



ACTUATE.
The BIRT Company™



BIRT iHub

Managing Volumes and Users

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 - 2014 by Actuate Corporation. All rights reserved. Printed in the United States of America.

Contains information proprietary to:
Actuate Corporation, 951 Mariners Island Boulevard, San Mateo, CA 94404

www.actuate.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, BIRT 360, BIRT Analytics, The BIRT Company, BIRT Content Services, BIRT Data Analyzer, BIRT for Statements, BIRT iHub, BIRT Metrics Management, BIRT Performance Analytics, Collaborative Reporting Architecture, e.Analysis, e.Report, e.Reporting, e.Spreadsheet, Encyclopedia, Interactive Viewing, OnPerformance, The people behind BIRT, Performancesoft, Performancesoft Track, Performancesoft Views, Report Encyclopedia, Reportlet, 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:

Mark Adler and Jean-loup Gailly (www.zlib.net): zlib. Adobe Systems Incorporated: Flash Player, Source Sans Pro font. Amazon Web Services, Incorporated: Amazon Web Services SDK. Apache Software Foundation (www.apache.org): Ant, Axis, Axis2, Batik, Batik SVG library, Commons Command Line Interface (CLI), Commons Codec, Commons Lang, Commons Math, Crimson, Derby, Hive driver for Hadoop, Kafka, log4j, Pluto, POI ooxml and ooxml-schema, Portlet, Shindig, Struts, Thrift, Tomcat, Velocity, Xalan, Xerces, Xerces2 Java Parser, Xerces-C++ XML Parser, and XML Beans. Daniel Bruce (www.entypo.com): Entypo Pictogram Suite. Castor (www.castor.org), ExoLab Project (www.exolab.org), and Intalio, Inc. (www.intalio.org): Castor. Alessandro Colantonio: CONCISE. Day Management AG: Content Repository for Java. Eclipse Foundation, Inc. (www.eclipse.org): Babel, Data Tools Platform (DTP) ODA, Eclipse SDK, Graphics Editor Framework (GEF), Eclipse Modeling Framework (EMF), Jetty, and Eclipse Web Tools Platform (WTP). Dave Gandy: Font Awesome. Gargoyle Software Inc.: HtmlUnit. GNU Project: GNU Regular Expression. Groovy project (groovy.codehaus.org): Groovy. Guava Libraries: Google Guava. HighSlide: HighCharts. headjs.com: head.js. Hector Project: Cassandra Thrift, Hector, Jason Hsueth and Kenton Varda (code.google.com): Protocole Buffer. H2 Database: H2 database. Groovy project (groovy.codehaus.org): Groovy. IDAutomation.com, Inc.: IDAutomation. IDR solutions Ltd.: JBIG2. InfoSoft Global (P) Ltd.: FusionCharts, FusionMaps, FusionWidgets, PowerCharts. Matt Inger (sourceforge.net): Ant-Contrib. Matt Ingenthron, Eric D. Lambert, and Dustin Sallings (code.google.com): Spymemcached. International Components for Unicode (ICU): ICU library. JCraft, Inc.: JSch. jQuery: jQuery. Yuri Kanivets (code.google.com): Android Wheel gadget. LEAD Technologies, Inc.: LEADTOOLS. The Legion of the Bouncy Castle: Bouncy Castle Crypto APIs. Bruno Lowagie and Paulo Soares: iText. MetaStuff: dom4j. Microsoft Corporation (Microsoft Developer Network): CompoundDocument Library. Mozilla: Mozilla XML Parser. MySQL Americas, Inc.: MySQL Connector. Netscape Communications Corporation, Inc.: Rhino. nullsoft project: Nullsoft Scriptable Install System. OOPS Consultancy: XMLTask. OpenSSL Project: OpenSSL. Oracle Corporation: Berkeley DB, Java Advanced Imaging, JAXB, JDK, Jstl, Oracle JDBC driver. PostgreSQL Global Development Group: pgAdmin, PostgreSQL, PostgreSQL JDBC driver. Progress Software Corporation: DataDirect Connect XE for JDBC Salesforce, DataDirect JDBC, DataDirect ODBC. Quality Open Software: Simple Logging Facade for Java (SLF4J), SLF4J API and NOP. Rogue Wave Software, Inc.: Rogue Wave Library SourcePro Core, tools.h++. Sam Stephenson (prototype.conio.net): prototype.js. Sencha Inc.: Ext JS, Sencha Touch. Shibboleth Consortium: OpenSAML, Shibboleth Identity Provider. Matteo Spinelli: icscroll. StAX Project (stax.codehaus.org): Streaming API for XML (StAX). SWFObject Project (code.google.com): SWFObject. ThimbleWare, Inc.: JMemcached. Twitter: Twitter Bootstrap. VMware: Hyperic SIGAR. Woodstox Project (woodstox.codehaus.org): Woodstox Fast XML processor (wstx-asl). World Wide Web Consortium (W3C)(MIT, ERCIM, Keio): Flute, JTI, Simple API for CSS. XFree86 Project, Inc.: (www.xfree86.org): xvfb. ZXing Project (code.google.com): ZXing.

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

Document No. 131215-2-530304 February 12, 2014

Contents

About <i>Managing Volumes and Users</i>	iii
Chapter 1	
Getting started	1
About Encyclopedia volume management	2
Logging in to Visualization Platform	2
Understanding volumes and users	5
Chapter 2	
Setting up application users and groups	7
Understanding iHub Administration	8
Tutorial 1: Creating users and user groups.....	8
About user types	11
Accessing iHub Administration	12
About users	13
Creating a user	13
Editing a user	18
Viewing the list of users	20
Filtering the list of users using a search string	21
Filtering the list of users by user group	22
Deleting users	22
About User Groups	24
Creating a user group	25
Editing a user group	27
Viewing the list of user groups	29
Deleting user groups	30
Accessing Logout and My Profile	32
Chapter 3	
Managing volume-level operations	35
Working at the volume level	36
Setting volume privileges	37
Setting volume archiving and purging policies	38
Setting volume level printer options	41
Understanding service requirements	43
Scheduling an archiving cycle	43
About user and user group limits	44
Chapter 4	
Exploring administrative capabilities	47
Using the /Applications folder	48

About locale maps	48
Using Advanced Jobs	49
Using the available job monitoring options	49
Filtering jobs	56
Editing a scheduled job	57
Deleting a scheduled job	58
Cloning a job	58
Configuring events	59
Accessing Visualization Platform using HTTPS	60
Using javaserver security to control access to protected resources	63
Index	67

About Managing Volumes and Users

Managing Volumes and Users discusses how to administer a BIRT iHub System Encyclopedia volume. The chapters in this guide are:

- *About Managing Volumes and Users.* This chapter provides an overview of this guide.
- *Chapter 1. Getting started.* This chapter discusses how to connect to a volume using Visualization Platform.
- *Chapter 2. Setting up volume users and groups.* This chapter discusses how to create and work with users and user groups.
- *Chapter 3. Managing volume-level operations.* This chapter discusses volume-level management tasks, such as archiving files, setting volume privileges, enabling DHTML document caching, and setting volume-level printer options.
- *Chapter 4. Exploring administrative capabilities.* This chapter discusses miscellaneous administrative best practices, capabilities, and tasks.

1

Getting started

This chapter discusses the topic, About volume management.

About volume management

BIRT iHub is a document server that generates, manages and securely delivers BIRT documents stored in a volume. A volume is a disk-based repository containing designs, documents, information objects, shared libraries, and user information. You access a volume by logging in to Visualization Platform.

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

- Visualization Platform
Use this console to perform volume management tasks such as:
 - Running designs
 - Scheduling designs based on time and events
 - Viewing and sharing documents
 - Managing user and user group access to designs and documents using privileges
 - Distributing documents
 - Accessing scheduled and completed jobs
- Visualization Platform—iHub Administration
Use this console to perform user management tasks such as:
 - Create users
 - Create user groups
 - Manage user membership to user groups

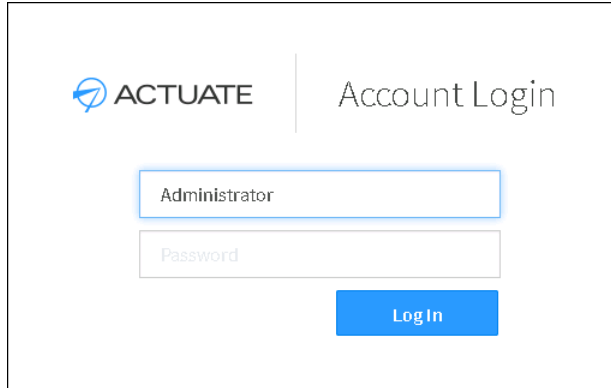
An out-of-the-box BIRT iHub installation comes with a default volume, named Default Volume. Default Volume contains samples of volume content. If you do not specify a volume name when logging in to Visualization Suite, you access Default Volume by default. To access a different volume, you specify the volume name when logging in.

Logging in to Visualization Platform

The following section describes logging in to Visualization Platform as the default user, Administrator, as a user having no home folder, and how to log in to access a volume other than Default Volume.

How to log in to Visualization Platform

- 1 Open a web browser. In the address bar, type the following URL:
`http://localhost:8700/iportal`
- 2 The first time you log in, log in as the default volume administrator user, Administrator, accessing the Default Volume. On Account Login, in Username, type Administrator. Leave Password blank, as shown in Figure 1-1.



ACTUATE | Account Login

Administrator

Password

Log In

Figure 1-1 Logging in to Visualization Platform as Administrator

The list of files and folders in the Administrator home folder appears. The list contains Examples, an HTML document giving an overview of the sample design and document files that the default volume contains, as shown in Figure 1-2.

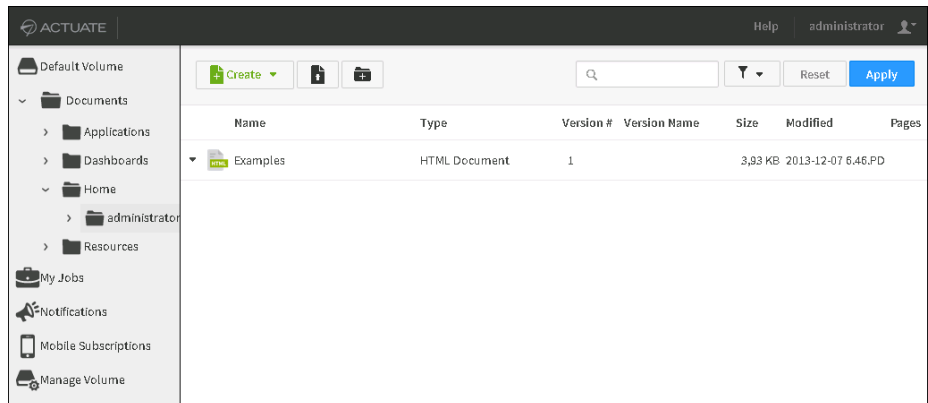


Figure 1-2 Viewing the Administrator home folder

Logging in as a user with no home folder

By default, Administrator has a home folder in Visualization Platform, /Home/administrator, as shown in Figure 1-2. When a user having a home folder logs in to Visualization Platform, the list of files and folders in that user's home folder appears. If a user does not have a home folder, the list of files and folders in the volume root folder, named Documents, appears, as shown in Figure 1-3. The volume administrator can create a home folder for a user when creating the user.

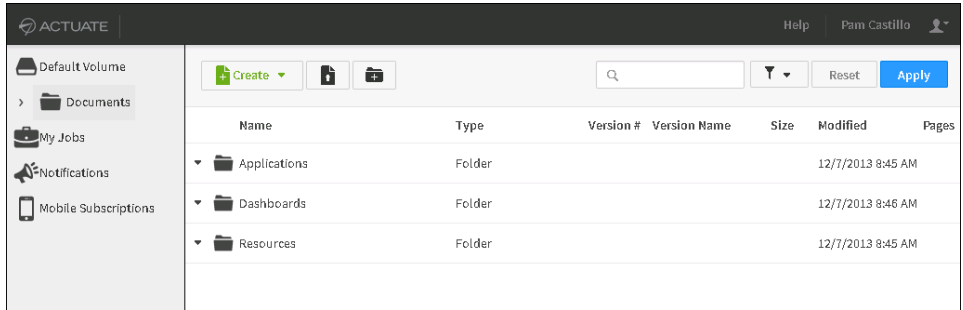


Figure 1-3 Logging in as a user that does not have a home folder

Accessing a volume other than Default Volume

To access a different volume, type the volume name, a backslash, and the user name in Username when logging in to Visualization Platform. For example, in Figure 1-4, Administrator is logging in to Visualization Platform accessing sales_volume.

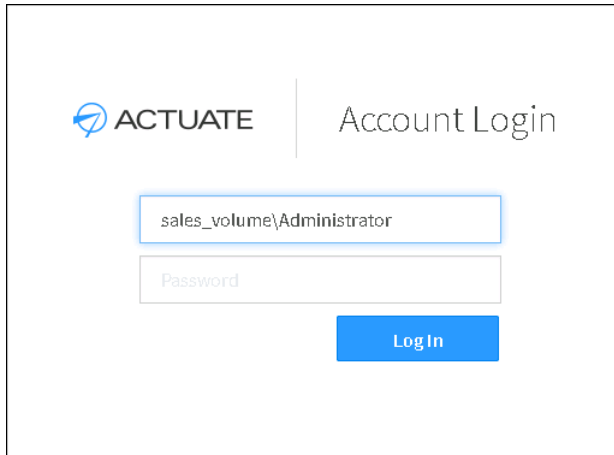


Figure 1-4 Logging in to Visualization Platform accessing sales_volume

Understanding volumes and users

In System Console, the system administrator creates a cluster typically consisting of two or more machines, or nodes. Then, the system administrator can create one or more volumes in the cluster.

If the system administrator has enabled e-mail notification and specifies a volume administrator e-mail address when creating a volume, BIRT iHub creates a password with which to access the volume when it is created. Then, BIRT iHub e-mails the password to the volume administrator. The volume administrator accesses the volume by logging in to Visualization Platform using the following credentials:

- Username: <volume name>\administrator
- Password: <volume password BIRT iHub creates and e-mails to the volume administrator>

Only the BIRT iHub default user, Administrator, can access a newly created volume. When logging in to Visualization Platform, the user name is not case-sensitive.

If the system administrator does not specify a volume administrator e-mail address when creating a volume, BIRT iHub does not create a password. The volume administrator can access the volume without using a password, logging in to Visualization Platform using the following credentials:

- Username: <volume name>\administrator
- Password: (blank)

In Visualization Platform, the administrator can choose My Profile to create a password for the volume.

Users are specific to a volume. A newly created volume has no users except the default user, Administrator. The Administrator user logs in to Visualization Platform, specifying the volume. Then, the Administrator user can create one or more users of the volume. One user can access only one volume, but the administrator can create a user having the same name and password on any number of volumes.

Setting up volume users and groups

This chapter contains the following topics:

- Understanding iHub Administration
- Tutorial 1: Creating users and user groups
- About user types
- Accessing iHub Administration
- Creating users
- Creating user groups
- Accessing Logout and My Profile

Understanding iHub Administration

A volume administrator uses iHub Administration to create users and user groups, and assign users to user groups. Users perform tasks such as running designs to create documents, viewing, and working with documents. A user group supports assigning privileges on items such as designs, documents, and folders to a group of users.

Tutorial 1: Creating users and user groups

An administrator has access to the entire contents of the volume. You can restrict access to the contents of the volume for other users. BIRT iHub Visualization Platform enables you to create users and assign privileges on files and folders to control access. Each user is assigned a user name and password that they use to log in to the volume.

Very often in an organization, a group of users has the same requirements for access to the reports in a volume. For example, corporate executives may all need access to the same sales reports. Because it is easier to assign privileges to a group of users than it is to assign privileges to individual users, you can create a user group that includes all executives and grant this user group access to sales reports.

You will create two users, User01 and User02. You will then create two user groups, UserGroup01 and UserGroup02. UserGroup01 will consist of one user, User01. Likewise, UserGroup02 will consist of User02.

Task 1: Creating users

Create the users User01 and User02.

- 1 Click the icon on the right end of the toolbar to display the User menu, as shown in Figure 2-1.



Figure 2-1 Displaying the User menu

- 2 Choose BIRT iHub Administration. Administration appears in a new tab. Only one user appears in the list, Administrator.
- 3 In Users, choose Add User.
- 4 In Create New User, in Name, type User01.
- 5 In Home Folder, type /Home/User01.

- 6 Provide a password and an email address. The password must be at least eight characters long. It must contain at least one lower case letter, one upper case letter, and one digit. Figure 2-2 shows the properties for User01.

The screenshot shows a 'Create New User' form with the following fields and values:

- *Name: User01
- Description: (empty)
- *Password: (masked with 8 dots)
- *Confirm Password: (masked with 8 dots)
- *Email: User01@acme.com
- Home Folder: /Home/User01 (Example: /Home/administrator)
- Default Dashboard: (empty) (Example: /dashboard/mydashboard.dashboard)
- Language: English (United States) (dropdown)
- Time zone: America/Los_Angeles (dropdown)

Buttons: Cancel, Save

Figure 2-2 Creating a user

- 7 Choose Save. In Confirmation, choose OK to confirm.
- 8 Create a second user named User02. User01 and User02 appear in the list of users, along with Administrator, as shown in Figure 2-3.

Name	Email
<input type="checkbox"/> ▼ Administrator	
<input type="checkbox"/> ▼ User01	User01@acme.com
<input type="checkbox"/> ▼ User02	User02@acme.com

Figure 2-3 List of users

Task 2: Creating user groups

Create the user groups UserGroup01 and UserGroup02.

- 1 In the upper left corner of Administration, click on User Groups, as shown in Figure 2-4.

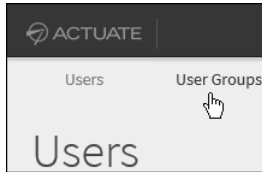


Figure 2-4 Choosing User Groups

- 2 In User Groups, choose Add User Group.
- 3 In Create New User Group, in Name, type UserGroup01, as shown in Figure 2-5.

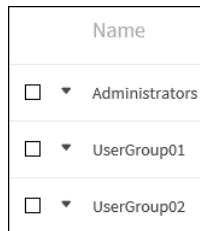
Figure 2-5 Creating a user group

- 4 In the left pane, choose Assign Users.
- 5 In Available Users, select User01. Choose the right arrow. User01 appears in Assigned Users, as shown in Figure 2-6.

Figure 2-6 Assigning a user to a group

- 6 Choose Save. In Confirmation, choose OK to confirm.

- 7 Create a second user group named UserGroup02. UserGroup01 and UserGroup02 appear in the list of user groups, along with the Administrators user group, as shown in Figure 2-7.



Name		
<input type="checkbox"/>	▼	Administrators
<input type="checkbox"/>	▼	UserGroup01
<input type="checkbox"/>	▼	UserGroup02

Figure 2-7 List of user groups

- 8 Close the Administration tab.

About user types

Visualization Platform supports the following types of users and user groups:

- **Administrator**
The default user. The Administrator user has privileges to perform all tasks in BIRT iHub System.
- **Administrators**
A user group. A user belonging to the Administrators user group has privileges to perform all tasks in the BIRT iHub System. Only the default user, Administrator, or a user belonging to the Administrators user group can:
 - Access iHub Administration and create users and user groups
 - Access My Jobs—Advanced Jobs
 - Assign privileges on any item in a volume
 - Configure Datamart Security when scheduling a job
 - Select a resource group when scheduling a job
 - Use Visualization Platform—Manage Volume to set properties pertaining to an entire volume

This book refers to a user having Administrators user group privileges as the administrator.

- **All**
A user group. All users belong to the All user group by default. The administrator assigns a privilege to the All user group to assign the privilege to all users.

- User

When differentiating between a user that has Administrators user group privileges in Visualization Platform and a user that does not, a user is any user that does not have Administrators user group privileges, and an administrator is a user that does have Administrators user group privileges. Otherwise, user is a term that can refer to any user. In Visualization Platform, a user with appropriate privileges can schedule jobs, view documents, and administer files and folders.

Accessing iHub Administration

Only a volume administrator can access iHub Administration. The volume administrator accesses iHub Administration from Visualization Platform.

How to access iHub Administration

- 1 Open a web browser. In the address bar, type the following URL:
`http://localhost:8700/iportal`
- 2 The first time you log in, log in as the default volume administrator user, Administrator. On Account Login, in Username, type Administrator. Leave Password blank, as shown in Figure 2-8.

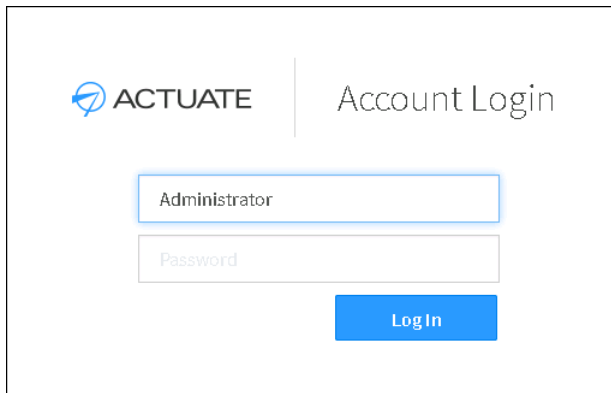


Figure 2-8 Logging in to Visualization Platform as Administrator

- 3 In Visualization Platform, left-click Administrator and choose iHub Administration, as shown in Figure 2-9.

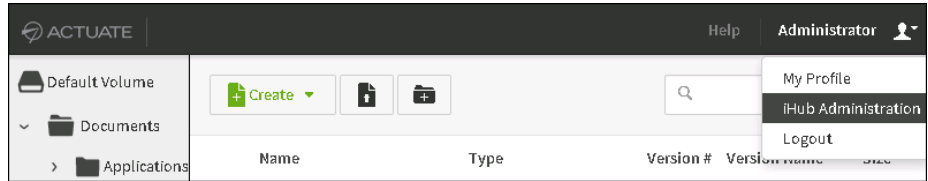


Figure 2-9 Choosing iHub Administration
Users appears, as shown in Figure 2-10.

Creating users

In iHub Administration, to perform the following tasks, choose Users, as shown in Figure 2-10:

- Create a user
- Edit an existing user
- View or filter the list of users
- Delete users

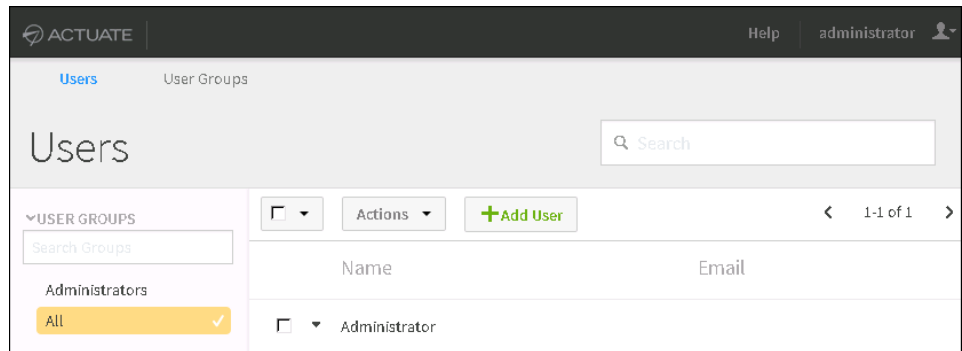


Figure 2-10 Viewing Users

The following sections describe how to perform these tasks.

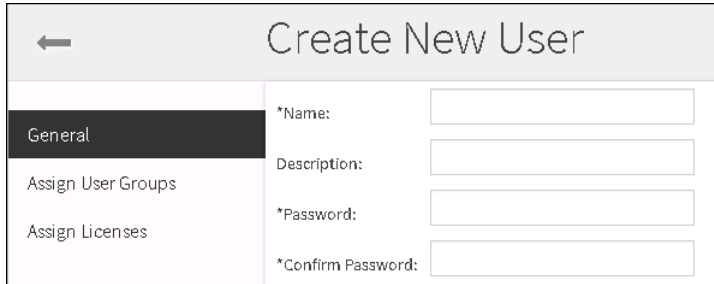
Creating a user

On Users, the administrator chooses Add User to create a new user, as shown in Figure 2-10. On Create New User—General, a side menu lists the following categories for which the administrator performs tasks to create a user, as shown in Figure 2-11:

- General

Configure general properties, such as user name, password, e-mail address.

- Assign User Groups
Assign one or more user groups to the user.
- Assign Licenses
Assign one or more licensed options to the user.



The screenshot shows a web interface for creating a new user. At the top, there is a header with a back arrow and the title "Create New User". Below the header is a side menu with three options: "General" (which is highlighted in black), "Assign User Groups", and "Assign Licenses". To the right of the side menu is a form with four input fields, each with a label and an asterisk indicating it is required: "*Name:", "Description:", "*Password:", and "*Confirm Password:". Each label is followed by a text input box.

Figure 2-11 Viewing the side menu on Create New User

How to create a user

This section demonstrates creating a user named Pam Castillo.

- 1 On Users, choose Add User.
- 2 Set the following properties on Create New User—General, as shown in Figure 2-12. A property name appearing with an asterisk (*) next to the name is a required property.
 - Name
Type the user name.
 - Description
Type a description for the user, such as job title.
 - Password
Type a password for the user. The password must be at least eight characters long, and must contain at least one lower case letter, one upper case letter, and one digit. If you create a user using IDAPI, there is no restriction on what the password can be.
 - Confirm Password
Type the password again.
 - Email
Type the user's e-mail address.
 - Home Folder

Type a path for the user's home folder, such as /home/username. The user's home folder appears in Visualization Platform.

- **Default Dashboard**

Type the name of a dashboard. Alternatively, leave Default Dashboard blank.

To create a .dashboard file that is the default dashboard for all users, save any .dashboard file to the root folder of the volume, giving the file the following name:

`__default__dashboard.dashboard`

If a user has a different dashboard URL set in the user's My Profile, that dashboard is the default dashboard for that user.

- **Language**

Select a language for which to display the user interface to the user. Alternatively, accept the default value, English (United States).

- **Time Zone**

Select a time zone. Alternatively, accept the default value of America/Los Angeles.

The screenshot shows a 'Create New User' form with the following fields and values:

- *Name: Pam Castillo
- Description: Sales Manager
- *Password: [masked]
- *Confirm Password: [masked]
- *Email: pcastillo@company.com
- Home Folder: /Home/pcastillo (Example: /Home/administrator)
- Default Dashboard: /dashboard/pcastillo.dashboard (Example: /dashboard/mydashboard.dashboard)
- Language: English (United States) [dropdown]
- Time zone: America/Los_Angeles [dropdown]

Buttons: Cancel, Save

Figure 2-12 Configuring user properties on General

3 Choose Assign User Groups from the side menu.

- 4 On Create New User—Assign User Groups, assign Pam Castillo to the Sales user group by moving the Sales user group from the left-hand list of user groups to the right-hand list of user groups, as shown in Figure 2-13. Use Search available user groups to isolate a particular user group or subset of user groups from which to choose, if necessary.

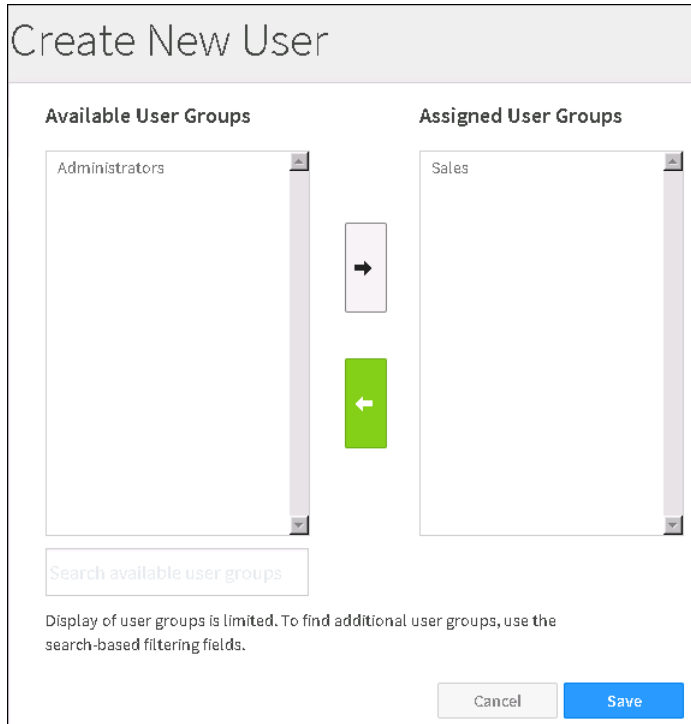


Figure 2-13 Assigning a user group to a user

- 5 Choose Assign Licenses from the side menu.
- 6 On Create New User—Assign Licenses, assign one or more license options to the new user. If using an evaluation license, all license options are unconditionally available for use, as shown in Figure 2-14.

Create New User

License Overview		
License Options	No. Purchased	No. Assigned To This Volume
Multi-Tenant Option	Unlimited	0
BIRT Option	Unlimited	0
BIRT Interactive Viewer Option	Unlimited	0
Report Studio Option	Unlimited	0
BIRT Page Level Security Option	Unlimited	0
Dashboards Option	Unlimited	0
Interactive Crosstabs Option	Unlimited	0
Accessible PDF Option	Unlimited	0

Figure 2-14 Viewing license options available to the new user

- 7 Choose Assign User Groups from the side menu. Choose Save. Confirm that you want to save the changes.

Pam Castillo appears in the list of users on Users, as shown in Figure 2-15.

Name	Email
<input type="checkbox"/> Administrator	
<input type="checkbox"/> Pam Castillo	pcastillo@company.com

Figure 2-15 Viewing the new user in the users list

Editing a user

The administrator has the same level of control over a user when editing the user as when creating it, including assigning a user group to a user, removing a user group from the user, and assigning license options to the user.

How to edit a user

- 1 On Users, left-click the arrowhead next to a user name and choose Edit, as shown in Figure 2-16.

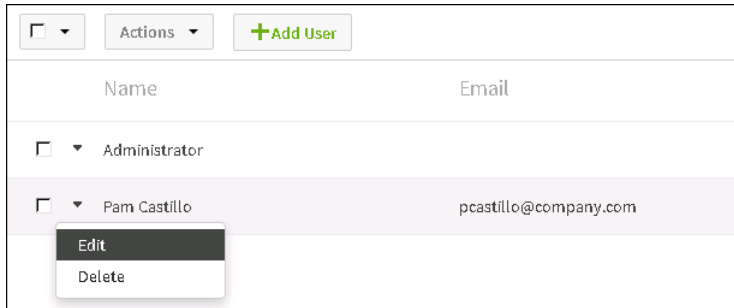


Figure 2-16 Choosing to edit a user

- 2 Make any necessary property changes on Edit <user name>—General, as shown in Figure 2-17.

Edit Pam Castillo

*Name:

Description:

*Password:

*Confirm Password:

*Email:

Home Folder: Example:/Home/administrator

Default Dashboard: Example:/dashboard/mydashboard.dashboard

Language: ▾

Time zone: ▾

Figure 2-17 Editing a user

- 3 Choose User Groups from the side menu.
- 4 On Edit <user name>—User Groups, assign one or more user groups to a user by moving one or more user groups from the left-hand user group list to the right-hand user group list using the right arrow. Remove one or more user groups from a user by moving one or more user groups from the right-hand user group list to the left-hand user group list using the left arrow, as shown in Figure 2-18. Use Search available user groups or Search assigned user groups to isolate a particular user group or subset of user groups from which to choose, if necessary.

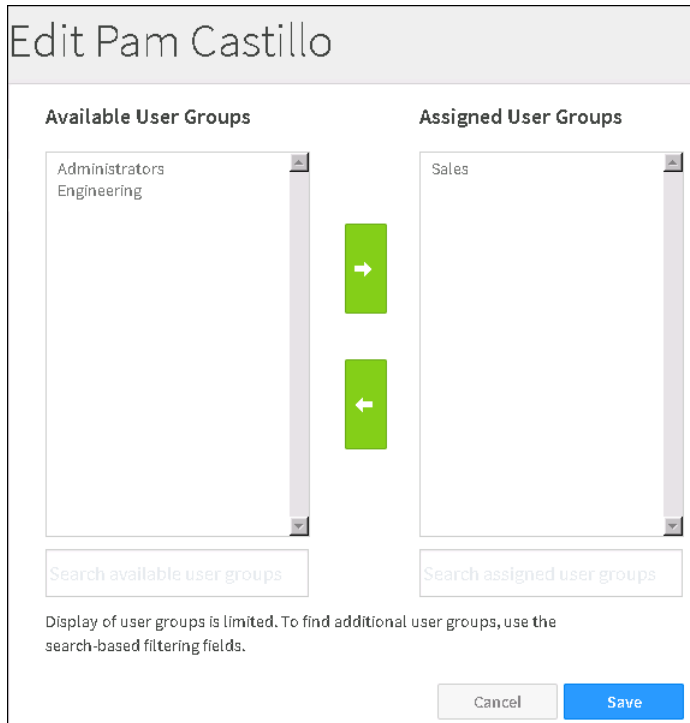


Figure 2-18 Assigning a user to or removing a user from a user group

- 5 Choose Assign Licenses from the side menu.
- 6 Assign or remove one or more license options for the user, if necessary.
- 7 Choose Assign User Groups from the side menu. Choose Save.

Viewing the list of users

Users displays all existing users. The account administrator can view the entire list, or a subset of the list. Choose Users to view the entire list. The administrator can filter the users list to display only the following user subsets:

- Users where the user name contains a specified search string
- Users belonging to a particular user group

The following sections describe how to filter the users list. These sections use the following example users:

- Pam Castillo
 - Belongs to a user group named Sales
- Walter Osborne

Belongs to a user group named Engineering

Filtering the list of users using a search string

The account administrator can filter the users list to display only users whose names contain a specified search string in the name. In Search, type the first letter or letters of a user name to display the names that start with the specified letter or letters. Search is not case-sensitive.

iHub Administration supports using an asterisk (*) in a search string as a wildcard character. The asterisk represents zero or more characters, excluding spaces and punctuation.

How to filter the list of users using a search string

Using the Users list shown in Figure 2-19, type 'w' in Search to find all user names that begin with this letter. iHub Administration automatically filters the list and displays the results, as shown in Figure 2-20.

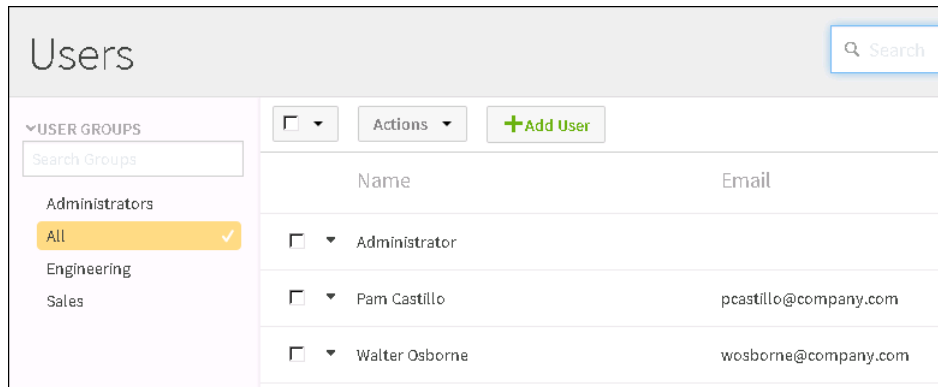


Figure 2-19 Viewing the users list before filtering

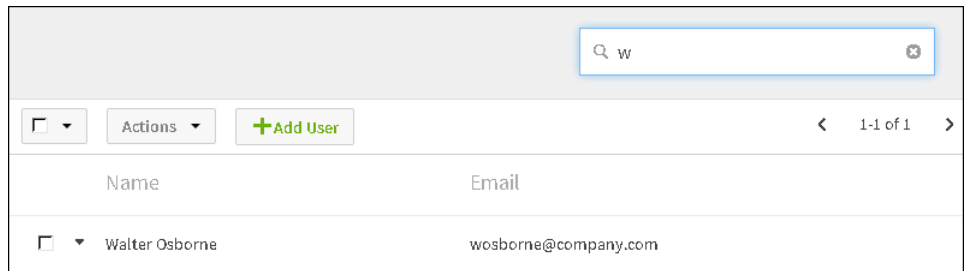


Figure 2-20 Viewing the results of filtering the users list

To display all list entries again, press the Backspace key or choose the 'x' icon in Search.

Filtering the list of users by user group

The account administrator can filter the users list to display only the users belonging to a selected user group.

How to filter the list of users by user group

- 1 In Users, choose a user group from the list of user groups appearing to the left of the users list to display only the users belonging to the chosen user group. For example, choose Sales to display Pam Castillo, the user belonging to the Sales user group, as shown in Figure 2-21.

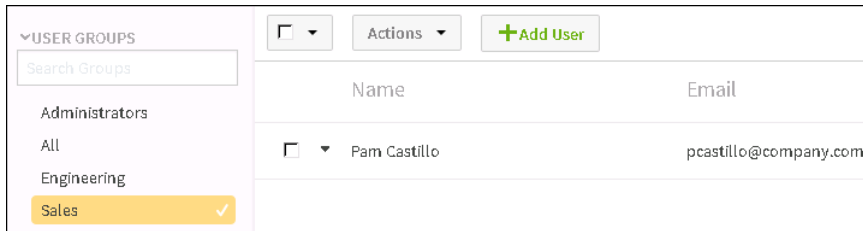


Figure 2-21 Left-clicking User Groups

Search Groups filters the list of user groups appearing to the left of the users list on Users similarly to the way Search filters the list of users.

- 2 Refresh the users list by choosing All from the list of user groups.

Deleting users

The administrator can delete one user only, or all users simultaneously.

How to delete a single user

Left-click the arrowhead icon next to the user name in the users list and choose Delete to delete a user, as shown in Figure 2-22.

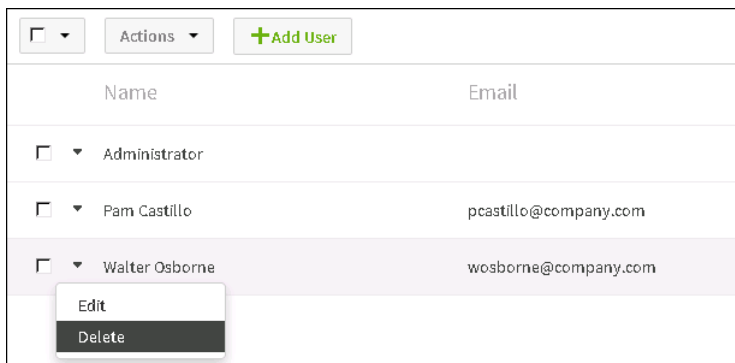


Figure 2-22 Deleting a single user

How to delete selected users

Check the boxes next to the users you want to delete. Then, left-click Actions and choose Delete. Using the users list shown in Figure 2-23 for example, System Console deletes Caroline Rojas and Jean Gaspard.

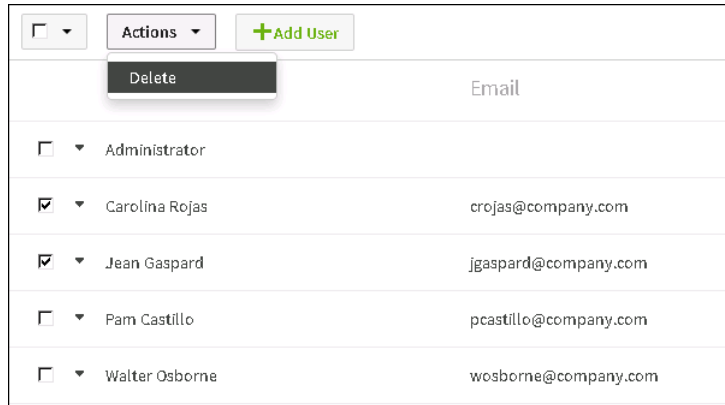


Figure 2-23 Deleting selected users

If the names of the users you want to delete share a common string, you can use the search feature to isolate the users, then use the Select All and Delete All features to delete the users. For example, using the users shown in Figure 2-23, perform the following tasks:

- 1 Type `*ar` in Search. Then choose the arrowhead icon in the checkbox to the left of Actions and select Select All, as shown in Figure 2-24.

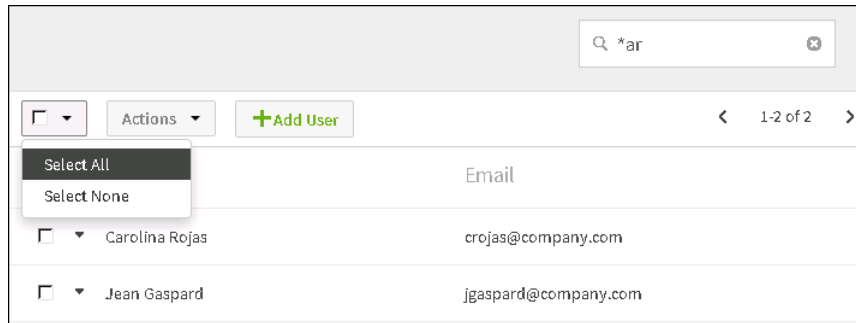


Figure 2-24 Choosing Select All to select all unhidden users

- 2 Choose Actions. Then, select Delete, as shown in Figure 2-25.

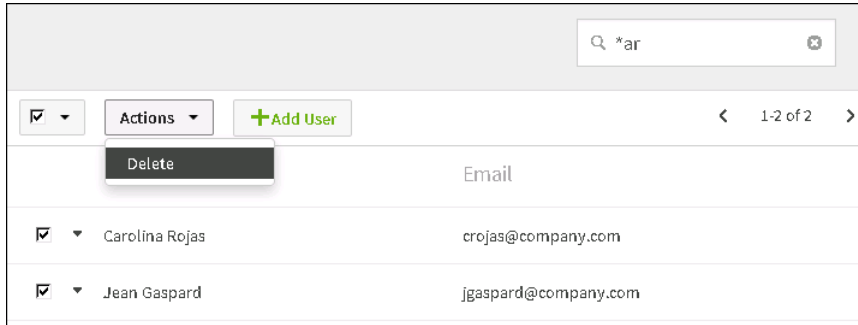


Figure 2-25 Choosing Delete All to delete all unhidden users

Choose All in the list of user groups or the 'x' icon in Search to display the entire users list. Caroline Rojas and Jean Gaspard no longer appear in the list.

Creating user groups

In iHub Administration, choose User Groups to perform the following tasks, as shown in Figure 2-26.

- Create a user group
- Edit a user group
- View or filter the list of user groups
- Delete user groups

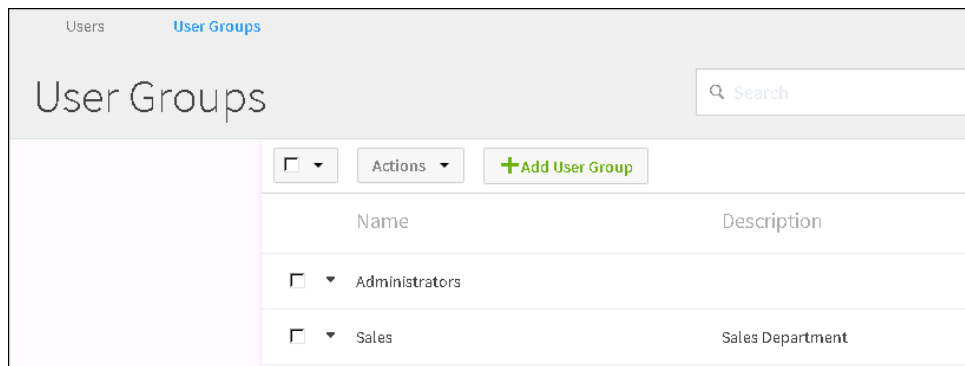


Figure 2-26 Viewing User Groups

The following sections describe how to perform these tasks.

Creating a user group

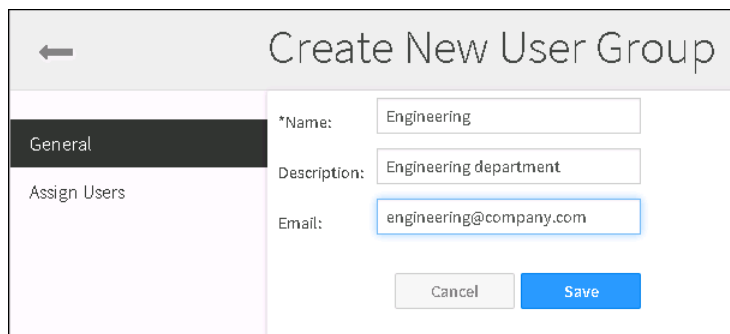
On User Groups, the administrator chooses Add User Group to create a new user group, as shown in Figure 2-26. On Create New User Group, a side menu lists the following categories, for which the administrator performs tasks to create a user group, as shown in Figure 2-27.

- **General**
Configure General properties, such as user group name and description.
- **Users**
Assign one or more users to the user group.

How to create a new user group

This section demonstrates creating a user group named Engineering.

- 1 On User Groups, choose Add User Group, as shown in Figure 2-26.
- 2 Set the following properties on Create New User Group—General, as shown in Figure 2-27.
 - **Name**
Type the user name.
 - **Description**
Type a description for the user group, such as the department name.
 - **Email**
Type an e-mail address for the user group.



The screenshot shows a mobile application interface for creating a new user group. The title is "Create New User Group" with a back arrow on the left. A side menu on the left has two options: "General" (which is selected and highlighted in black) and "Assign Users". The main content area contains three input fields: "*Name:" with the value "Engineering", "Description:" with the value "Engineering department", and "Email:" with the value "engineering@company.com". At the bottom right, there are two buttons: "Cancel" and "Save".

Figure 2-27 Specifying user group properties on General

- 3 Choose Assign Users from the side menu.
- 4 On Create New User Group—Users, assign Walter Osborne to the new user group by moving Walter Osborne from the left-hand list of users to the right-hand list of users, as shown in Figure 2-28. Use Search available users to isolate a particular user or subset of users from which to choose, if necessary.

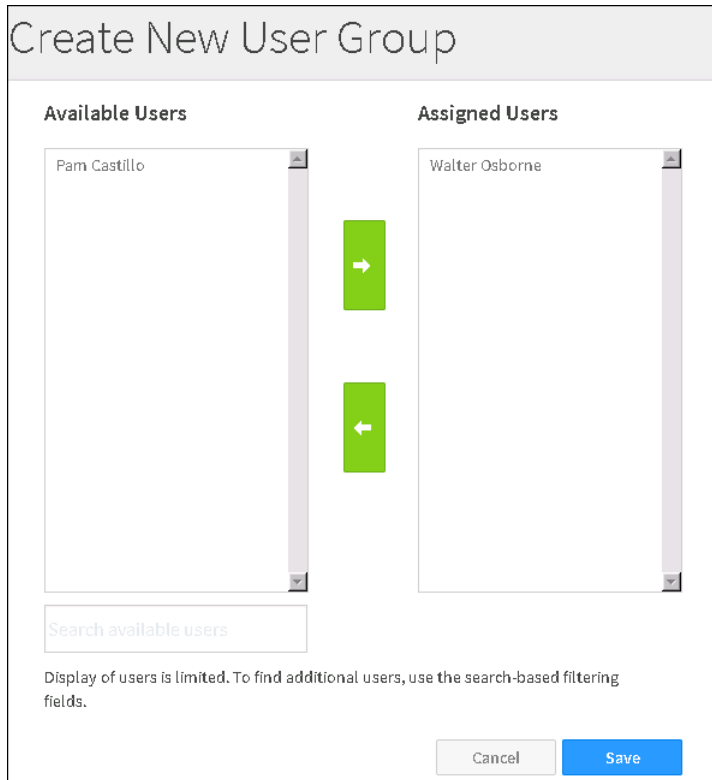


Figure 2-28 Assigning a user to a user group

Choose Save. Confirm that you want to save the changes.

Engineering appears in the list of user groups on User Groups.

Editing a user group

The administrator has the same level of control over a user group when editing the user group as when creating it, including adding or removing one or more users from the group.

How to edit a user group

- 1 Left-click the arrowhead icon next to a user group name and choose Edit, as shown in Figure 2-29.

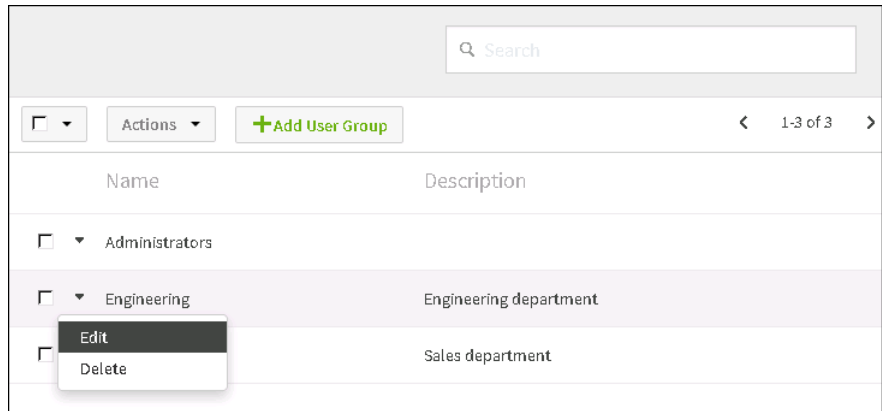


Figure 2-29 Choosing to edit a user group

- 2 On Edit <user group name>—General, make any necessary changes to any user property on Edit <user group name>, as shown in Figure 2-30.

Edit Engineering

*Name:

Description:

Email:

Figure 2-30 Editing a user group

- 3 Choose Assign Users from the side menu.
- 4 On Edit <user group name>—Assign Users, assign one or more users to a user group by moving one or more users from the left-hand user list to the right-hand user list using the right arrow. Remove one or more users from a user group by moving one or more users from the right-hand user list to the left-hand user list using the left arrow, as shown in Figure 2-31. Use Search available users or Search assigned users to isolate a particular user or subset of users from which to choose, if necessary.

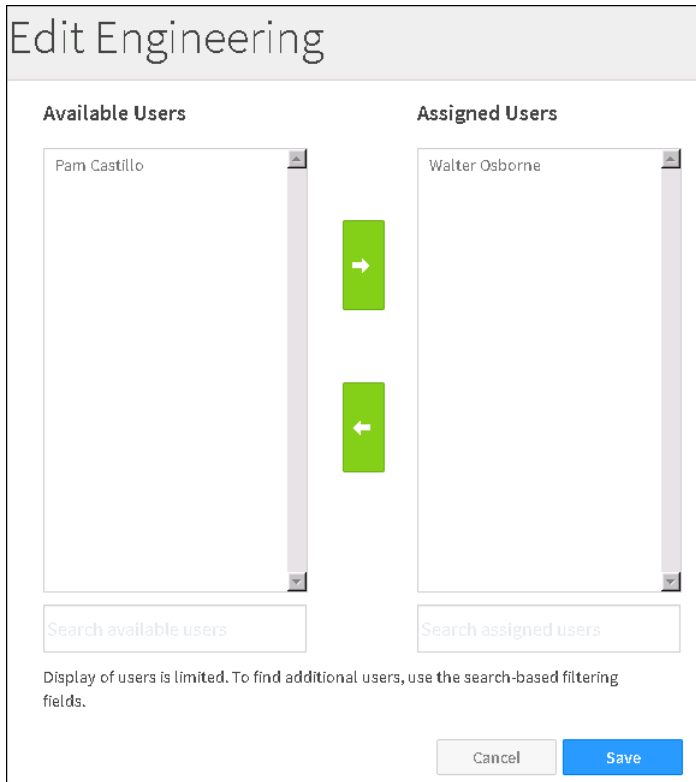


Figure 2-31 Assigning or unassigning a user to or from a user group
Choose Save to save any changes to the user group.

Viewing the list of user groups

User Groups displays all existing user groups. Choose User Groups to view the entire user groups list, or filter the list to display only the user groups where the user name contains a specified search string.

iHub Administration supports using an asterisk (*) in a search string as a wildcard character. The asterisk represents zero or more characters, excluding spaces and punctuation.

How to filter the list of user groups using a search string

Using the User Groups list shown in Figure 2-32 as an example, type *ee, one character at a time, in Search. Watch the effect of the filtering on the list of user groups after typing each character of the string. BIRT iHub automatically filters the list based on the string that Search contains. After typing the entire string in Search, the list contains one entry, the Engineering user group, as shown in

Figure 2-33.

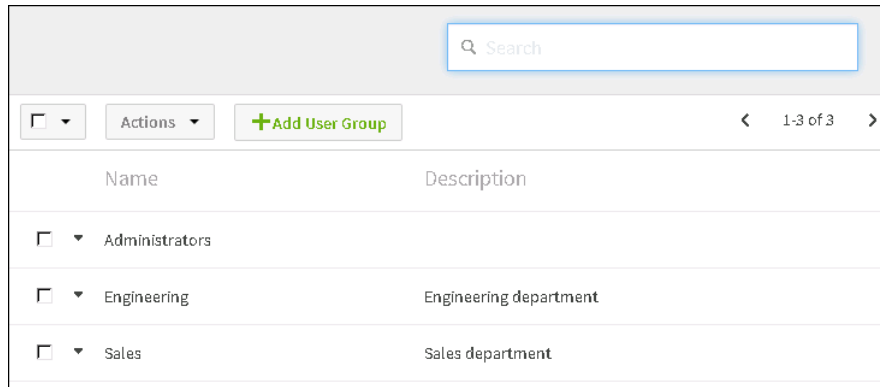


Figure 2-32 Viewing the user groups list before filtering

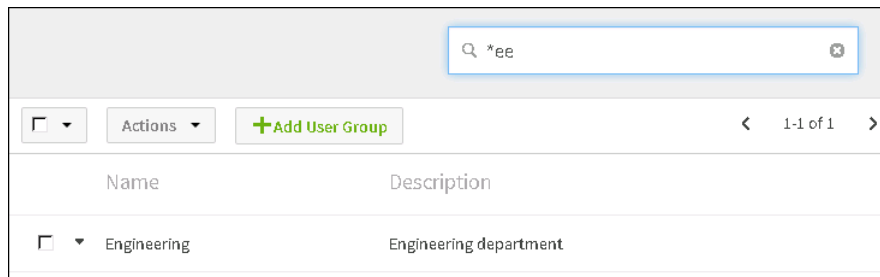


Figure 2-33 Viewing the results of filtering the user groups list

To display all list entries again, delete the string in Search by choosing the 'x' icon in Search, or press the Backspace key.

Deleting user groups

The administrator can delete one user group only, or all user groups simultaneously.

How to delete a single user group

Left-click the arrowhead icon next to the user group name in the list of user groups and choose Delete to delete a user group, as shown in Figure 2-34.

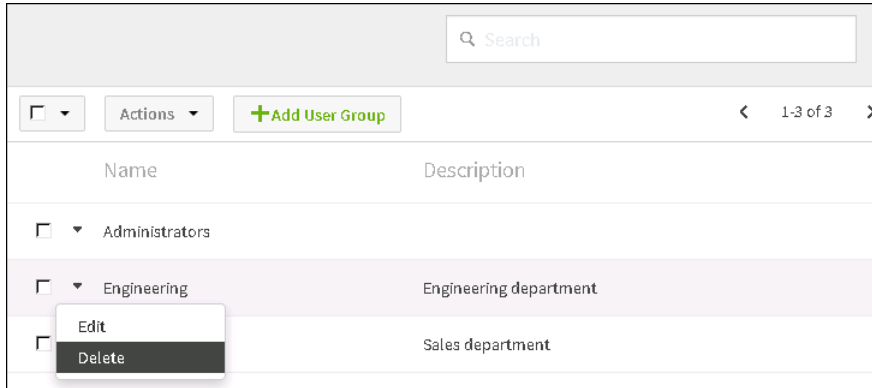


Figure 2-34 Deleting a single user group

How to delete selected user groups

Check the boxes next to the user groups you want to delete. Then, left-click Actions and choose Delete All. Using the user groups list shown in Figure 2-35 for example, System Console deletes Eastern and Western.

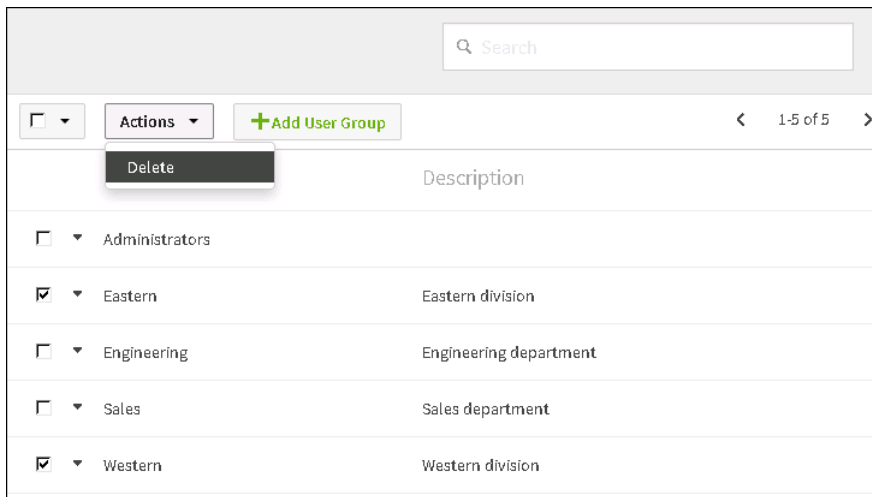


Figure 2-35 Deleting selected user groups

If the names of the user groups you want to delete share a common string, you can use the search feature to isolate the user groups, then use the Select All and Delete All features to delete the user groups. For example, using the user groups shown in Figure 2-35, perform the following tasks:

- 1 Type *ern in Search. Then choose the arrowhead icon in the checkbox to the left of Actions and select Select All, as shown in Figure 2-36.

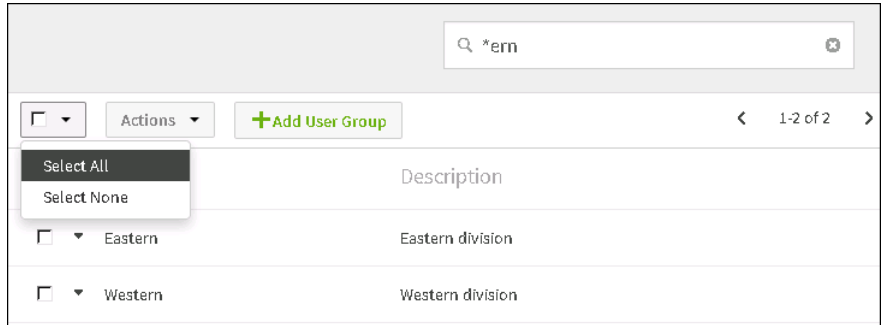


Figure 2-36 Choosing Select All to select all unhidden user groups

- 2 Choose Actions. Then, select Delete, as shown in Figure 2-37.

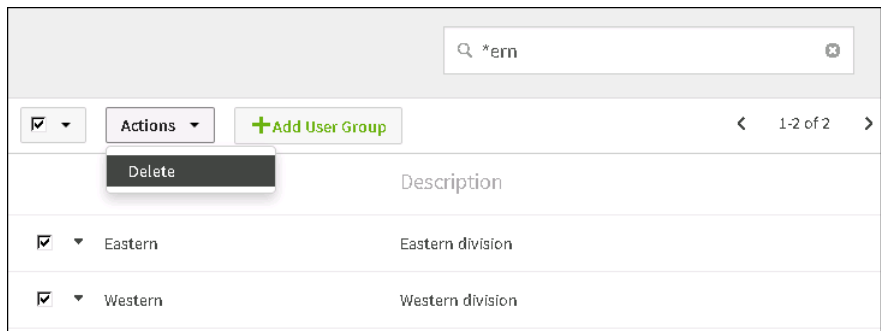


Figure 2-37 Choosing Delete All to delete all unhidden user groups

- 3 Choose the 'x' icon in Search to display the entire user groups list. The Eastern and Western user groups no longer appear in the list.

Accessing Logout and My Profile

Left-click the icon shown in Figure 2-38 to access Logout and My Profile.

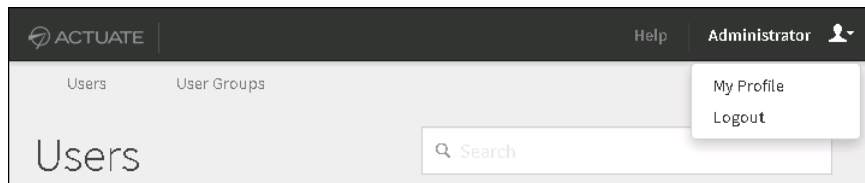


Figure 2-38 Accessing My Profile and Logout

The following descriptions of Logout and My Profile detail these features:

- Logout

Supports logging out of iHub Administration

- My Profile

Displays the properties of the logged in user, as shown in Figure 2-39

My Profile

*Name: Administrator

Description:

*Email:

Language: English (United States) ▾

Time zone: America/Los_Angeles ▾

Home Folder: /Home/administrator

Dashboard URL:

Change Your Password

Passwords are case sensitive.

Current Password:

Password:

Confirm Password:

Cancel Save

Figure 2-39 Viewing the properties of the logged-in user

3

Managing volume-level operations

This chapter contains the following topics:

- Working at the volume level
- About user and user group limits

Working at the volume level

The volume administrator performs management tasks for a volume by logging in to Visualization Platform and accessing Manage Volume. Manage Volume is visible only when logged in to Visualization Platform as a volume administrator.

How to access Manage Volume

- 1 Log in to Visualization Platform. For more information on this task, see "How to log in to Visualization Platform," in Chapter 1, "Getting started."
- 2 From the side menu, choose Manage Volume. Manage Volume—General appears, as shown in Figure 3-1.

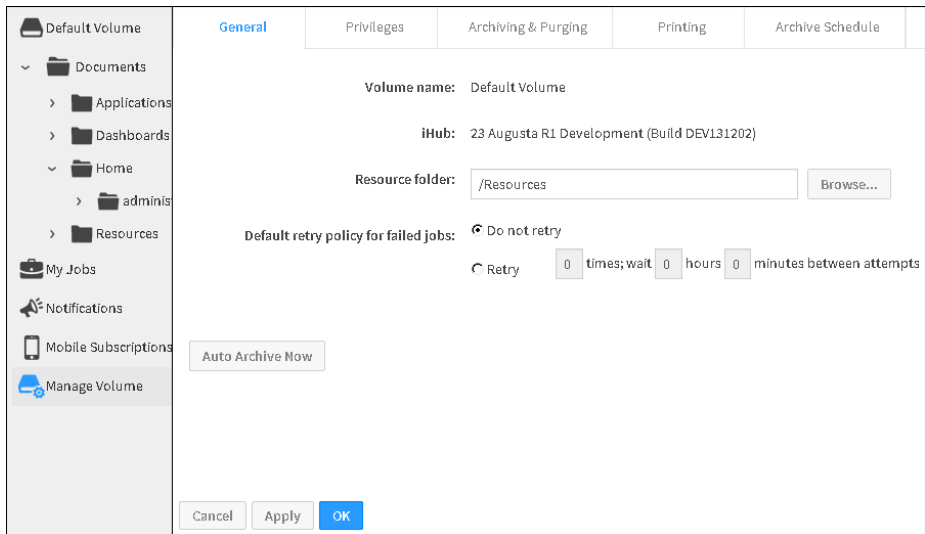


Figure 3-1 Choosing Manage Volume

Visualization Platform groups the tasks the volume administrator performs in Manage Volume into the following categories:

- **General**
Includes the following elements, as shown in Figure 3-1:
 - **Volume name**
Displays the name of the volume with which the volume administrator logged into Visualization platform.
 - **iHub**
Displays the name of the BIRT iHub version.
 - **Resource folder**

Displays the name of the folder containing sample resources. /Resources is the default.

- **Default retry policy for failed jobs**
Choose whether to retry a job that has failed. If choosing to retry a failed job, specify the number of times to retry the job, and the hours and minutes between attempts.
- **Auto Archive Now**
Choose Auto Archive Now to run an archiving cycle immediately. Auto Archive Now changes to Stop Archive Thread after choosing. Choose Stop Archive Thread to stop the archiving cycle.
- **Privileges**
Assign privileges such as read, write, and execute on the volume root folder to users and user groups. For more information, see “Setting volume privileges,” later in this chapter.
- **Archiving and Purging**
 - Set an autoarchiving policy for the volume.
 - Set a volume-level purge policy for job notices.For more information, see “Setting volume archiving and purging policies,” later in this chapter.
- **Printing**
Set volume-level printing properties. For more information, see “Setting volume level printer options,” later in this chapter.
- **Archive Schedule**
Schedule an archiving cycle. For more information, see “Scheduling an archiving cycle,” later in this chapter.

The following sections describe these categories.

Setting volume privileges

By default, all volume users have visible and read privilege on the volume root folder. The All user group represents all users. Assigning visible and read privileges to the All user group assigns these privileges to all users. The volume administrator can assign privileges on the root folder to any user or user group.

How to set privileges on the volume root folder

- 1 Choose Manage Volume from the side menu in Visualization Platform. Then, select Privileges.

- 2 On Privileges, select a user or user group from Available and move it to Selected using the right arrow.
- 3 Assign privileges to a selected user or user group by selecting from the list of privileges. For example, Figure 3-2 shows assigning write privilege on the volume root folder to the Engineering user group. Choose OK.

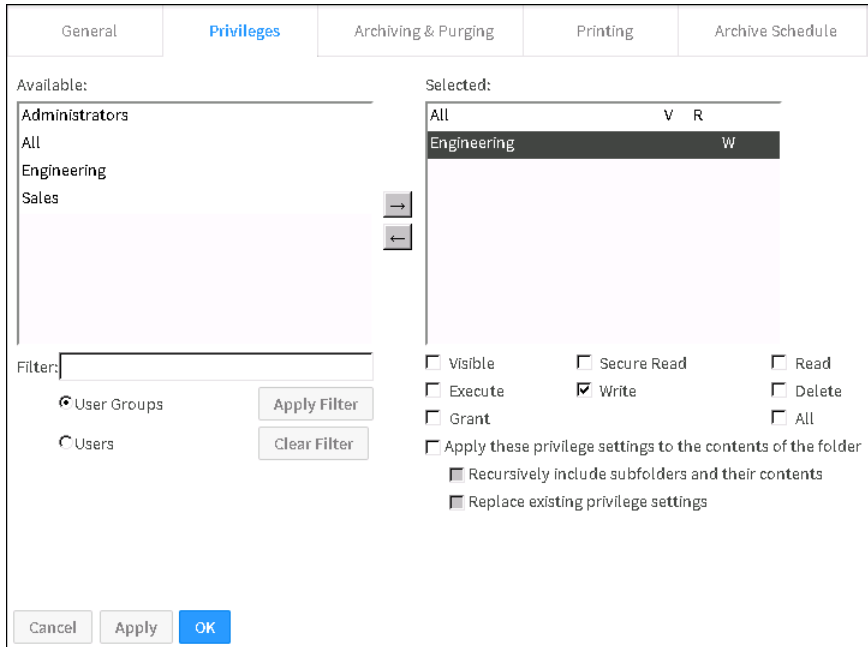


Figure 3-2 Setting privileges on the volume root folder

Setting volume archiving and purging policies

On Manage Volume—Archiving and Purging, shown in Figure 3-3, the administrator can set the autoarchive policy for all the files and empty folders in the 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, BIRT iHub 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. BIRT iHub retains the values you set for multiple file types and applies the values when you choose OK.

General	Privileges	Archiving & Purging	Printing	Archive Schedule
<p>Auto archive policy for this volume:</p> <p>File Type: <input type="text" value="Default"/></p> <p> <input checked="" type="radio"/> Use the default policy <input type="radio"/> Do not automatically delete files <input type="radio"/> Delete when older than <input type="text" value=""/> days <input type="text" value=""/> hours <input type="checkbox"/> Archive files before deletion </p> <p>Default user notice purging setting for this volume:</p> <p> <input type="checkbox"/> Purge success notices after <input type="text" value="0"/> days <input type="text" value="0"/> hours <input type="checkbox"/> Purge failure notices after <input type="text" value="0"/> days <input type="text" value="0"/> hours </p> <p><small>Note : Changes to expiration settings apply only to newly created or uploaded files. Settings for existing files will be unaffected.</small></p> <p> <input type="button" value="Cancel"/> <input type="button" value="Apply"/> <input type="button" value="OK"/> </p>				

Figure 3-3 Setting the default archiving and purging policy for the volume Manage Volume—Archiving and Purging also displays the settings for the volume’s default purging policy. Using the options described in Table 3-1, the volume administrator sets the volume default policy specifying how long a job completion notice remains on the volume before BIRT iHub can delete the notice.

Table 3-1 Purge settings

Property	Description
Purge success notices after <i>n</i> days <i>n</i> hours	Enable deleting job completion notices for jobs that succeed. Set the time after which BIRT iHub can delete the notice. If the administrator specifies 0 days 0 hours, or does not select this option, BIRT iHub does not purge success notices.
Purge failure notices after <i>n</i> days <i>n</i> hours	Enable deleting job completion notices for jobs that fail. Set the time after which BIRT iHub can delete the notice. If the administrator specifies 0 days 0 hours, or does not select this option, BIRT iHub does not purge failure notices.

Archiving files and removing empty folders

By performing the following volume autoarchiving tasks, volume administrators and users specify the policy that BIRT iHub uses to delete files and empty folders, and archive files and folders in the volume:

- Using Visualization Platform, an administrator can set the autoarchive policy for the entire volume and for specific files and folders.
- 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.

BIRT iHub 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 volume

To see a folder's autoarchive policy, point to the arrowhead icon next to a folder and choose Auto Archive. On Auto Archive policy for this folder, choose View Policy.

To see a file's auto archive policy, left-click the arrowhead icon next to the file and choose Details. The policy appears under the Auto Archive heading.

When BIRT iHub performs autoarchiving, it starts from the volume's root folder. For each file whose age has expired, BIRT iHub deletes the file. If the Archive files before deletion option is selected, BIRT iHub calls the archive application for the volume, then deletes the file if the archive process succeeds. If the archive process fails, BIRT iHub does not delete the file.

Setting volume level printer options

The volume recognizes and supports printers that are set up for BIRT iHub. You do not have to install printers specifically for the volume. You do, however, customize printer settings for each printer that is available to the volume.

Only a volume administrator can set printer options at the volume level. Users can accept values for these printer properties as defaults, or set them on individual print jobs.

Table 3-2 describes these properties.

Table 3-2 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.
2-Sided printing	Select: <ul style="list-style-type: none">■ 1-Sided Print■ Flip on long edge (double-sided, side by side)■ Flip on short edge (double-sided, top to top)
Page size	An extensive drop-down list of standard international formats.
Paper tray	The paper source.

Some printers do not support all these options.

When a user prints a document, BIRT iHub adheres to printing specifications from the following sources, in order of precedence:

- Printer property values set for the current print job.
- Printer property values that are set at the volume level by the volume administrator.

For a print request when scheduling a job, BIRT iHub uses the page size that the user explicitly selects. If the user does not select a page size, BIRT iHub uses the page size that the scheduled design or document specifies. If the scheduled design or document does not specify a page size, BIRT iHub uses the volume default setting.

Using Manage Volume—Printing, a volume administrator can set property values for any BIRT iHub printer and specify the default printer for a volume.

How to set volume-level printer properties

- 1** Choose Manage Volume from the side menu in Visualization Platform. Then, select Printing.
- 2** On Printing, specify a default printer and printer settings for the volume, as shown in Figure 3-4.

If available, BIRT iHub 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.

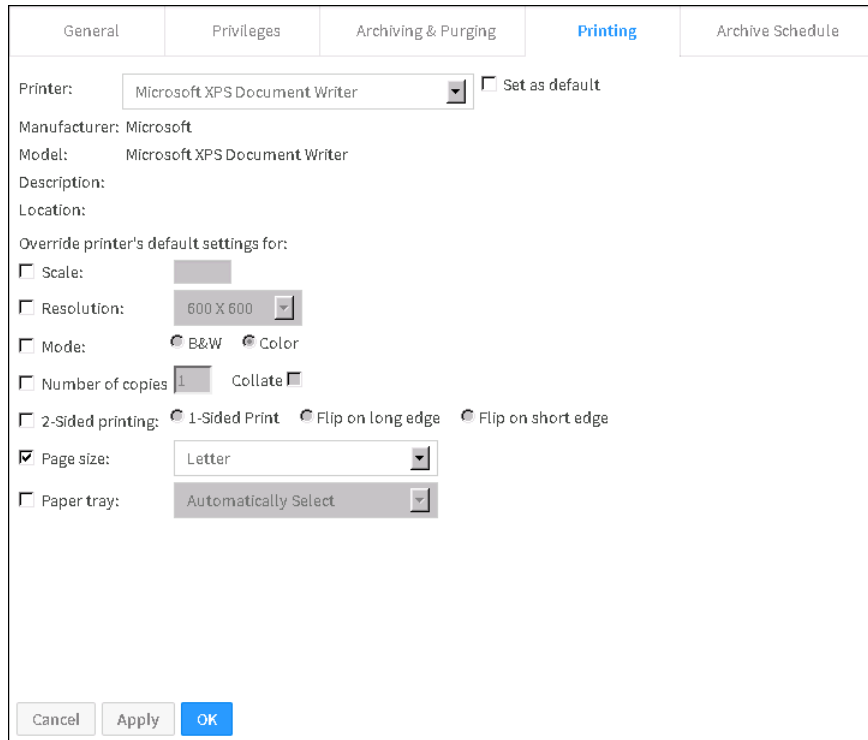


Figure 3-4 Setting print properties on Volume—Properties—Printing

Understanding service requirements

Running jobs in a volume requires the following BIRT iHub services, which the installation program configures by default:

- View and Factory services for running designs unscheduled
- The Factory service for running scheduled jobs

BIRT iHub 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.

Scheduling an archiving cycle

Choose Archive Schedule, as shown in Figure 3-5, to schedule regular archive sweeps. You can specify the time zone, frequency, date, and time. You can exclude specific dates from the pattern that you create using Excluding these dates. You specify duration using the Start date and End date. Add the schedule to the list of schedules by choosing Add Schedule Line. Remove a schedule by selecting the schedule from the list of schedules and choosing Delete Schedule Line.

By default, BIRT iHub performs an autoarchive sweep once daily.

General Privileges Archiving & Purging Printing **Archive Schedule**

TimeZone: America/Los_Angeles

Every day at 2:15 AM starting 12/6/2013

Frequency :

Once

Every 1 days

Every weeks on: Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Day of every months

The First Day of every months

Time: 2:15 AM (h:mm a)

Start date: 12/6/2013 # (M/d/yyyy) Excluding these dates:

End date: # (M/d/yyyy) > <

(M/d/yyyy)

Cancel Apply **OK** Add Schedule Line Delete Schedule Line

Figure 3-5 Configuring an archiving schedule

About user and user group limits

Some of the relationships in the volume have recommended and hard limits. If you adhere to the recommended limits, the appearance, behavior, and performance of Visualization Platform is acceptable. Your web browser imposes

the hard limits. Table 3-3 shows the limits for the volume.

Table 3-3 Limits for the volume

Relationship	Recommended limit	Hard limit
User groups of which a particular user is a member	100	2000
Users and user groups notified about a particular job	100	1000
Users and user groups in a single access control list (ACL) for a file or folder, including ACLs that jobs create	100	2000
Users who are members of a particular user group	Unlimited (greater than 1,000,000)	

Exploring administrative capabilities

This chapter contains the following topics:

- Using the /Applications folder
- About locale maps
- Using Advanced Jobs
- Configuring events
- Using a java policy file to control access to protected resources

Using the /Applications folder

In Visualization Platform, /Applications is a folder for BIRT iHub applications that developers publish. Actuate recommends that the administrator perform the following actions regarding the /Applications folder as a best practice:

- Create a user group named Developers for example, then assign read, execute, and write privilege on the /Applications folder to the Developers user group.
- Assign only execute privilege on the /Applications folder to users who are not developers and to the default All user group so that the /Applications folder is visible only to users belonging to the Developers user group. Users who do not belong to the Developers user group can still access an application in /Applications using a URL such as `http://localhost:8700/portal/Applications/<application name>` after logging in to Visualization Platform. The application developer or administrator provides this URL.

About locale maps

The administrator can customize a date, time, or currency expression for a particular locale by modifying a date, time, or currency format for that locale in a localemap.xml file. A localemap.xml file contains a Locale ID element for each language in which Visualization Platform displays content. The Locale ID element contains subelements specifying the date, time, and currency formats for each language. BIRT iHub uses the following locale maps:

- `AC_SERVER_HOME\web\portal\WEB-INF\localemap.xml`
Formats timestamps that Visualization Platform displays in:
 - the Modified column of a file or folder listing.
 - the Finished column of a My Jobs or Notifications listing.
- `AC_SERVER_HOME\etc\localemap.xml`
Formats a date or time that one of the following items generates when used in an output document name or output document version name:
 - A predefined date-and-time format keyword
 - A date format symbol
 - A time format symbol

If you update localemap.xml, you must restart the cluster for the changes to take effect. In a cluster, the same localemap.xml files must reside on every BIRT iHub machine to achieve consistency among nodes. For information about starting and stopping a cluster, see Chapter 5, “Managing Clusters,” in *System Administrator Guide*.

A locale definition in `localemap.xml` does not necessarily specify a value for every date, time, or currency field. For a field with no specified value, BIRT iHub uses the default locale's value for that field. In a `localmap.xml` file, the Locale ID named "default" specifies the default date, time, and currency formats.

For more information about date and time formats, see Chapter 3, "Scheduling and managing jobs," in *Using Visualization Platform*.

Using Advanced Jobs

My Jobs displays basic information about the status of jobs. For each category in My Jobs, there is a basic view available to all users and an Advanced Jobs view available only to the administrator. The administrator can cancel a scheduled job or override settings specified by a user. Additionally, when performing advanced scheduling tasks, the administrator can use the file menu next to each job to perform additional actions. For more information on My Jobs, see Chapter 3, "Scheduling and managing jobs," in *Using Visualization Platform*.

Using the available job monitoring options

For scheduled jobs, administrators can perform the following tasks:

- View details for a job
- View and modify scheduling properties for one or more jobs
- Clone a job
- Delete a job

For scheduled jobs waiting for an event, pending, or running administrators can cancel one or more of these jobs simultaneously.

For completed jobs administrators can perform the following tasks:

- Retry one or more jobs
- Delete one or more jobs
- Open Document
Opens the output document. You can also choose the output document name to view the output document.
- Print Document on Server
Displays the same printing properties as on Advanced Scheduling—Print. Configure print properties and choose OK to print the output document on the server.
- Schedule

Displays Advanced Scheduling job properties. Modify any scheduled job property. Then choose OK to submit the job.

- Delete
Deletes this job from Completed.

Table 4-4 describes the available options in the categories in My Jobs and lists whether the option is available in the basic or advanced jobs view.

Table 4-4 Options for job schedules

Option	Description	Basic	Advanced
Cancel	Cancels this job and moves it from Waiting for Event to Completed.		✓
Clone	Creates a copy of the job. Displays Advanced Scheduling job properties. Modify any scheduled job property.		✓
Details	Job details.	✓	✓
Document Pages	Number of pages in the output document.		✓
Event Name	Name the user gives to the event that triggers job execution.	✓	✓
Event Parameter	Identifies the event criteria BIRT iHub uses to determine whether to trigger job execution. For example, if Event Type is FileEvent and Event Parameter is a file name, BIRT iHub executes the job when iHub detects that the file that Event Parameter specifies has been created.	✓	✓

Table 4-4 Options for job schedules

Option	Description	Basic	Advanced
Event Status	<p>Status of the state between BIRT iHub and the event that triggers job execution. Possible states are:</p> <ul style="list-style-type: none"> ■ Uninitialize BIRT iHub did not start monitoring the system for the event. ■ Polling While monitoring the system for event criteria that triggers job execution BIRT iHub has not found matching criteria. ■ Satisfied BIRT iHub found matching event criteria and executed the job. ■ Expired BIRT iHub did not find matching event criteria within the polling interval or a user canceled the job. 	✓	✓
Event Type	<p>Can be one of the following:</p> <ul style="list-style-type: none"> ■ File Event BIRT iHub runs the job when a file the user specifies is created. ■ Job Event BIRT iHub runs the job when a job the user specifies succeeds or fails. The user specifies whether job event success or failure triggers execution of the job being scheduled. ■ Custom Event BIRT iHub runs the job when a web service the user specifies returns a signal to BIRT iHub. 	✓	✓
Executable Name	Name of the design being run.		✓
Finished	Date and time the job finished.	✓	✓

(continues)

Table 4-4 Options for job schedules

Option	Description	Basic	Advanced
Job Name	By default, the name of the design being run. Alternatively, a job name the user specifies.	✓	✓
Next Run	Date and time the job runs next.		✓
Owner	The name of the user who submitted the job		✓
Priority	Job priority. The higher the number, the higher the priority.		✓
Properties	Displays Advanced Scheduling job properties. Modify any scheduled job property.		✓
Report Name	Name of the design being run.	✓	✓
Result	Succeeded or Failed.	✓	✓
Retry	Submits the job again, making no changes to any job property.		✓
Started	Date and time the job was started.	✓	✓
Submitted	Date and time the user submitted the job.	✓	✓

The following section describes the actions an administrator can perform in Advanced Jobs, for each job phase category:

Working with scheduled jobs

For a single job, point to the arrowhead icon next to a job name and select one of the following options:

- Details
 - In Advanced Jobs, Details consists of the following categories:
 - Summary
 - Details about the following job components:
 - Job
 - Executable
 - Output document
 - Properties
 - Details about the following scheduled job properties:
 - Job

- Executable
- Schedule
- Parameters
- Output Document
- Privileges
- Notifications
- Email Notification
- Print
- Properties
Displays Advanced Scheduling job properties. Modify any scheduled job property.
- Clone
Creates a copy of this job. Displays Advanced Scheduling job properties. Modify any scheduled job property.
- Delete
Deletes this job from Schedules.

Select two or more jobs. Then, point to Act upon selected schedules and select one of the following options:

- Properties
Displays Advanced Scheduling job properties for the jobs you select. BIRT iHub displays only the properties that do not need to be unique to each job. For example, BIRT iHub does not show job name or output document name because these properties must remain unique for each job. Modify any scheduled job property that appears.
- Delete
Deletes the jobs you select from Schedules.

Working with jobs waiting for an event

For a single job, point to the arrowhead icon next to the job name and select one of the following options:

- Details
In Advanced Jobs, Details consists of the following categories:
 - Summary
Details about the following job components:
 - Job

- Executable
 - Output document
- Properties
 - Details about the following scheduled job properties:
 - Job
 - Executable
 - Schedule
 - Parameters
 - Output Document
 - Privileges
 - Notifications
 - Email Notification
 - Print
- Cancel
 - Cancels this job and moves it from Waiting for Event to Completed.

For two or more jobs, select the jobs. Then, select Actions—Cancel to cancel the jobs you select. BIRT iHub moves the jobs from Waiting for Event to Completed.

Working with pending jobs

The selectable options on Pending for a single job and for two or more jobs are the same options as on Waiting for Event.

Working with running jobs

The selectable options on Running for a single job and for two or more jobs are the same options as on Waiting for Event.

Working with completed jobs

For a single job that succeeds, point to the arrowhead icon next to the job name and select one of the following options:

- Details
 - In Advanced Jobs, Details consists of the following categories:
 - Summary
 - Details about the following job components:
 - Job

- Executable
 - Output document
- Status

Details about the outcome of the completed job include the following information:

 - Results
 - Status
- Properties

Details about the following scheduled job properties:

 - Job
 - Executable
 - Schedule
 - Parameters
 - Output Document
 - Privileges
 - Notifications
 - Email Notification
 - Print
- Open Document

Opens the output document. You can also choose the output document name to view the output document.
- Print Document on Server

Displays the same printing properties as on Advanced Scheduling—Print. Configure print properties and choose OK to print the output document on the server.
- Schedule

Displays Advanced Scheduling job properties. Modify any scheduled job property. Then choose OK to submit the job.
- Delete

Deletes this job from Completed.

For a single job that fails, point to the arrowhead icon next to the job name and select one of the following options:

- Details

Displays the same details as for a single job that succeeds.

- **Retry**
Submits the job, making no changes to any job property.
- **Schedule**
Displays Advanced Scheduling job properties. Modify any scheduled job property. Then choose OK to submit the job.
- **Delete**
Deletes this job from Completed.

For two or more jobs, select the jobs. Then, point to Actions and select one of the following options:

- **Retry**
- **Delete**

Filtering jobs

Users can specify filter conditions in any job category to view specific jobs. This feature is useful when a job category contains a long list of jobs. Additionally, an administrator can specify filters in Advanced Jobs—Schedules and Advanced Jobs—Completed to view scheduled jobs that meet the following conditions:

- **Active**
- **Canceled**
- **Expired**
- **Failed**
- **Succeeded**

For example, in Advanced Jobs—Schedules, to view all Active jobs, deselect Canceled and Expired as shown in Figure 4-6.

Schedules	Waiting for Event	Pending	Running	Completed
Filter:	<input type="text"/>	<input checked="" type="checkbox"/> Active	<input type="checkbox"/> Cancelled	<input type="checkbox"/> Expired
		<input type="button" value="Reset"/>	<input type="button" value="Apply"/>	

Figure 4-6 Creating a filter to view active jobs

Visualization Platform excludes all jobs that were canceled and all jobs that were run in the past from the displayed results.

To view Failed jobs, in Advanced Jobs—Completed, deselect Succeeded and Canceled, as shown in Figure 4-7.

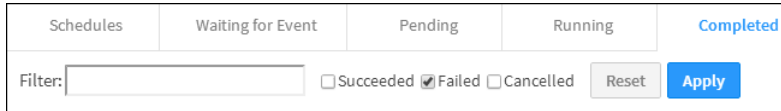


Figure 4-7 Creating a filter to view failed jobs

Visualization Platform excludes all jobs that were canceled and all jobs that were run successfully from the displayed results.

Editing a scheduled job

The administrator can edit a scheduled job. A user can only delete a scheduled job.

How to edit a scheduled job

- 1 Log in to Visualization Platform as Administrator.
- 2 In the navigation pane, choose My Jobs.
- 3 In the inner banner, choose Advanced Jobs, as shown in Figure 4-8.

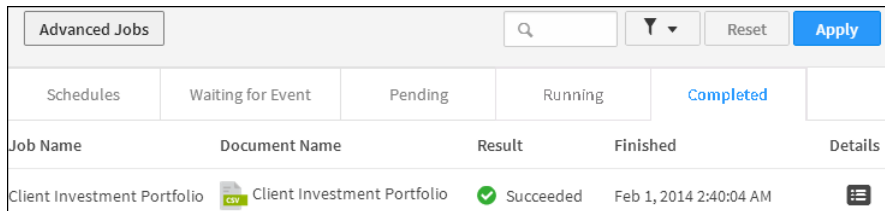


Figure 4-8 Choosing Advanced Jobs

- 4 In Schedules, from the menu icon next to a job, choose Properties, as shown in Figure 4-9.

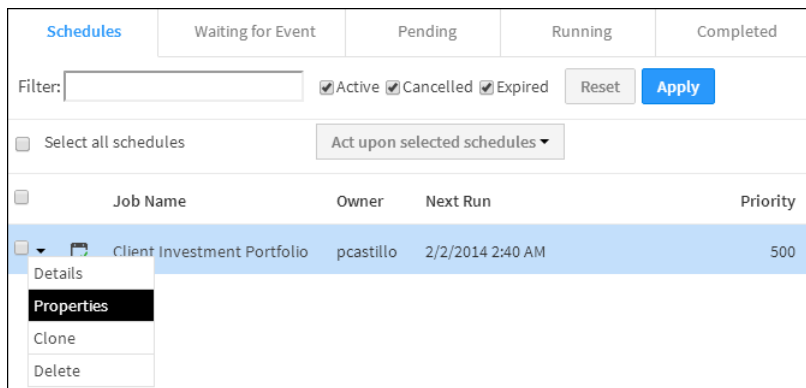


Figure 4-9 Viewing properties for a scheduled job

- 5 Visualization Platform displays the Advanced Scheduling job categories for the job. Make any desired job property modifications and choose OK.

Deleting a scheduled job

The administrator can delete a job before BIRT iHub processes it. You cannot recover a deleted job. After BIRT iHub processes a job, iHub removes the job from Jobs—Schedules and moves it to Jobs—Completed.

How to delete a scheduled job

In Advanced Jobs—Schedules, from the file menu for the job to delete, choose Delete, as shown in Figure 4-10.

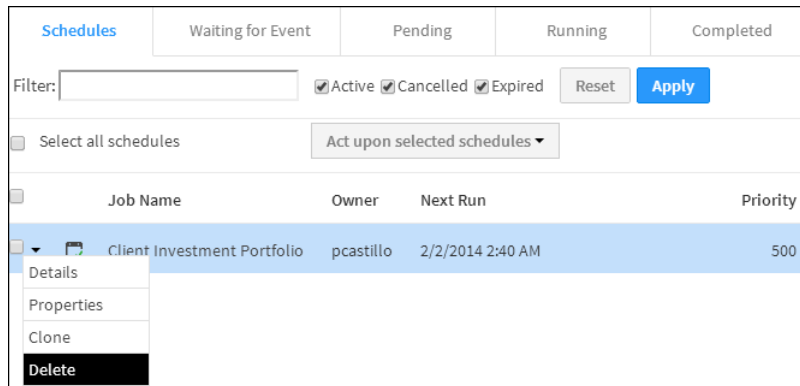


Figure 4-10 Deleting a scheduled job

The administrator can also cancel a job in Waiting for Event, Pending, and Running using the file menu for the job and choosing Cancel from the menu that appears.

Cloning a job

The administrator can create a copy of a job by selecting Clone in the file menu. Visualization Platform displays Advanced Scheduling job properties. You can modify any scheduled job property.

How to clone a job

In Advanced Jobs—Schedules, from the file menu for the job to clone, choose Clone. Visualization Platform displays the Advanced Scheduling job categories for the new job. Make any desired job property modifications and choose OK to schedule the job.

Configuring events

When a user needs to schedule a job based on a custom event, the administrator configures properties in the shared configuration file, `acsserverconfig.xml`, to set up a web service application for triggering the job to run. This section describes these properties.

The `AC_CONFIG_HOME` variable represents the path to the folder containing `acsserverconfig.xml`. In a default BIRT iHub installation on Windows, performed using the graphical installer, in which the install folder is `C:\Actuate`, `AC_CONFIG_HOME` represents the following path:

```
C:\Actuate\BIRTiHubVisualization\modules\BIRTiHub\iHub\shared
  \config
```

In a cluster consisting of two or more nodes, `AC_CONFIG_HOME` represents the shared configuration directory the system administrator created before adding the second node to a cluster. For more information, see "Adding cluster nodes to a cluster," in Chapter 5, "Managing clusters," in *BIRT iHub System Administration Guide*.

The administrator configures event-based job properties by specifying values for the following variables in `acsserverconfig.xml`:

- **EventPollingInterval**
Specifies the frequency in minutes that iHub checks for a system event. The default value is 5 minutes.
- **EventPollingDuration**
Specifies the duration in minutes that BIRT iHub checks for an event. If the event does not occur within the allotted time, BIRT iHub marks it as expired. A user can customize this value when creating an event-driven schedule. This value applies to all types of system events. The default value is 300 minutes.
- **EventLagTime**
Specifies the minutes that BIRT iHub scans for completed jobs to determine if an event occurred. For example, if you submit an event-based schedule with the default event lag time, BIRT iHub checks the status of jobs for the previous 60 minutes. If the event occurred within the previous 60 minutes, it sets the event status to satisfied. The default value is 60 minutes.
- **EnableCustomEventService**
A flag that enables BIRT iHub custom event processing for a scheduled job. If the value is true, the service is enabled. If you change the value to false, all the existing instances of scheduled jobs using the custom event fail. This configuration value also affects the `EnableEventService` property value in the Actuate IDAPI `GetVolumeProperties` response. The default value is True.

- CustomEventServiceIPAddress
Specifies the server name or IP address where the custom event service resides. The default value is localhost.
- CustomEventServicePort
Specifies the number of a valid, used port for the custom event service. iHub uses an application container to host web services applications. The default value is 8700.
- CustomEventServiceContextString
Specifies the context string of the request URL for sending a message to the custom event service. The default value is /acevent/servlet/AxisServlet.

Using a java policy file to control access to protected resources

By default, a BIRT design cannot obtain permission to perform a potentially unsafe operation, such as opening an internet connection. If the administrator needs to further restrict operations a BIRT design has permission to perform, the administrator can implement restrictions using a java policy file. A volume implements a java.security.Policy object. The Policy object obtains permission information from a java policy file. This section describes how to use a policy file.

If the administrator wants to keep a set of restrictions in place, but the design developer needs to work around a restriction, the developer can implement a java-based event handler, which the administrator can place in a .jar file in the AC_SERVER_HOME/resources folder. BIRT iHub places no restriction on the actions a program residing in AC_SERVER_HOME/resources may perform. As an example, if a report developer wants to create a BIRT design that obtains customer-specific information from a public entity, the developer can create an event handler that calls an application which obtains the customer information. The administrator places the event handler in AC_SERVER_HOME/resources. When the BIRT design needs to load the customer information, the design calls the event handler, which in turn calls the application that retrieves the customer information.

This section makes reference to the AC_CONFIG_HOME variable, which represents the shared configuration directory which all nodes in a cluster access. In a default BIRT iHub installation on Windows, performed using the installer, in which the install folder is C:\Actuate, AC_CONFIG_HOME represents the following path:

```
C:\Actuate\BIRTiHubVisualization\modules\BIRTiHub\iHub\shared
  \config
```

In a cluster consisting of two or more nodes, AC_CONFIG_HOME represents the shared configuration directory the system administrator created before adding

the second node to a cluster. For more information, see "Adding cluster nodes to a cluster," in Chapter 5, "Managing clusters," in *BIRT iHub System Administration Guide*.

How to create and enable a policy file

- 1 In System Console—Clusters, edit the cluster. Then, from the Manage Cluster menu, choose Stop Cluster to stop the cluster. Wait until all services stop before going to the next step.
- 2 Using Windows Explorer, navigate to AC_CONFIG_HOME.
- 3 Open acserverconfig.xml in a text editor.
- 4 Edit each <ServerResourceGroupSetting> element, adding the Djaserver.security argument to the StartArguments attribute definition, as shown in the following code sample:

```
StartArguments="-Djaserver.security -Xmx512M
-XX:MaxPermSize=256m -XX:-UsePerfData
-Djava.awt.headless=true
-Djava.protocol.handler.pkgs=com.actuate.jaserver.protocol
com.actuate.jaserver.Server"
```

The following example shows the <ServerResourceGroupSetting> element for the Default BIRT Online resource group in the small template after adding the Djaserver.security argument to the StartArguments attribute definition:

```
<ServerResourceGroupSetting
    Name="Default BIRT Online"
    Activate="TRUE"
    MinFactory="1"
    StartArguments="-Djaserver.security -Xmx512M
-XX:MaxPermSize=256m -XX:-UsePerfData
-Djava.awt.headless=true
-Djava.net.preferIPv4Stack=true
-Djava.protocol.handler.pkgs=
com.actuate.jaserver.protocol
com.actuate.jaserver.Server"/>
```

Save and exit acserverconfig.xml.

- 5 In AC_CONFIG_HOME, create a new file named jaserver.policy. You can create this file manually, or use the Policy Tool utility to create the file. Launch the Policy Tool by executing AC_JAVA_HOME\bin\policytool.exe in a command prompt. In a default BIRT iHub installation on Windows, performed using the installer, in which the install folder is C:\Actuate, AC_JAVA_HOME represents the following path:

```
C:\Actuate\BIRTiHubVisualization\modules\JDK64
```

Instructions for using the Policy Tool utility can be found at the following location:

<http://docs.oracle.com/javase/7/docs/technotes/guides/security/PolicyGuide.html>

Listing 4-1 shows example policy file content:

Listing 4-1 Viewing example policy file content

```
grant codeBase "file:${AC_SERVER_HOME}/Jar/-" {
    permission java.security.AllPermission;
};
grant codeBase "file:${AC_SERVER_HOME}/MyClasses/-" {
    permission java.security.AllPermission;
};
grant codeBase "file:${AC_SERVER_HOME}/drivers/-" {
    permission java.security.AllPermission;
};
grant codeBase "file:${AC_SERVER_HOME}/oda/-" {
    permission java.security.AllPermission;
};
grant codeBase "file:${AC_SERVER_HOME}/reportengines/-" {
    permission java.security.AllPermission;
};
```

- 6 Using Windows Explorer, navigate to AC_JRE_HOME\lib\security. In a default BIRT iHub installation on Windows, performed using the installer, in which the install folder is C:\Actuate, AC_JRE_HOME represents the following path:

C:\Actuate\BIRTiHubVisualization\modules\JDK64\jre

Create a copy of the java.security file, then open java.security using a text editor.

- 7 Do a find on policy.url. By default, java.security contains two policy.url.*n* properties where *n* is a number, as shown in Listing 4-2.

Listing 4-2 Viewing policy.url.*n* properties in java.security

```
# The default is to have a single system-wide policy file,
# and a policy file in the user's home directory.
policy.url.1=file:${java.home}/lib/security/java.policy
policy.url.2=file:${user.home}/.java.policy
```

Add another policy.url.*n* property, specifying the location of javaserver.policy, as shown in the example in Listing 4-3.

Listing 4-3 Specifying the location of `javaserver.policy` in `java.security`

```
# The default is to have a single system-wide policy file,  
# and a policy file in the user's home directory.  
policy.url.1=file:${java.home}/lib/security/java.policy  
policy.url.2=file:${user.home}/.java.policy  
policy.url.3=file:C:/Actuate/BIRTiHubVisualization/modules  
    /BIRTiHub/iHub/shared/config/javaserver.policy
```

Save and exit `java.security`.

- 8** In System Console—Clusters, edit the cluster. Then, from the Manage Cluster menu, choose Start Cluster to start the cluster.

Index

A

- access control lists
 - creating 45
- access permissions. *See* privileges
- accessing
 - console applications 2
- adding
 - archiving policies 40
 - security roles 45
- Administrator user 11
- Administrator user group 11
- administrators
 - managing Encyclopedia volumes and 2
- Archive Schedule button 43
- archiving
 - folders 40
 - report files 40–43
- Archiving and Purging page (Volume Properties) 38
- archiving policies
 - creating 40
 - inheriting 40
 - setting on Encyclopedia 38
- archiving rules 38
- area charts
 - See also* charts
- autoarchiving 40–43
- axes values
 - See also* charts

B

- bar charts
 - See also* charts
- BIRT iHub. *See* iHub System
- BIRT reports
 - See also* reports
- BIRT repository. *See* Encyclopedia volumes
- browsers. *See* web browsers

C

- canceling jobs 58
- channels

- removing notifications from 39
- character strings. *See* strings
- clusters 48
- Collate property 41
- columns
 - See also* fields
- Configuration Console
 - archiving report files and 40
- configurations
 - printing and 43
 - specifying locale-specific formats and 49
- creating
 - access control lists 45
 - archiving policies 40
 - security roles 45
- customizing
 - date-and-time formats 48
 - printer settings 41

D

- data
 - See also* values
 - retrieving from
 - data sources 2
- data filters. *See* filters
- data points
 - See also* charts
- data repository
 - See also* Encyclopedia volumes
- data rows. *See* rows
- data series
 - See also* charts
- data sources
 - retrieving data from 2
- default archiving policy 38
- default printer 42
- deleting
 - jobs 58
 - notifications 39
- displaying
 - printer information 42
- Do not archive file before deletion setting 38
- Do not automatically delete setting 38

documentation iii
documents
 See also reports
Duplex property 41

E

Encyclopedia volumes
 aging items in 40
 archiving items in 40–43
 printing reports and 41–42
 removing items from 40
 running jobs and 43
 setting properties for 39

F

Factory service 43
fields
 See also columns
File type property 38
file types
 archiving specific 38, 40
files
 archiving 40–43
folders
 archiving 40
formats
 customizing 48
functions
 See also methods

G

graphs. *See* charts

I

iHub
 autoarchiving and 40
 localizing reports and 49
 printing reports and 42
iHub services 43
Information Console
 localizing reports and 48
inheriting
 archiving policies 40
installing system printers 41

J

jobs
 canceling 58
 deleting 58
 printing reports and 42, 43
 running scheduled 43
 running unscheduled 43

L

line charts
 See also charts
locale maps 48
locales
 formatting date and time values for 48

M

Management Console
 localizing reports and 48
 managing users and 11
 setting volume properties and 44
manuals. *See* documentation
methods
 See also functions
Mode property 41

N

notifications
 deleting 39
Number of copies property 41

O

online documentation iii
output
 printing and 43

P

Page size property 41
permissions. *See* privileges
print options 41
printer settings 41
printers
 scheduling jobs and 43
 setting properties for 41
 specifying default 42

- viewing information about 42
- printing
 - report documents 42
- Printing page (Volume Properties) 42
- privileges
 - archiving reports and 40
- properties
 - autoarchive 40
 - Encyclopedia volumes 39
 - printing 41
- Properties page (Job Schedules) 58
- protecting data. *See* security
- Purge failure notices after property 39
- Purge success notices after property 39
- purging notifications 39
- purging rules 38

Q

- queries
 - See also* SQL statements

R

- records. *See* rows
- relational databases
 - See also* databases
- report documents
 - See also* reports
- Report Encyclopedia. *See* Encyclopedia volumes
- report files
 - archiving 40–43
- reporting system. *See* iHub System
- reports
 - printing 42
- repository
 - See also* Encyclopedia volumes
- Resolution property 41
- roles
 - accessing reports and 11
 - assigning to users 45
 - creating 45
- running
 - scheduled jobs 43
 - unscheduled jobs 43

S

- Scale property 41
- scatter charts
 - See also* charts
- scheduled jobs
 - canceling 58
 - running 43
- Schedules page (Job Schedules) 58
- security roles
 - accessing reports and 11
 - assigning to users 45
 - creating 45
- series
 - See also* charts
- servers
 - See also* iHub servers
- SQL statements
 - See also* queries
- summary values
 - See also* aggregate data
- system printers 41

T

- text strings. *See* strings
- types. *See* data types

U

- Uniform Resource Locators. *See* URLs
- UNIX systems
 - printing reports and 43
- updating
 - locale maps 48
- users
 - assigning security roles 45
 - setting printer options for 41

V

- values
 - See also* data
- View service 43
- viewing
 - printer information 42
- Visualization Platform
 - archiving and 40
- volumes. *See* Encyclopedia volumes

W

- web browsers
 - accessing console applications and 2
 - setting volume properties and 45
- Windows systems
 - printing reports and 43

X

- x*-axis values
 - See also* charts

Y

- y*-axis values
 - See also* charts