performs functions such as creating users and security roles and assigning privileges.

About the administrator user and external registration

When an Encyclopedia volume uses external user registration, for a user to administer the Encyclopedia volume, the user must belong to the Administrator security role.

For example, when configuring the RSSE application that ships with iServer, you specify a role in the external security source that the Encyclopedia volume uses as the Administrator role. A user who is a member of the role has Encyclopedia volume administrative privileges.

About the Operator security role and external authentication

The Operator security role is a system security role. Members of the Encyclopedia volume's Operator security role can transition the Encyclopedia volume to read-only mode for online backup and return the Encyclopedia volume to normal mode from read-only mode. When using external registration, the Operator security role is defined in the Encyclopedia volume. Users who are assigned to the security role named Operator have the same capabilities in the Encyclopedia volume.

About channels and external authentication

The Encyclopedia volume maintains a list of channels. The Encyclopedia volume or an external security source maintains the list of channels to which a user subscribes.

Using Management Console with Open Security

Using Open Security functionality, developers can create a custom login from an Actuate desktop product to the Encyclopedia volume. The login application passes the login information from the desktop product to the Encyclopedia volume for authentication. Using the iPortal Security Extension, developers can create a custom login to be used when accessing the Encyclopedia volume with a web browser and Information Console.

Home folder privileges, printer properties, and other properties are affected when you use Open Security.

About home folder privileges

If the Encyclopedia volume uses the Open Security RSSE application that ships with iServer, iServer assigns the default privileges for the externally defined user's home folder.

About printer properties

The following levels exist for setting printer properties for externally defined users:

- Default printer properties for the Encyclopedia volume
- Default printer properties for a user
- Printer properties for a specific job

If the Encyclopedia volume is using Open Security, and users are defined externally, iServer disables the ability to modify default printer properties for a user.

About externally defined properties

Any fields that are used for properties defined externally are disabled. Figure 9-8 shows how user properties appear when the user name, password, e-mail address, and home folder are defined externally. Each of these fields is read-only.

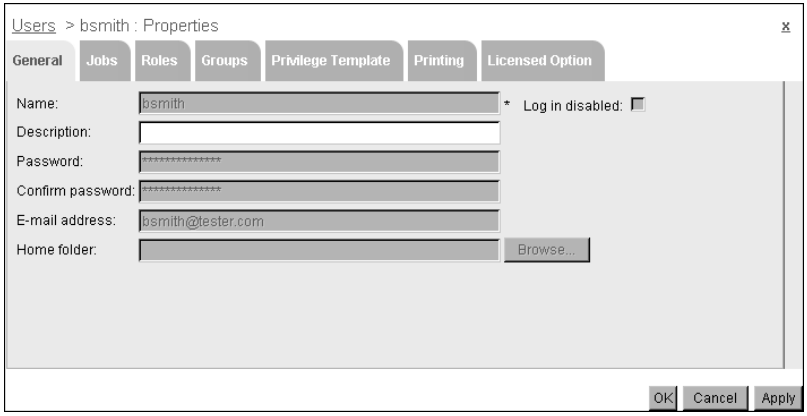

Figure 9-8 Viewing externally defined properties

About searching when using an RSSE application

iServer limits the number of search conditions that you can impose when the Encyclopedia volume uses an RSSE application that uses external registration. When searching for a security role, user, or notification group, iServer supports using only one search condition for each search. You can use the wildcard character, or an asterisk (*), in Filter on any page in Management Console if the Encyclopedia volume uses Open Security.

Using RSSE with page-level or SmartSheet security

Using the Report Server Security Extension (RSSE) and page-level or SmartSheet security, developers can create an RSSE application that associates security IDs in an ACL to one or more users or security roles.

For example, a design developer can create an Actuate Basic design that contains Demo as a security ID in some of the design's ACLs. Using an RSSE application, Demo does not have to be a user or security role. The RSSE application can take the security ID Demo and map it to a set of users. When a user who is associated with Demo views the document the design generates, that user can see the document pages for which the page's ACL contains Demo.

Index

Symbols

, (comma) character 123
: (colon) character 123
* wildcard character 14, 195
\ (backslash) character 15

A

About page (Management Console) 13
AC_DATA_HOME variable 93
AC_JDRV_CLASSPATH parameter 164
AC_JDRV_LAUNCH_WAIT parameter 163
AC_JDRV_LOG_LEVEL parameter 164
AC_JDRV_TIMEOUT parameter 164
AC_JRE_HOME parameter 163
AC_JVM_PARAMETERS parameter 163
AC_RUNNING_HEADLESS parameter 165
AC_SS_BOOKCACHESIZE parameter 165
AC_SS_CONNECTION_OVERRIDE parameter 165
AC_SS_DESIGNDPI parameter 165
AC_SS_DPI parameter 165
access control lists
  accessing external data and 193
  accessing reports and 185
  associating with security roles 195
  changing 189
  creating 169, 185, 189
access permissions. *See* privileges
access restrictions 59, 60, 114, 180, 181, 185
accessing
  channels 138, 139
  console applications 2
  cube data sources 159, 160, 161
  cube reports 60
  Encyclopedia volumes 20, 22, 31, 190, 194
  external security information 188
  external security sources 188
  files or folders 54, 58, 181
  information objects 184
  reports 54, 58, 181
  resources 188
  sample applications 188, 190
  sample designs 5, 6
  user accounts 11
accounts
  accessing 11
  changing user properties for 31
  cloning 36
  creating user 20, 21, 22
  deleting 37, 38
  determining status of login 15
  external security sources and 192
  setting user properties for 29
ACLs. *See* access control lists
Act upon selected channels icon 142
Act upon selected groups icon 150
Act upon selected items icon 61, 70
Act upon selected users icon 31
Active Portal Administrator role 42
Active Portal Advanced role 42
Active Portal Intermediate role 42
Actuate Analytics Option. *See* Analytics Option
Actuate Basic reports 2, 112, 181
  See also reports
Actuate BIRT iServer Properties dialog 3
Actuate Query. *See* queries
Actuate Query Generation page 158
Actuate Query Option 156
Actuate Query Wizard. *See* Query Wizard
Add File page 73
adding
  archiving policies 66, 69, 70, 170, 173
  cache tables 86
  channels 139, 140
  file dependencies 76
  folders 71
  information objects 83
  notification groups 147, 148, 169
  passwords 22
  resource groups 98
  security roles 40, 43, 44, 47, 169
  user accounts 20, 21, 22
  user names 22
  users 22, 36

addresses (e-mail) 22
Administrator role 9, 41, 193
Administrator user 9, 193
Administrator user accounts 20
administrators
  accessing external security sources and 193
  accessing report files and 54, 58, 180
  assigning privileges and 58, 60, 182, 184, 185
  creating security roles and 40, 41, 43
  defining functionality levels and 42
  deleting user accounts and 37
  filtering user lists and 14, 15
  managing channels and 138, 139
  managing Encyclopedia volumes and 2, 54, 168, 181
  managing users and 9, 11, 20
  scheduling jobs and 94, 97, 98, 127
  troubleshooting strategies for 119–121, 163
Advanced property 95
aging cycles (autoarchiving) 173, 174
aging intervals (autoarchiving) 63, 68
aging intervals (channel properties) 140
aging rules. *See* archiving rules
AIS. *See* Integration service
All role 42, 175, 193
Allow browser-side caching setting 174
Always use latest version setting 98
Always use version number setting 98
Analytics Cube Designer 159, 160
Analytics Cube Viewer 158, 160
Analytics file types 159
Analytics Option 158, 160
analyzing data 158
anonymous users 193
application programming interfaces (APIs) 7, 171
applications
  accessing sample 188, 190
  creating 96, 188, 195
  externalizing user information and 192, 193, 194, 195
  generating access control lists for 189
  logging in to Encyclopedia and 194
  managing external user properties and 191
  verifying user information and 191, 192
Apply these privilege settings setting 72
AQTemplate.rod 157
archive applications 171
archive drivers 68, 105
Archive files before deletion setting 68, 77
archive libraries 170, 172
Archive Schedule button 174
archive service providers 171
Archive the document before deletion setting 105
Archive the files before deletion setting 69
Archive this file before deletion setting 68
archiving
  folders 63–71, 170
  jobs 104
  report files 63–71, 170–174
Archiving and Purging page (System Volumes) 129
Archiving and Purging page (Volume Properties) 128, 172, 173
archiving options 65, 67, 76
archiving policies
  changing 67
  creating 66, 69, 170
  displaying 67, 77, 104
  inheriting 67, 170
  running jobs and 104
  setting aging intervals for 63, 68
  setting archiving properties and 65
  setting default 67
  setting for multiple files 67, 69, 70
  setting on Encyclopedia 172, 173
  setting on folders 65, 67, 69, 72
  uploading files and 76
archiving properties 63, 65
archiving rules 74
  See also archiving policies
Attach document setting 23, 116
attachments 23, 86, 106, 116
authentication 188, 189, 191, 192, 194
authorization 188
Auto Archive Now button 173
Auto Archive page (Files and Folders Properties) 56, 63, 65, 69, 70, 76
Auto Archive page (New Folder) 72
Auto delete after property 140

autoarchive applications 171
autoarchive drivers 68, 105
Autoarchive policy property 104
Autoarchive rules property 74
autoarchiving 63–71, 170–174
autoarchiving options 65, 67, 76
autoarchiving policies. *See* archiving policies
autoarchiving properties 63, 65
autoarchiving rules. *See* archiving rules
autoversioning options 73, 75, 98, 104
Available list (Privileges page) 60

B

background jobs. *See* scheduled jobs
backslash (\) character 15
Basic reports. *See* Actuate Basic reports
BIDI processing setting 108, 119
bi-directional data processing 108, 119
BIRT iServer. *See* iServer
BIRT report libraries 7
BIRT reports 2, 6, 107, 109, 181
  See also reports
BIRT Spreadsheet Designer 7, 162
BIRT Spreadsheet Option 162
bundling report files 104, 105
bursting 121

C

cache connection definitions 86
cache databases 86
  See also cache tables
cache objects 86, 87
cache states 87
cache tables 86, 87, 88
caching
  DHTML reports 174
  information objects 86–88
  spreadsheet books 165
Caching service 86
calendar 68
callback classes 162
cancelling jobs 121, 135
case sensitivity 22
.cb4 files. *See* cube data files
changing
  access control lists 189
  archiving policies 67
  autoarchiving options 67
  channel names 144
  channel subscriptions 35
  file names 57, 75
  file types 57, 75
  fonts 157
  headlines 106
  home folders 31
  job names 97
  job priorities 22
  job settings 134
  licensed options 34
  notification groups 32
  passwords 20
  printer settings 33, 117, 194
  privilege templates 33
  privileges 33, 60, 72, 142
  queries 84
  role properties 46, 48
  roles 32, 41, 51
  search conditions 18
  user properties 28–36
channel icons 140, 141, 145
Channel Privileges page (New Security Role) 45
Channel Subscriptions page (Users) 30, 35
channels
  accessing 138, 139
  changing privileges for 142
  changing subscriptions to 35
  cloning 144
  creating 139, 140
  deleting 144
  displaying 30
  distributing reports and 138
  externalizing information for 194
  naming 140
  removing notifications from 24, 128, 130, 135, 140, 173
  removing privileges on 142, 143
  removing subscriptions to 36
  renaming 144
  selecting 115, 141
  sending notifications to 24, 115, 128, 139, 169
  setting privileges for 30, 45, 139, 141, 143

channels *(continued)*
setting properties for 140, 142
subscribing to 29, 138, 169
unsubscribing from 138
updating 141
viewing completion notices and 130, 139
viewing documents in 147
viewing subscriber lists for 139, 144
Channels icon 10
Channels page (Management Console) 10, 138
Channels page (Schedule) 115
Channels property 94
character strings. *See* strings
characters
creating passwords and 22
creating user names and 22
entering in expressions 123, 125
filtering data and 14, 195
searching for 15
Chart DPI setting 108, 119
charts 107, 158
child roles 40, 49, 169
Child Roles page (New Security Role) 45
Child Roles page (Security Roles Properties) 49
classes 158
classpaths 164
clearing data filters 15
cloning
channels 144
notification groups 148
security roles 47
user accounts 36
clusters 93, 123, 124
Collate property 118, 176
colon (;) character 123
Column list setting 107
column names 107
columns in tabular lists 16, 17
Columns page (Search) 16
comma (,) character 123
comma-separated values files. *See* CSV output formats
completed jobs 31, 132, 147
See also jobs
Completed page (Jobs) 127, 135
Completed property 127, 132
completion notices 24, 117, 127, 138, 139
See also notifications
Configuration Console
archiving report files and 170, 171
connecting to external files and 160
customizing query templates and 158
managing Encyclopedia and 2
purging job notices and 24, 129
running event-based jobs and 96
running iServer services and 119
running spreadsheet reports and 163
Configuration file for connections parameter 160
configurations
activating cache objects and 87
connecting to spreadsheet reports and 163
customizing query templates and 158
enabling Datamart Security and 114
enabling Open Security and 190
generating data cubes and 160
printing and 119
specifying locale-specific formats and 124
starting iServer services and 3, 4
Configure page 87
ConnConfigFile parameter 163
connecting to
data sources 156, 157, 160, 185
spreadsheet reports 163, 165
connection definition files. *See* data connection definition files
connection information 156, 160, 165
connection properties 86, 163
connections, securing 185
Copy dialog 80, 81
copying
channels 144
file properties 74
folders 79–82
notification groups 148
report files 79–82
security roles 47
user properties 36
Create a new version setting 73, 75, 81
Create Parameter Values File dialog 102, 161
Created property 75

creating
access control lists 169, 185, 189
archiving policies 66, 69, 70, 170, 173
cache tables 86
channels 139, 140
file dependencies 76
folders 71
information objects 83
notification groups 147, 148, 169
passwords 22
PostScript files 118
privilege templates 25
queries 83–84
resource groups 98
RSSE applications 188, 195
security roles 40, 43, 44, 47, 169
user accounts 20, 21, 22
user names 22
users 22, 36
Criteria page (Search) 16
CSV output formats 107, 109
cube data files 159
Cube Designer 159, 160
cube file types 159
cube profiles 158, 159
cube reports 60, 158, 159, 160
Cube Viewer 158, 160
cube views 159
cubename parameter 160
custom events 96
customizing
date-and-time formats 122, 123, 125
Encyclopedia logins 194
job schedules 95
Management Console 11
printer settings 175
query templates 157, 158
.cvw files. *See* cube views

D

Dashboard folder 6
dashboard sample designs 6
data
analyzing 158
displaying 83, 157, 160
exporting 112
filtering 13, 15, 114
retrieving from
data cubes 158, 159, 160
data sources 2
databases 90
external security source 188, 192
information objects 156, 185
searching for 16, 195
data connection definition files 73, 185, 187
data cube file types 159
data cubes 158–161
See also cube reports
data filters 13, 15, 195
Data Integration Option 156
data object executable files 156, 157, 158
data object instance files 83, 157
data object value files 83, 84
data rows. *See* rows
data sets 107
data source map files 59, 73, 156, 184
data sources
accessing data cubes and 159
connecting to 156, 157, 160, 185
retrieving data from 2, 156, 185
running information objects and 157, 184
data types 107
database drivers 159, 164
See also drivers
databases 86, 90, 156, 160
Datamart Security 114
datasourcename parameter 160
datasourceprovider parameter 160
date expressions 122, 123, 124
date format symbols 124
date formats 122, 123
date stamps 75, 122, 124, 125
dates 68, 107, 123
.dcd files. *See* data connection definition files
debugging options 164
default archiving policy 66, 67, 172
default font 157
default printer 26, 33, 177
default resource groups 98
Default user notice purging options 24
default values 102
default wait period 96
Delete after date/time setting 65, 68

Delete cache table setting 87
Delete notice options 24
delete privilege 58, 78, 180
Delete when older than setting 65, 68
deleting
  cache tables 87
  channel subscriptions 36
  channels 144
  file dependencies 76
  folders 63, 72, 78, 79
  job information 121
  jobs 135
  licensed options 27, 34
  notification groups 152
  notifications 24, 128, 130, 135, 140, 173
  privileges 33, 40, 61, 142, 143
  report files 63, 68, 78, 79
  security roles 32, 48, 51
  subfolders 66
  temporary files 93
  user accounts 37, 38
  users 181
demand paging 106
dependencies. *See* file dependencies
Dependencies page (Files and Folders Properties) 56, 62, 76
Dependencies page (Properties) 120
description parameter 160
Description property 74, 75, 140
design elements 7
design files 6, 58, 107, 185
design templates 157
design tools 71, 162
designs 6, 7, 21, 90, 91, 157
DHTML formats 59, 174
DHTML reports 174
DHTML viewer 113
directories
  accessing data cubes and 159
  accessing sample RSSE application and 188
  displaying channel icons and 146
  storing temporary files and 93
directory paths
  current volume folder 5
  event-based jobs 95
  home folders 22
  JRE installations 163
  report executables 62
  XML data files 160
displaying
  archiving policies 67, 77, 104
  channel icons 145
  channel subscribers 139, 144
  channels 30
  completion notices 130, 138, 139
  data 83, 157, 160
  file or folder information 54, 55, 56
  file type properties 67, 156
  file types 65
  files 5, 58
  job information 121, 127, 131–134
  licensed options 27, 34
  notification groups 147
  printer information 118, 177
  query output 85
  reports 147, 185
  sample designs 6
  scheduling information 133
  security roles 43
  user account information 11
distributing reports 24, 115, 138
Do not archive file before deletion setting 67, 172
Do not automatically delete setting 65, 67, 68, 172
Do not share setting 60, 61, 72
document files
  accessing data cubes and 159
  archiving 67
  assigning privileges to 58, 113, 185
  attaching to e-mail 23, 86, 106, 116
  converting 94, 107, 109, 112
  distributing over channels 24, 115, 138
  embedding executable files in 105
  generating 71, 90, 91, 105
  running 97
  setting dependencies for 76, 120
  viewing information about 133
Document format property 103, 104, 106, 112
Document name property 103
document names 122
documentation vii

documents 2
See also document files; reports
.doi files. *See* data object instance files
.dov files. *See* data object value files
downloading report files 59, 82
.dox files. *See* data object executable files
.dp4 files. *See* cube profiles
DPI settings 165
drivers
accessing cube data sources and 159
archiving report files and 68, 105
creating 188
retrieving data and 156, 157
running spreadsheet reports and 164
Duplex property 118, 176
dynamic hypertext markup language. *See* DHTML formats

E

Edit Schedule dialog 95
editing. *See* changing
e-mail
See also notifications
attaching reports to 23, 86, 106, 116
entering user addresses for 22
sending 23, 116, 169
Embed the executable… property 104, 105
Embedded font setting 108
Enable pivot table setting 107
encoding options 107
Encoding setting 107
Encyclopedia volumes
accessing items in 54, 58, 181
adding items to 71, 73, 83
aging items in 170, 172, 173
archiving items in 63–71, 170–174
authenticating users for 189, 191, 192, 194
controlling access to 188
creating users for 36
deleting user accounts and 37
downloading files to 59, 82
externalizing user information for 189, 190, 191, 192, 193, 194, 195
filtering data in 13–15
logging in to 20, 22, 31, 190, 194
managing reports in 2, 54, 78, 168
navigating through 5
preserving items in 68
printing reports and 26, 175–177
publishing information objects to 83
publishing spreadsheet reports to 162
removing items from 68, 78, 93, 170
restricting access to items in 59, 60, 114, 180, 181, 185
running jobs and 100, 101, 119
saving cube reports in 158, 159
searching 16–18
setting privileges for 54, 180, 182
setting properties for 168, 172
specifying home folder for 22
uploading files to 57, 71, 73, 158
uploading spreadsheets to 162
viewing items in 5, 58, 181, 185
viewing privileges on 175
viewing specific file types in 65
error messages 120, 165
errors 96, 125, 163
event states 132
event-based jobs 94, 95, 96, 119, 132
events 95, 132
Examples folder 6
Excel output formats 86, 107, 112
Excel spreadsheets 107, 112, 162
See also spreadsheet reports
executable file types 159
executable files
See also specific Actuate report executable
bundling with report documents 104, 105
creating 157
opening report documents and 62
publishing spreadsheet reports and 162
running 62, 157
setting dependencies for 76, 120
viewing information about 133
execute privilege 58, 180
execution failed messages 121
expiration policies 129
Export charts as images setting 107
Export columns data type setting 107
exporting data 112
expressions
entering literal characters in 15, 125
generating access control lists and 185

expressions *(continued)*
naming files and 122, 123, 124, 125
external archiving tools 171
external authentication 189, 190, 191, 194
external authorization application 190
external files 160
external registration 189, 190, 192–193, 195
external registration application 190
external security information 188
external security sources
See also Open Security applications
accessing Encyclopedia and 189, 193
authenticating users and 189, 191, 192, 194
defining anonymous users and 193
interfacing with 188
obtaining user information from 192, 194, 195
prioritizing jobs and 22
running sample applications for 190
storing user properties in 191
external security systems 189
external user properties 190, 191, 192, 194, 195

F

Factory processes 98, 157, 163, 164, 165
Factory service 93, 119
failed jobs 98, 100, 101
features 42
file dependencies
migrating 73
missing 119
opening report documents and 62
removing 76
running parameter values files and 63
saving queries and 157
setting 76, 120
updating 63
file descriptions 74, 75, 78
File Download dialog 83
file events 95
file name extensions 103
file name restrictions 78, 123
file names 57, 75, 103, 122
file paths. *See* directory paths
file size property 75
File Type list (Auto Archive Folder Properties) 65
File type property 74, 172
file types
accessing data cubes and 159
accessing report designs and 6
archiving specific 66, 67, 69, 170, 172
changing 57, 75
creating 78
displaying 65
generating output and 103
running queries and 156
setting parameters for 163
setting privileges across 61
setting properties across 74
viewing properties of 67, 156
viewing spreadsheet reports and 162
File Types icon 10
File Types page 10, 156
files
See also specific type
accessing 54, 58, 181
archiving 63–71, 170–174
assigning privileges to 58, 59, 72
bundling 104, 105
changing privileges for 60
converting 94, 107, 109, 112
copying 79, 81
deleting 63, 68, 78, 79
displaying archiving policies for 67, 77, 104
displaying information about 54, 55, 56
downloading 59, 82
marking as private 60, 61, 72
moving 79, 81
naming 103, 122
preserving 68
printing to 117, 118
removing privileges on 61
removing temporary 93
renaming 57, 75
restricting access to 72
selecting 60
setting archiving policies for 65, 69, 70
setting autoversioning options for 73, 75
setting date/time stamps for 122, 123, 124, 125

setting properties for 55, 56, 74
uploading 57, 71, 73
viewing 5, 58
Files and Folders icon 10
Files and Folders page 5, 10, 54, 55
filtering
data 13, 15, 114
notification groups 115
user names 14
filters 13, 15, 195
Flash gadgets 6
folder names 6, 22, 78
Folder property 104
folders
accessing contents 58
archiving 63–71, 170
changing home 31
changing privileges for 60
changing properties for 175
copying 79, 81
creating 71
deleting 63, 72, 78, 79
marking as private 60, 61, 72
moving 79, 81
naming 71, 78
navigating through 5
preserving 68
removing items in 63, 68
removing privileges on 61
removing temporary files in 93
restricting access to 72
saving reports to 98, 104
selecting 6, 60
setting archiving policies for 65, 67, 69, 70, 72
setting privileges on 54, 58, 59, 72, 181, 194
setting properties for 55, 56
specifying home 22
updating privileges for 22
viewing archiving policies for 67, 77
viewing file types in 65
viewing information about 54, 55, 57
viewing items in 5, 58, 181
Font substitution setting 108, 119
fonts 108, 157
Format for attached report setting 116
format symbols 124, 125
formats
customizing 122, 123, 125
displaying data and 157
naming files and 122, 123, 124, 125
preserving 112
unescaped literal characters in 125
Fully Editable RTF formats 86, 112
functionality levels 42

G

gadgets 6
General Date formats 123
General page (Files and Folders Properties) 56, 74
General page (New Channel) 140, 144
General page (New Security Role) 44
General page (New User) 22
General page (Options) 12
General page (Security Roles Properties) 49
General page (Users Properties) 31
General page (Volume Properties) 101, 168, 174
General property 29
generating
access control lists 185, 189
data cubes 158–161
query output 83, 85
reports 71, 90, 91, 105
spreadsheet designs 163
temporary files 93
Get Images button 141
grant privilege 58, 180
graphics port 165
graphs 107, 158
groups. *See* notification groups
Groups page (New User) 24
Groups page (Personal Settings) 147
Groups page (Users Properties) 32
Groups property 29

H

Headline property 104, 106
headlines 106
heap 164
hidden parameters 102
hierarchical security roles 40

home folders 22, 31, 54, 181, 194
hyperlinks 23, 127
See also URLs

I

icons 10, 140, 141, 145
IDAPI 158
image files 140, 146
images 108, 119
immediate jobs. *See* unscheduled jobs
Information Console
accessing completion notices and 115
analyzing cube data and 158
defining functionality levels for 42
displaying channel icons in 145
localizing reports and 122, 123
logging in to Encyclopedia and 194
managing Encyclopedia and 2
Information Delivery API 158
information object data sources 157
Information Object Designer 86, 185
information object files 59, 73, 83, 156
See also specific type
information object template files 156
information objects
accessing sample files for 7
assigning privileges to 59, 184
building queries for 83–86, 158
caching 86–88
creating 83
defining connections for 156, 185
enabling security policy for 185, 186
retrieving data and 156, 157
running 59, 157
uploading 73
inheriting
archiving policies 66, 67, 170
privileges 40
installing system printers 175
insufficient privileges 119
Integration service 157
.iob files. *See* information object files
iPortal Security Extension 194
iServer
accessing external user information and 188, 195
accessing external user information for 188
archiving files on 63–71
assigning privileges and 184
autoarchiving and 171, 173
bursting reports and 121
changing notification group names and 152
configuring query templates for 158
displaying channel icons on 145
displaying file types on 65
displaying reports and 147
downloading files to 59, 82
generating data cubes and 158, 159, 160
generating spreadsheet reports and 163
generating temporary files and 93
localizing reports and 122, 124
nesting security roles and 40, 186
overview 2
preserving items on 68
printing reports and 117, 176, 177
publishing to 83, 162
removing items on 68, 78, 93
retrieving data and 156, 157
running event-based jobs and 96, 132
running reports on 62, 90, 91, 93, 162
running scheduled jobs and 93, 95, 96, 100, 127, 135
running unscheduled jobs and 96
saving query output and 85
saving reports to 91, 93, 98, 104
sending notifications over 23, 117, 127, 139
specifying parameters and 102
specifying wait period for 98
uploading files from 57, 71
viewing information about 13
viewing licensed options for 27, 34
iServer Enterprise service properties 3
iServer reporting environments 2
iServer services 2, 3, 4, 119
See also specific service

J

Java Report Server Security Extension. *See* Report Server Security Extension
Java Runtime Environment 163
Java Virtual Machines 163

Java-based autoarchive application 171
JavaScript API 7
JDBC drivers 159
job events 96
Job Schedule Builder 95
Job Selector 96
jobs
  adding new users and 23
  archiving 104
  cancelling 121, 135
  changing settings for 134
  creating notification groups for 147
  creating resource groups for 98
  deleting 135
  displaying information about 121, 131–134
  generating query output and 85
  monitoring 90, 127
  naming 97
  printing reports and 119, 176
  refreshing cache tables and 88
  running event-based 94, 95, 96, 119, 132
  running recurring 122
  running scheduled 95, 96, 98, 119
  running unscheduled 91, 94, 96, 119
  saving 102
  scheduling 93–98, 100, 103, 113, 115
  sending completion notices for 24, 115, 128, 139, 169
  setting event types for 95
  setting output options for 103, 105
  setting parameters for 101–103
  setting priorities for 21, 23, 31, 98
  setting privileges for 113
  setting properties for 94, 131
  setting retry options for 98, 100, 101
  timing out 96
Jobs icon 10
Jobs page (Management Console) 10
Jobs page (New Users) 23
Jobs page (Personal Settings) 116, 139
Jobs page (Users Properties) 31, 128, 139
Jobs property 29
JRE_HOME environment variable 163

K

Keep only the latest *n* versions setting 75, 81

L

language settings 5, 13, 68
Large (32x32) icon URL property 140
LDAP sample applications 189
LDAP servers 188, 190
libraries 7, 170, 172, 188
Licensed Option page (New User) 27
Licensed Option page (Users Properties) 34
Licensed Option property 29
licensing options 34, 121, 156, 158, 162, 171, 181
Lightweight Directory Access Protocol. *See* LDAP servers
links 6
  See also hyperlinks; URLs
Linux systems 4, 93
  See also UNIX systems
lists
  customizing Management Console and 11
  external user information and 192
  filtering items in 13, 16
  viewing access permissions and 185
  viewing channel subscribers and 139, 144
literal characters 15, 125
locale maps 122, 123
Locale neutral format setting 107
locales
  archiving and 68
  changing fonts for 157
  formatting date and time formats for 122
  formatting date and time values for 122, 123, 125
  scheduling jobs for 97
  viewing information about 13
lock files 93
Log in disabled list 15
Log in disabled setting 22
logging in to
  Encyclopedia volumes 20, 22, 31, 190, 194
  Management Console 2, 5
login accounts 15
login applications 194
login information 20, 188
logins
  customizing 194
  defining anonymous users and 193

logins *(continued)*
disabling 22, 31
verifying user information for 188, 191
Long Date formats 123
Long Time formats 123

M

Management Console
accessing external data sources and 195
analyzing cube data and 158
archiving and 63, 65, 67, 68, 69, 70, 170
assigning privileges and 59, 60, 180, 192
changing channel subscriptions and 35
changing user properties and 28, 31
creating user accounts and 21, 22
defining functionality levels and 42
distributing reports and 86, 106, 115, 116
enabling Open Security and 194
filtering data for 13–15
generating reports and 91, 105
localizing reports and 122, 123
logging in to 2, 5
managing channels and 138, 139
managing Encyclopedia and 2, 54, 168
managing report files and 54, 55, 78
managing security roles with 43
managing users and 9, 20, 22
naming restrictions and 78
navigating report files and 5
querying information objects and 83, 85
running information objects and 86, 186
running jobs and 90, 94, 97
running Open Security applications and 22
searching volume data for 16
sending notifications and 127, 128, 130
setting display options for 11
setting volume properties and 169
starting 4
troubleshooting strategies for 119–121, 163
uploading files and 73, 162
map files. *See* data source map files
mapping security IDs 195
Maximum job priority setting 23
Maximum rows setting 107
Medium Date formats 123
Medium Time formats 123
menus 9, 11
methods 158
Microsoft Analysis Services 159, 160
Microsoft Excel spreadsheets 107, 112
Microsoft SQL databases 159, 160, 161
migrating file dependencies 73
missing file dependencies 119
Mode property 118, 176
Move dialog 80, 81
moving report files and folders 79–82

N

Name property 74, 140
names
See also user names
adding date or time stamps to 122, 123, 124, 125
changing notification group 152
creating folders and 78
displaying icons with 145
filtering on 14
running jobs and 97
specifying home folders and 22
uploading files and 78
viewing folder 5, 6
naming
channels 140
folders 71, 78
jobs 97
notification groups 148, 152
report files 103, 122
security roles 44
users 22
naming conventions 22, 78, 140, 152
nesting security roles 40, 186, 193
New Channel page 140
New Folder page 71
New Notification Group page 148, 149
New Security Role page 44, 48
New User page 22
notification groups
adding users 24, 149, 150
cloning 148
creating 147, 148, 169
deleting 152

displaying 147
editing descriptions 152
enabling Open Security for 190
externalizing information for 189, 192
filtering 115
naming 148, 152
removing users 32, 150, 151
renaming 152
searching for 195
selecting 150
sending completion notices and 115
updating 32
Notification Groups icon 10
Notification Groups page 10, 147
Notification page (Schedule) 115
Notification property 94
notifications
See also e-mail; notification groups
adding new users and 23
deleting 24, 128, 130, 135, 140, 173
displaying 130, 138, 139
running queries and 86
sending to personal channels 24, 115, 128, 139, 169
setting options for 24, 31, 116
setting properties for 128, 129
specifying headlines for 106
Number of copies property 118, 176

O

ODA drivers 156, 157
ODBC data sources 160
.odp files. *See* OLAP parameters files
OLAP parameters files 159, 160, 161
olapserver parameter 161
Once property 95
on-demand paging 106
online archive API 171
Online Archive Option 171
online documentation vii
open data access drivers. *See* ODA drivers
Open Security applications
accessing sample 190
assigning privileges and 22
authenticating users and 191, 192, 194
configuring 190
defining anonymous users and 193
defining security roles and 193
externalizing user information and 192, 193, 194, 195
filtering data and 195
logging in to Encyclopedia and 194
managing external user properties and 191
printing reports and 194
prioritizing jobs and 22
setting home folder privileges and 194
Open Security technology 188
opening
Job Schedule Builder 95
Query Wizard 85
report documents 62, 147
operating systems. *See* UNIX systems; Windows systems
Operator role 9, 42, 194
Operator user 9
operators 15
options (licensing) 34, 121, 156, 158, 162, 171, 181
Options dialog 11
Options link 11
output
converting 94, 107, 109, 112
creating queries and 83, 85, 156
generating reports and 71, 91, 93, 105
printing and 117, 119
running scheduled jobs and 96
setting parameter values and 102
output files 103, 105, 127
output formats
generating documents and 103, 104, 106, 112
selecting 106
sending attachments and 86, 116
output options 92, 103, 105
Output page (Run) 92
Output page (Schedule) 103, 105, 112
Output property 94
Override user preferences setting 116, 130
overriding printer settings 33, 117
overwriting reports 73, 75, 104
owners 75, 181

P

Page Level Security Option 181
Page range setting 108, 118
Page size property 118, 176
Page style setting 108, 118
page-level security
  accessing external security sources and 192
  assigning privileges and 59
  creating RSSE applications for 195
  enabling 185
  viewing reports and 181, 185, 189
Paper tray property 118
parameter values files 63, 97, 102, 120, 161
parameters
  accessing data cubes and 159, 160, 161
  generating reports and 91
  running jobs and 101–103
  running spreadsheet reports and 163–165
  saving 102
  setting values for 102
Parameters page (File Types) 161
Parameters page (Run) 102
Parameters page (Schedule) 102
Parameters property 94
parent roles 40, 49, 169
Parent Roles page (New Security Role) 45
Parent Roles page (Security Roles Properties) 49
Pass Through Security page 186
pass-through security 40, 185–188
passwords
  accessing information objects and 187
  authenticating users and 188
  changing 20
  cloning users and 37
  creating 22
  defining anonymous users and 193
  protecting volume data and 180
  verifying 191
paths. *See* directory paths
PDF output formats 86, 108, 112
pending jobs 100, 131
Pending property 127, 131
performance 86, 165
permissions. *See* privileges
Permissions property 74
Personal Channel page 135
personal channels 24, 29, 128, 135, 138
Personal Settings icon 11
Personal Settings page 11, 116
pipe-separated values files. *See* PSV output formats
pivot tables 107
Place job completion notice in Personal Channel setting 24, 128
port number conflicts 165
PostScript files 118
PostScript output formats 108
PowerPoint files 108, 113
print options 118, 176, 194
Print page (Schedule) 117, 119
Print property 94, 119
Print the output document setting 117, 118
Print to file property 118
Printer property 118
printer settings 26, 33, 117, 175
printers
  scheduling jobs and 119
  selecting 118
  setting properties for 118, 176, 177, 194
  specifying default 26, 33, 177
  viewing information about 118, 177
printing
  images 108, 119
  report documents 93, 117, 119, 176
  to files 117, 118
Printing page (New User) 26
Printing page (Users Properties) 33
Printing page (Volume Properties) 177
Printing property 29
priority settings (jobs) 21, 23, 31, 98
private files 58, 60, 61, 72
private folders 58, 60, 61, 72
Privilege Template page (New User) 25
Privilege Template page (Users Properties) 33
Privilege Template property 29
privilege templates 25, 33, 170
privileges
  accessing information objects and 59, 83, 84, 184
  archiving reports and 170

assigning to Encyclopedia 54, 180, 182
assigning to security roles 25, 33, 60, 71
assigning to users 25, 33, 60, 71
cancelling 114
changing 33, 60, 72, 142
copying files and 181
creating security roles and 40, 45
defining functionality levels and 42
deleting 33, 40, 61, 142, 143
displaying volume 175
distributing reports and 23, 116
enabling page-level security and 185
external security sources and 191, 192, 193
generating output and 93, 113
inheriting 40
overriding 59
removing Encyclopedia items and 78
running parameter values files and 63
selecting multiple items for 60
sending notifications and 115, 117
setting channel 30, 45, 139, 141, 143
setting file 58, 59, 72
setting folder 58, 59, 72, 181, 194
specifying home folders and 22
troubleshooting 121
updating 22
uploading files and 73, 76
Privileges page (Channels Properties) 142
Privileges page (Channels) 143
Privileges page (Files and Folders Properties) 56, 59, 61, 76
Privileges page (New Channel) 141
Privileges page (New Folder) 71
Privileges page (Run) 92
Privileges page (Schedule) 113
Privileges property 94
properties
autoarchive 63, 65, 170
cache connection 86
channel 140, 142
copying 74
Encyclopedia volumes 168, 172
external user 190, 191, 192, 194, 195
externalizing 188
file types 156
folders 55, 175
iServer service startup 3, 4
jobs 94, 127, 131
notifications 128, 129
output files 103, 105
printing 26, 118, 176, 177, 194
query definition files 84
report files 55, 74
security roles 43, 44, 46, 47, 48
updating 191
user accounts 21
users 28–36, 37, 189
Properties page (Channels) 142, 146
Properties page (File Types) 156
Properties page (Files and Folders) 55, 74
Properties page (Job Schedules) 135
Properties page (Jobs Details) 133
Properties page (Notification Groups) 152
Properties page (Security Roles) 48
Properties page (Users) 29, 31
Properties page (Volume) 168
proxy security 186
PSV output formats 107
Public folder 6
publishing
information objects 83
report files 71
spreadsheet reports 162
Purge failure notices after property 173
Purge success notices after property 173
purging notifications 24, 128, 130, 173

Q

queries
changing 84
creating 83–84
displaying data and 83
generating information objects and 83, 157, 158
generating output and 156
retrieving data with 157
running 83, 85, 94, 97
saving 84, 85
scheduling 85
query definition files 83
See also data object value files
query definitions 85
Query Option 156

query output files. *See* data object instance files
query template files 157–158
Query Wizard 84, 85

R

read privilege 58, 139, 181
readme files 5, 6, 189
recurring jobs 122
Recurring property 95
Recursively include subfolders setting 72
relational databases. *See* databases
renaming
  channels 144
  files 57, 75
  jobs 97
  notification groups 152
  security roles 41, 48
Replace existing privilege setting 72
Replace the latest version setting 73, 75, 80
report bursting 121
report design elements 7
report design files 6, 58, 107, 185
report design templates 157
report design tools 71, 162
report designs 6, 7, 21, 90, 91, 157
report document files
  accessing data cubes and 159
  archiving 67
  assigning privileges to 58, 113, 185
  attaching to e-mail 23, 86, 106, 116
  converting 94, 107, 109, 112
  distributing over channels 24, 115, 138
  embedding executable files in 105
  generating 71, 90, 91, 105
  running 97
  setting dependencies for 76, 120
  viewing information about 133
report executables. *See* executable files
report files
  See also specific type
  accessing 54, 58, 181
  archiving 63–71, 170–174
  assigning privileges to 58, 59, 72
  bundling 104, 105
  changing privileges for 60
  converting 94, 107, 109, 112
  copying 79, 81
  deleting 63, 68, 78, 79
  displaying archiving policies for 67, 77, 104
  displaying information about 54, 55, 56
  downloading 59, 82
  marking as private 60, 61, 72
  moving 79, 81
  naming 103, 122
  preserving 68
  removing privileges on 61
  removing temporary 93
  renaming 57, 75
  restricting access to 72
  selecting 60
  setting archiving policies for 65, 69, 70
  setting autoversioning options for 73, 75
  setting date/time stamps for 122, 123, 124, 125
  setting dependencies for. *See* file dependencies
  setting properties for 55, 56, 74
  uploading 57, 71, 73
  viewing 5, 58
report object executable files 62, 105, 157
report object instance files 62, 106, 113
  See also report document files
report object parameter files 163
report object values files 102
  See also parameter values files
report parameters. *See* parameters
Report Server Security Extension 188, 189
  See also RSSE applications
report specifications 90
reporting environments 2
reports
  See also cube reports; spreadsheet reports
  accessing 54, 58, 181
  displaying 147, 185
  distributing 24, 115, 138
  generating 71, 90, 91, 105
  opening 62, 147
  overwriting 73, 75, 104
  printing 93, 117, 119, 176
  restricting access to 59, 60, 114, 180, 181, 185

running 90, 96, 97
saving 91, 93, 98, 104
scheduling 93–98, 100, 103, 113, 115
requests. *See* jobs
Reset button 65
Resolution property 118, 176
Resource Group page 99
resource groups 98
resources 164, 188
Resources folder 7
restricting access to reports 59, 60, 114, 180, 181, 185
retry options 100, 101
retrying failed jobs 98, 100, 101
rich-text formats. *See* RTF formats
Right now property 95
.roi files. *See* report object instance files
ROI formats 113
roles
accessing channels and 45, 139, 141, 142, 143
accessing reports and 9, 58, 60, 61, 72
adding to privilege templates 33
assigning privileges to 25, 33, 45, 60, 71
assigning to users 24, 40, 47, 50, 169
associating security IDs with 195
changing 32, 41, 51
cloning 47
creating 40, 43, 44, 47, 169
defining functionality levels and 42
defining hierarchies of 40, 49
deleting 32, 48, 51
displaying 43
enabling Open Security for 190
enabling page-level security for 181, 185
enabling pass-through security for 186
externalizing 193
externalizing information for 189, 192
generating information objects and 186
generating output and 92, 113
managing 43
naming 44
nesting 40, 186, 193
removing privileges for 40
removing users 47, 51
renaming 41, 48
searching for 195
selecting 48, 61
sending notifications to 115
setting properties for 44, 46, 48
Roles page (New User) 24
Roles page (Users Properties) 32
Roles property 29
.rop files. *See* report object parameter files
.rov files. *See* report object values files
rows
displaying in tabular lists 13
setting maximum number of 107
updating cache tables and 88
.rox files. *See* report object executable files
.rptlibrary files. *See* BIRT report libraries
RSSE applications
See also Open Security applications
accessing external security sources and 188
accessing sample 188
assigning privileges and 22
authenticating users and 191, 192, 194
creating 188, 195
defining anonymous users and 193
defining security roles and 193
defining user properties and 191
externalizing user information and 192, 193, 194, 195
logging in to Encyclopedia and 194
printing reports and 194
searching from 195
setting home folder privileges and 194
RSSE interfaces 188
RSSE service 188
RTF formats 86, 113
Run dialog 7, 91
running
event-based jobs 94, 95, 96, 119, 132
information objects 59, 157
iService services 4
parameter values files 63
queries 83, 85, 94, 97
report designs 6, 7, 21, 90, 91, 157
report executables 62, 157
reports 90, 96, 97
scheduled jobs 95, 96, 98, 119
spreadsheet reports 162, 165
unscheduled jobs 91, 94, 96, 119

Running property 127, 131
run-time errors 163

S

sample applications 188, 189, 190
sample designs 5, 6, 109
sample templates 157
Save the output document setting 91
saving
  cube reports 158
  DHTML files 174
  jobs 102
  queries 84, 85
  report parameters 102
  reports 91, 93, 98, 104
  spreadsheet reports 162
  temporary files 93
Scale property 118, 176
Schedule for purging notices setting 130
Schedule page 95, 97
Schedule property 94
scheduled jobs
  See also jobs
  cancelling 135
  changing settings for 134
  failing 100, 101
  naming 97
  running 94, 96, 98, 119
  saving 102
  setting output options for 103, 105
  specifying as event 96
  specifying resource groups for 98, 100
  viewing status of 127
Scheduled property 127, 131
Schedules page (Job Schedules) 135
scheduling
  autoarchiving cycles 174
  jobs 93–98, 100, 103, 113, 115
  queries 85
  spreadsheet reports 162
scheduling information 133
scheduling options 95, 97
scheduling properties 94
search conditions 16, 18, 195
search criteria. *See* search conditions
Search dialog 16
search expressions 15, 195
Search link 16
search operators 15
search results 16
searching
  Encyclopedia volumes 16–18
  for specific users 15
  from RSSE applications 195
secure read privilege 59, 181
security
  accessing Encyclopedia volumes and 54, 180
  accessing external sources and 188, 192
  assigning privileges and 59, 180, 182
  changing access control lists and 189
  creating passwords and 22
  enabling page-level 181, 185
  enabling pass-through 185–188
  nesting roles and 40
security applications 188
security IDs 195
security information 185, 190
security options 185
security roles
  accessing channels and 45, 139, 141, 142, 143
  accessing reports and 9, 58, 60, 61, 72
  adding to privilege templates 33
  assigning privileges to 25, 33, 45, 60, 71
  assigning to users 24, 40, 47, 50, 169
  associating security IDs with 195
  changing 32, 41, 51
  cloning 47
  creating 40, 43, 44, 47, 169
  defining functionality levels and 42
  defining hierarchies of 40, 49
  deleting 32, 48, 51
  displaying 43
  enabling Open Security for 190
  enabling page-level security for 181, 185
  enabling pass-through security for 186
  externalizing 193
  externalizing information for 189, 192
  generating information objects and 186
  generating output and 92, 113
  managing 43
  naming 44

nesting 40, 186, 193
removing privileges for 40
removing users 47, 51
renaming 41, 48
searching for 195
selecting 48, 61
sending notifications to 115
setting properties for 44, 46, 48
Security Roles icon 10
Security Roles page 10, 43
security rules 185
security sources. *See* external security sources
selection criteria. *See* parameters
Send e-mail notification setting 23
sending e-mail notifications 23, 116, 169
services. *See* iServer services
Set file access type setting 61
Share setting 61
shared files 58, 60, 61, 72
shared folders 58, 60, 61, 72
shared reports 185
Short Date formats 123
Short Time formats 123
side menu (Management Console) 9, 11
Size property 75
.sma files. *See* data source map files
Small (16x16) icon URL property 140
Small icon URL property 146
SmartSheet security 59, 195
SmartSheet Security Option 181
SOAP-based API 171
.soi files. *See* spreadsheet object instance files
.sox files. *See* spreadsheet object executable files
special characters
date-time expressions and 123
filtering data and 14
search expressions and 15
spreadsheet designer. *See* BIRT Spreadsheet Designer
spreadsheet designs 7, 162, 163
spreadsheet object executable files 108, 162, 163
spreadsheet object instance files 108, 162, 163
spreadsheet reports
accessing sample 7
connecting to 163, 165
converting 108
exporting data and 112
generating output for 107, 112
publishing 162
restricting access to 181
running 162, 165
saving 162
setting parameters for 163–165
setting privileges for 59
SQL databases 159, 160, 161
SQL statements. *See* queries
starting
iServer services 2, 3, 4
Management Console 4
Status page (Jobs Details) 134
Stop Archive Thread button 173
strings
creating date expressions and 125
creating user names and passwords and 22
naming report items and 78
subfolders 66, 72
subreports 121
subscriber lists 139, 144
Subscribers page (Channels) 145
subscribing to channels 29, 138, 169
Summary page (Jobs Details) 133
syntax errors 125
system events 95
system printers 175
system-defined security roles 41

T

Table name setting 107
tables. *See* cache tables
tab-separated values files. *See* TSV output formats
template files 156, 157, 158
templates
assigning privileges and 25, 170
creating spreadsheet reports and 162
customizing 157, 158
querying information objects and 157–158
temporary files 85, 93
text strings. *See* strings
Text wrapping setting 108, 119

third-party security systems 189
time 68, 107, 123, 127
time expressions 122, 123, 125
time format symbols 125
time formats 122, 125
time stamps 122, 124, 125
time zones 5, 13, 97
time-out errors 96
TMPDIR variable 93
transient files 85, 93
troubleshooting 119–121, 163
trusted execute privilege 59, 181
TSV output formats 107

U

unauthorized users 180
unescaped literal characters 125
UNIX systems
  accessing Analytics data sources and 160
  assigning privileges and 58
  configuring iServer startup properties for 4
  generating temporary files for 93
  printing reports and 119
  running spreadsheet reports and 163
  starting console applications on 4
unscheduled jobs 91, 94, 96, 121
unscheduled requests. *See* unscheduled jobs
unsubscribing from personal channels 138
updating
  cache tables 88
  channel icons 141
  channels 141
  dependency information 63
  external user properties 191
  locale maps 123
  notification groups 32
  privileges 22
  user properties 31
upgrades 93
uploading
  files 57, 71, 73
  information objects 73
  query templates 158
  spreadsheet reports 162
URLs
  associating with channel icons 140, 141, 146
  limitations for 78
  starting Management Console and 4
Use default/inherited policy setting 65, 67
user accounts
  changing properties for 31
  cloning 36
  creating 20, 21, 22
  deleting 37, 38
  external security sources and 192
  setting properties for 29
  viewing information about 11
user-defined formats 125
user groups 40
user names
  accessing information objects and 187
  cloning users and 37
  creating 22
  filtering 14
  searching on 15
  verifying 191
user properties
  changing 28–36
  copying 36
  externalizing 189, 190, 191, 192, 194, 195
User property 75
User role 9
user types 9
userid parameter 161
users
  accessing Encyclopedia items and 6, 60, 61
  adding 22, 36
  assigning passwords 22
  assigning privileges 25, 33, 60, 71
  assigning security roles 24, 40, 47, 50, 169
  assigning to notification groups 24, 32, 149, 150
  authenticating 189, 191, 192, 194
  changing channel subscriptions for 35
  changing home folders for 31
  changing licensed options for 34
  changing passwords for 20
  changing privilege templates for 33
  changing security roles for 32, 41, 51
  creating accounts for. *See* user accounts
  creating privilege templates for 25

deleting 181
externalizing information for 189, 190, 191, 192, 193, 194, 195
generating access control lists for 185
managing 11, 14
mapping security IDs to 195
removing channel subscriptions for 36
removing from notification groups 32, 150, 151
returning login information for 15
searching for 15, 195
selecting 31, 61
sending notifications to 24, 115, 128, 139, 169
setting channel subscriptions for 29, 138, 169
setting default printers for 26, 33, 118
setting home folders for 22
setting job priorities for 21, 23, 31, 98
setting licensed options for 27
setting printer options for 33, 117, 176
setting properties for. *See* user properties
viewing available jobs for 127
viewing notification groups for 147
viewing purge settings for 173
viewing subscribed channels for 145
Users icon 10
Users page (Management Console) 10, 20, 28, 31
Users page (Notification Groups) 149, 151
Users page (Security Roles) 46, 51

V

VBA templates 162
Version control property 104
Version name property 75, 104
version names 75, 104, 122
See also autoversioning options
Version number property 75
View Policy button 65, 67, 77
View Policy property 104
View processes 185
View service 93, 119
viewers 147
viewing
archiving policies 67, 77, 104
channel icons 145
channel subscribers 139, 144
channels 30
completion notices 130, 138, 139
data 83, 157, 160
file or folder information 54, 55, 56
file type properties 67, 156
file types 65
files 5, 58
job information 121, 127, 131–134
licensed options 27, 34
notification groups 147
printer information 118, 177
query output 85
reports 147, 185
sample designs 6
scheduling information 133
security roles 43
user account information 11
viewing restrictions 59, 60, 114
visible privilege 58, 59, 181
Volume Actuate Query template file parameter 158
volume administrators. *See* administrators
Volume icon 11
Volume page 11, 168
volumes. *See* Encyclopedia volumes

W

Wait for Event property 95
wait periods 96, 98, 163, 164
Waiting for Event page 132
Waiting for Event property 127, 131
web browsers
accessing console applications and 2
accessing Encyclopedia and 194
caching report documents and 174
setting volume properties and 169
viewing reports and 120, 147
web service applications 96
web services 96, 119
wildcard characters 14, 195
Windows systems
accessing Analytics data sources and 159, 160
assigning privileges and 58

Windows systems *(continued)*
configuring iServer startup properties for 3
generating temporary files for 93
printing reports and 119
running spreadsheet reports and 163
starting console applications on 4
Word documents 108
word wrapping 108, 119
write privilege 58, 139, 181

X

XML data files 160
XML processors 164
XSL processors 164