Actuate One™

One Design
One Server
One User Experience

Managing an Encyclopedia Volume

Document No. 130131-2-530304 January 23, 2013

Content

About Managing an Encyclopedia Volume

Managing an Encyclopedia Volume discusses how to administer a BIRT iHub 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 BIRT iHub system jobs.
- *Chapter 6. Managing channels and notification groups.* This chapter discusses how to manage channels and notification groups.
- *Chapter 7. 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 8. 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
- Length limits for iHub names
- About file types and volume management

About Encyclopedia volume management

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

iHub extracts data from common data sources, such as relational databases and other data sources. iHub 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 iHub 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 iHub generates documents, manages an Encyclopedia volume, and connects to multiple data sources.

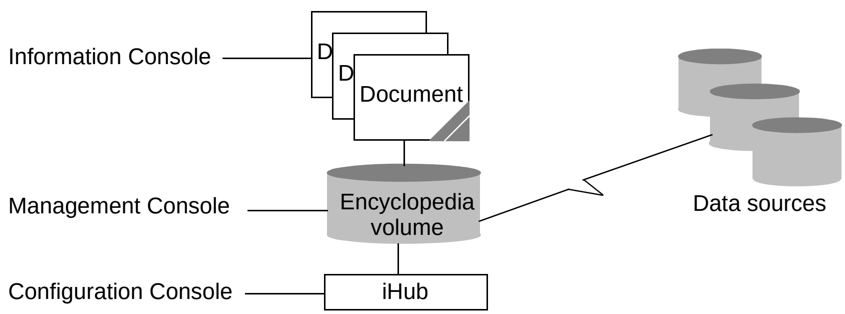


Figure 1-1 iHub reporting environment

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 iHub 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 iHub startup properties

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

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

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

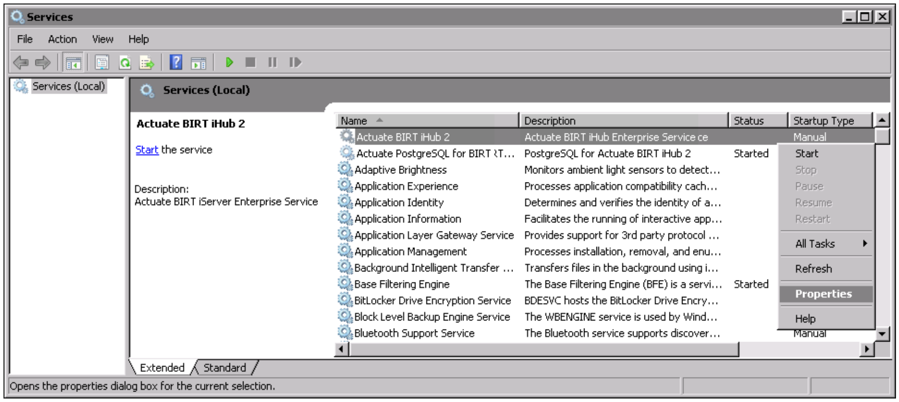


Figure 1-2 Choosing Actuate BIRT iHub service properties

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

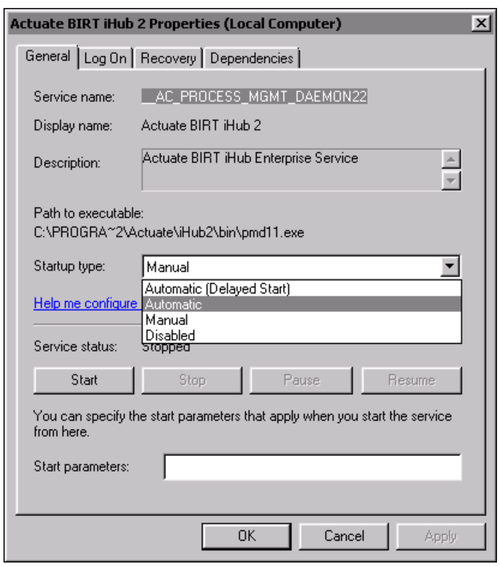


Figure 1-3 Configuring the startup type for Actuate BIRT iHub service

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 iHub service Start, as shown in Figure 1-4.

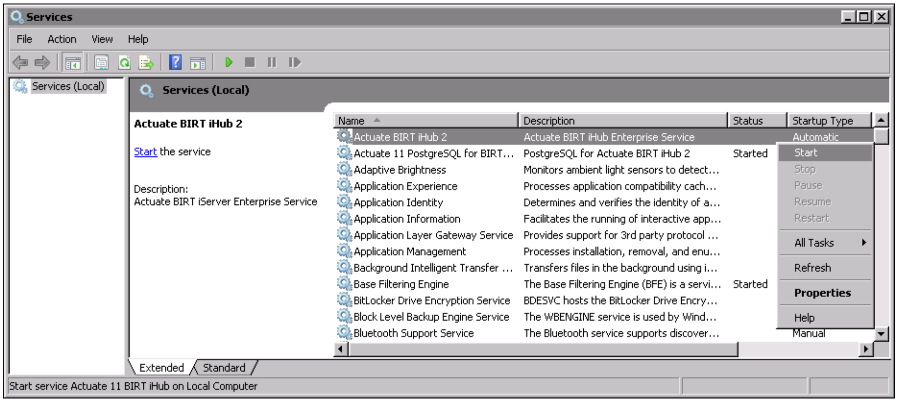


Figure 1-4 Choosing to start iHub service

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

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

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

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

   1 Go to the iHub bin directory. For example:

   ```
   cd /home/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➛BIRT iHub 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.

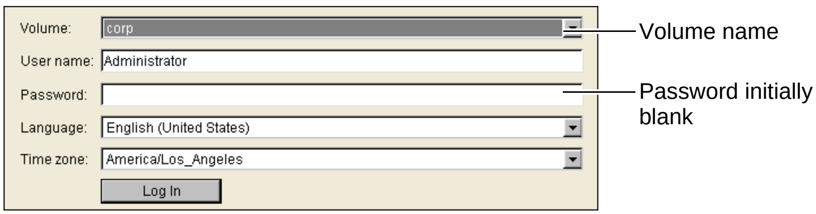


Figure 1-5 Logging in to Management Console

   Choose Log In.

Navigating in Files and Folders

When you log in, Management Console displays the list of files and folders in the administrator's home folder. The list contains Examples, an HTML document giving an overview of the sample design and document files that the default Encyclopedia volume contains.

The path to the current folder appears above Filter. To navigate to another folder, choose a folder in the path. For example, choose the root folder, corp, which is the Encyclopedia volume name, as shown in Figure 1-6.

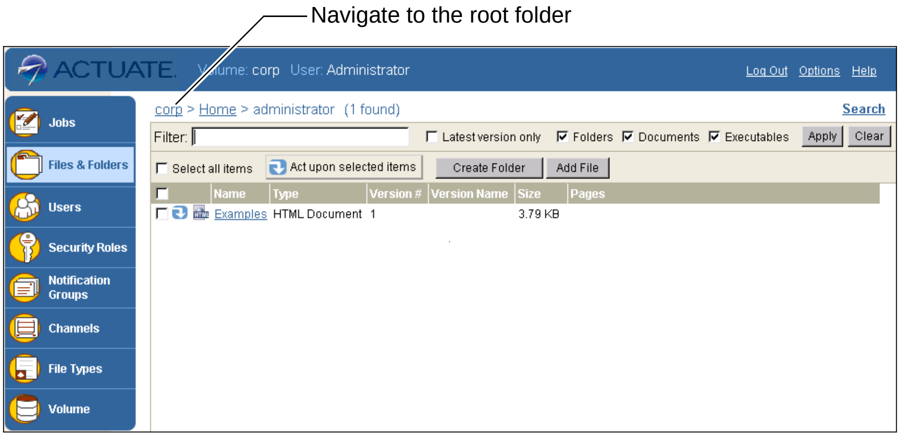


Figure 1-6 Viewing Files and Folders

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.

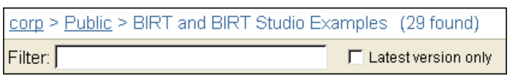


Figure 1-7 Viewing the path to the current folder

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, such as an Actuate BIRT Design (.rptdesign), is an executable file that, when run, generates a document.The files in /Public/BIRT and BIRT Studio Examples include sample .rptdesign files and sample Actuate BIRT document (.rptdocument) files, as shown in Figure 1-8. Executing a .rptdesign file generates a .rptdocument file.

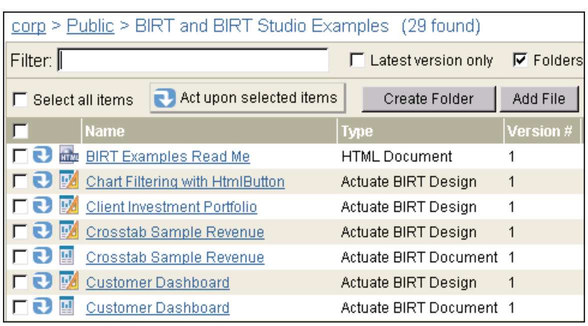


Figure 1-8 Viewing sample .rptdesign and .rptdocument files

Running a design

The following folders in the Management Console root directory 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 and BIRT documents.

  - Information Objects Based Examples

    Contains a readme file, a sample project folder, and a BIRT design.

  - JSAPI Examples

    Contains examples of designs that call the Actuate JSAPI. View the documents these designs create in Information Console.

- 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.

  - Contains an Actuate BIRT Data Object Design (.datadesign) file and an Actuate BIRT Data Object Store (.data) file, both named Classic Models. A scheduled job runs a .datadesign file, generating a .data file. Opening the .data file in Information Console enables you to view and work with the file using Actuate Crosstab Data Analyzer.

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

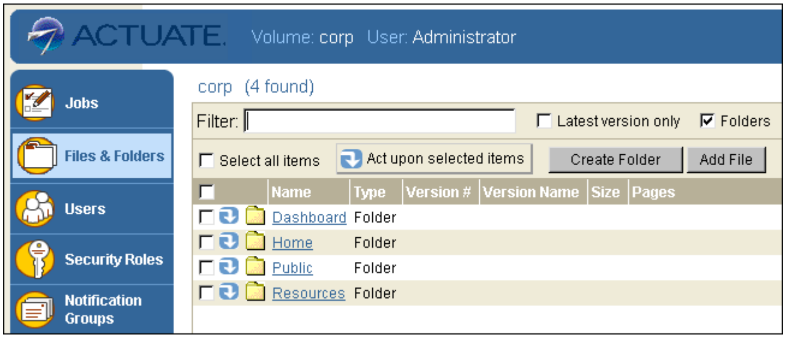


Figure 1-9 Accessing sample designs and design libraries

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 Customer Order History and choose Run, as shown in Figure 1-10.

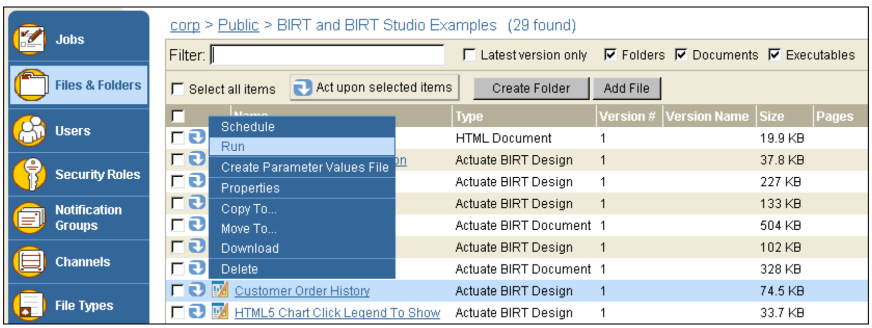


Figure 1-10 Choosing to run Customer Order History

On Run—Parameters, choose the parameter named Classic Gift Ideas, Inc., as shown in Figure 1-11. Choose OK.

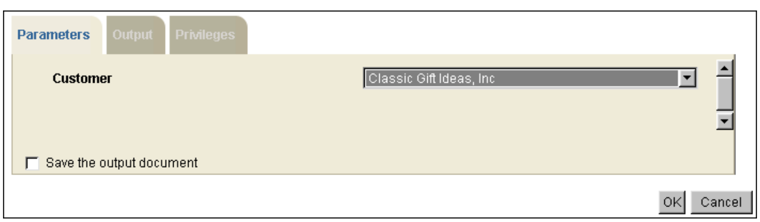


Figure 1-11 Running a design

iHub 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.

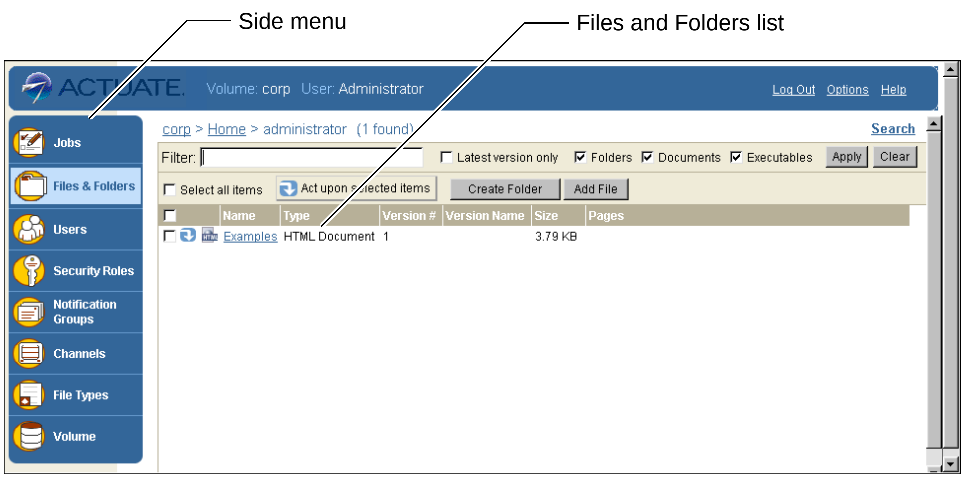


Figure 1-13 Viewing Administrator's list of files and folders

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 iHub System.

- Operator

  A security role. A user with Operator role privileges performs tasks such as scheduling jobs, administering files and folders, performing autoarchive 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.

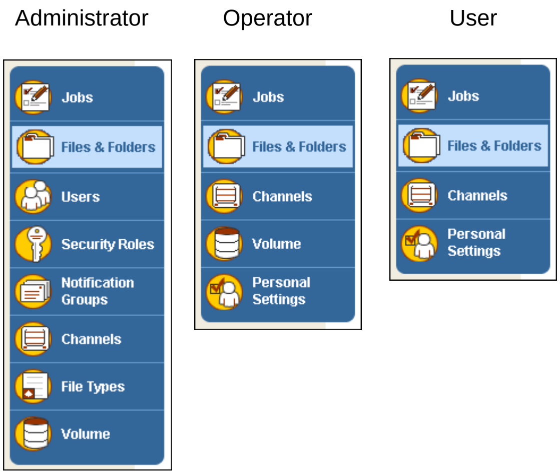


Figure 1-14 Menu options available to different types of users and roles

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		
Volume	Allows the administrator and operator to configure volume properties, and perform autoarchive 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.

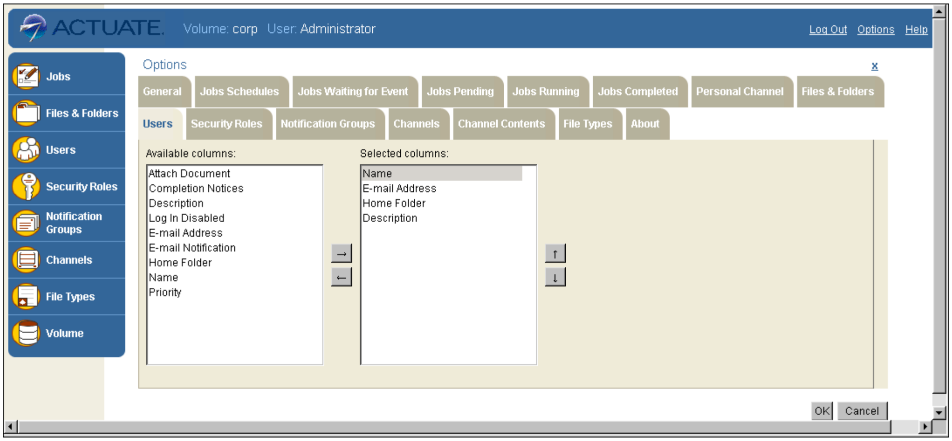
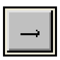


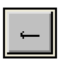
Figure 1-15 Selecting Options—Users

How to modify a tabular list

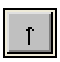
To modify the tabular list for Users, customizing:Management Console perform the following tasks:



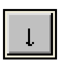
1 To add a column from Available columns, such as Log in Disabled, select the column and choose the right arrow. Log in Disabled appears in the Selected columns list.



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.

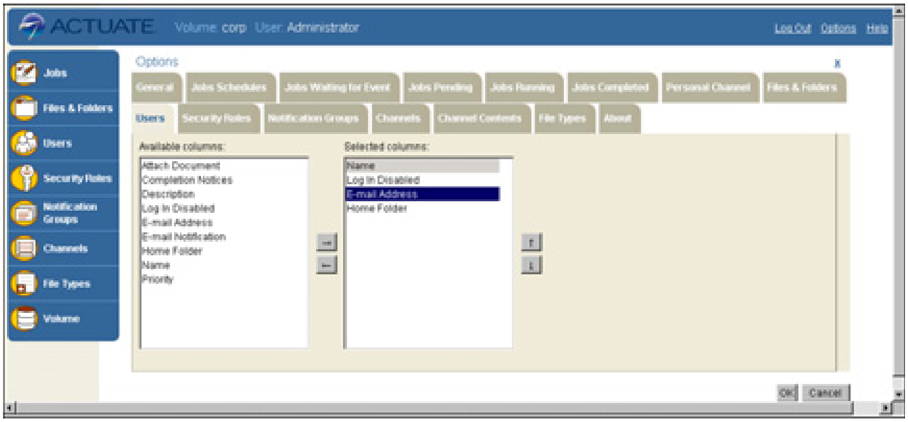


Figure 1-16 Modifying the tabular list in Options—Users

5 Choose OK.

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

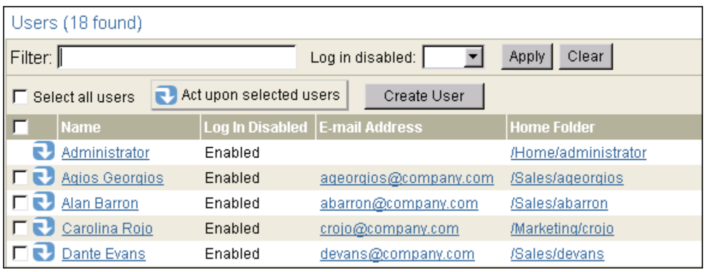


Figure 1-17 Viewing the modified tabular list in Users

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.

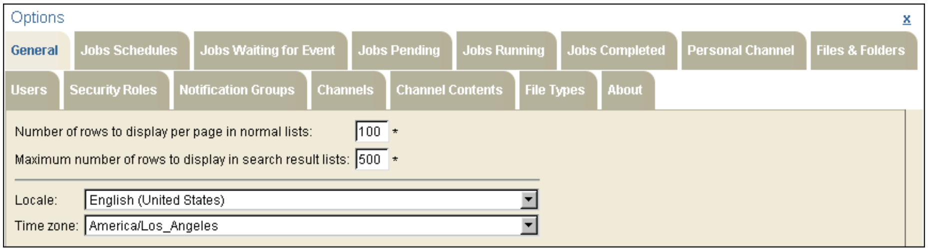


Figure 1-18 Modifying settings in Options—General

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

- Actuate Management Console version
- Actuate BIRT iHub System name
- Volume name
- Actuate BIRT iHub 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.

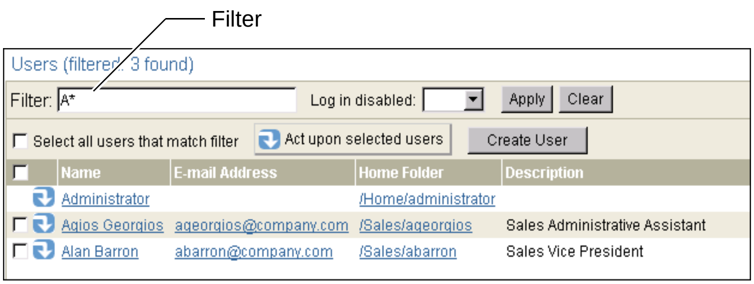


Figure 1-20 Filtering for "A"

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.

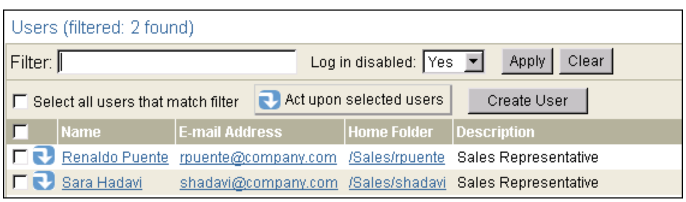


Figure 1-21 Filtering for disabled login accounts

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.

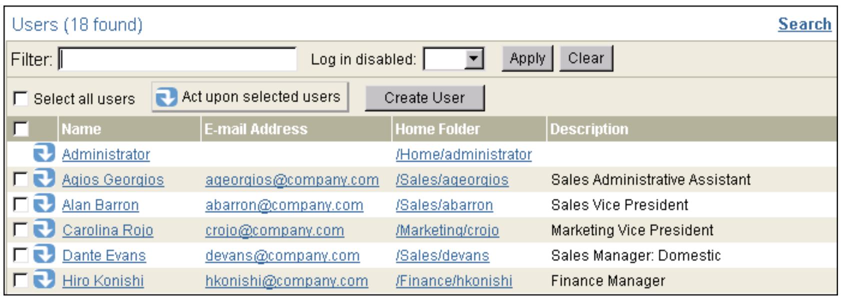


Figure 1-22 Searching for users meeting a specific criteria

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 @company.com.
- Maximum job priority is greater than 500.
- Preference is to receive e-mail notification for all jobs.
- 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
- Completion Notices

- E-mail Notification
- Description

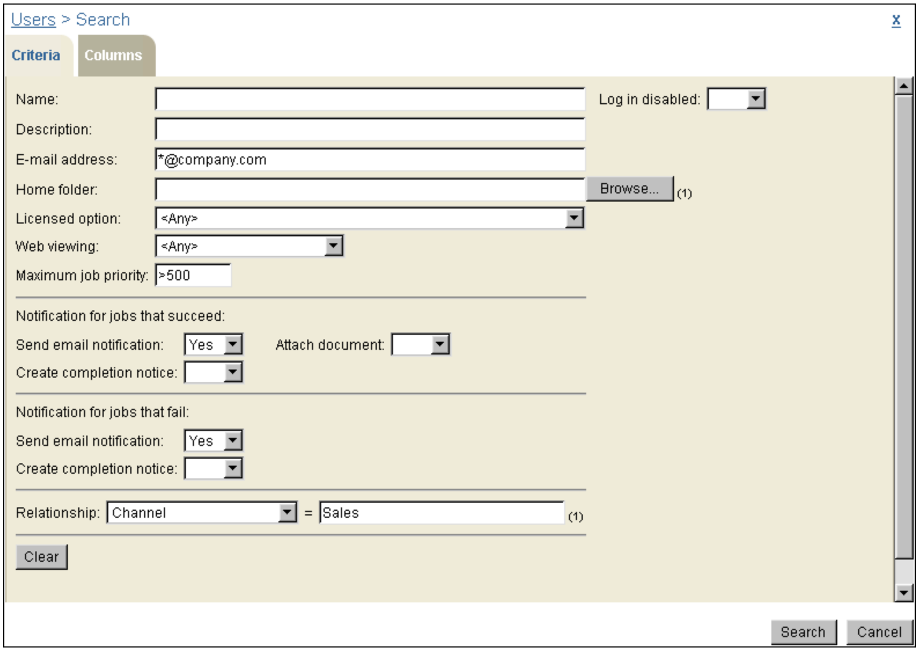
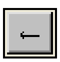
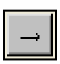


Figure 1-23 Users—Search—Criteria



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

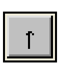
   - E-mail Address
   - Home Folder



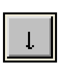
2 Move the following fields from Available columns to Selected columns, using the right arrow:

   - 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 three times to move Priority to the position below Name.



   2 Select Description. Choose the down arrow twice to move Description below E-mail Notification.

Figure 1-24 shows Search—Columns.

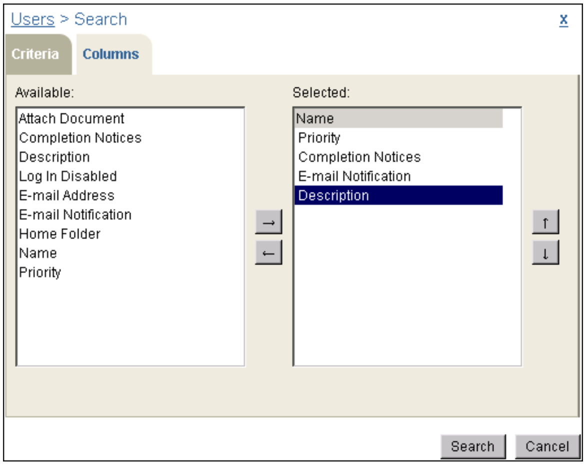


Figure 1-24 Users—Search—Columns

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

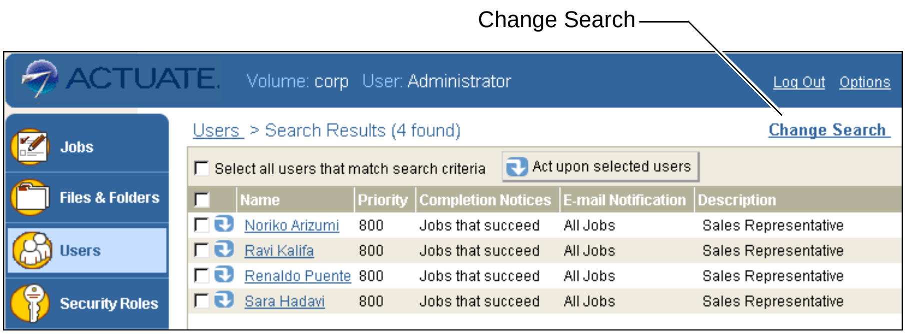


Figure 1-25 Users—Search Results

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

Length limits for iHub names

iHub names, such as file and folder names, must not exceed the character string lengths listed in Table 1-2. These character string length limits apply to the number of Unicode characters. For certain languages, such as Japanese and Thai, the length limit is expressed in terms of the number of code points used to compose Unicode characters. One Japanese character, for example, can comprise up to 4 code points. All code points used count toward the limit. For example, using more than 250 Japanese characters, consisting of 4 code points each, for the name of a file or folder exceeds the 1000 character string limit.

Table 1-2 Length limits of names

Names	Maximum character string length
Channel description	500
Channel icon, large image URL	100
Channel icon, small image URL	100
Channel name	50
Driver path	100
E-mail Address	80
E-mail description	100
File or folder description	500
File or folder version name	100
File type	20
File type description	60
File type short description	40
Group description	500
Group name	50
Headline, notice table	100
Headline, request	100
Input file name	1000
Job description	200
Job name	100
Node name	50
Object name	255
Output file name	1000
Output file version name	100
Partition name	50
Role description	500
Role name	50
User name	50

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 1-26.

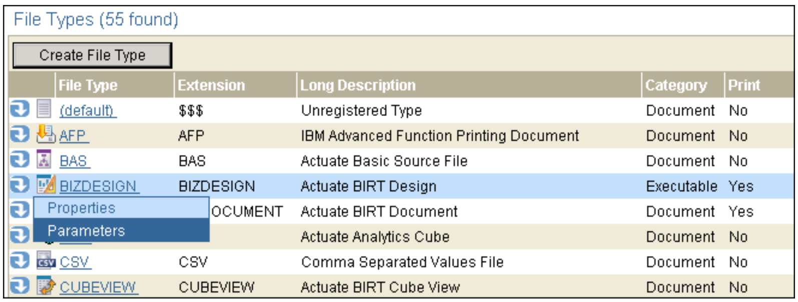


Figure 1-26 Viewing the property values of a file type

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

Chapter

2

Managing users

This chapter contains the following topics:

- About user accounts
- Creating a user account
- Modifying user properties
- Modifying user properties for multiple accounts
- 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.

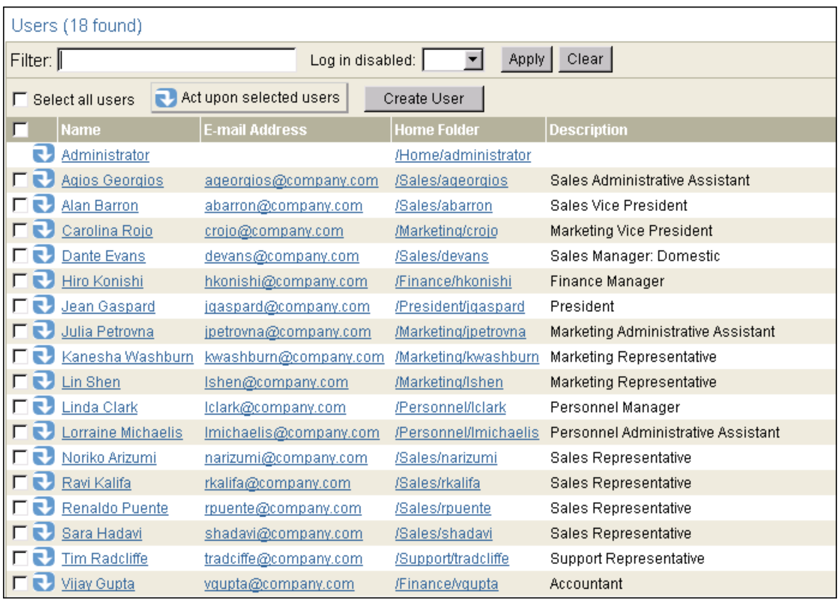


Figure 2-1 Viewing Users

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 option or BIRT Page Level Security option.
- Dashboard
  Default Information Console dashboard settings, such as template and layout.

The administrator can control the priority that iHub gives to running a user's designs. When creating a user account, the administrator specifies the maximum priority that the user can assign to running a design. Settings include:

- Low (200)
- Medium (500)

- High (800)
- Other (1–1000)

Choosing Other opens a text field that accepts a numeric value from 1 through 1000.

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. iHub 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, iHub creates the folder, and any folders in the path that do not exist. iHub 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.

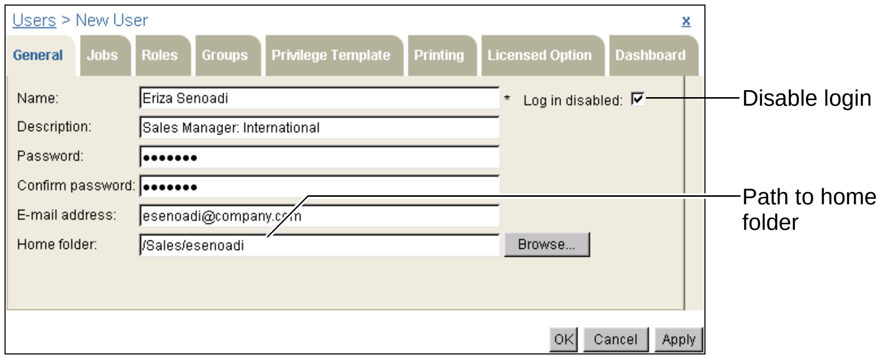


Figure 2-2 Making selections on New User—General

Choose Jobs.

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

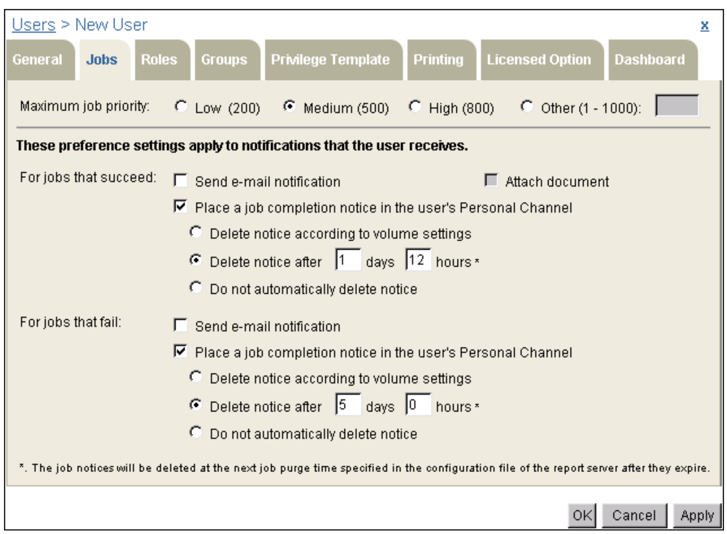


Figure 2-3 Making selections on New User—Jobs

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

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

- Attach document

  iHub 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

  iHub 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

    iHub 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.

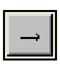
  - Delete notice after n days n hours, where n is a number you specify

    iHub does not delete job notices until after the specified number of days and hours expires.

  - Do not automatically delete notice

    iHub 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 choose the right arrow to move the role to Selected. For example, assign Eriza Senoadi to the Sales Managers role by selecting Sales Managers in Available and moving the role to Selected, as shown in Figure 2-4.

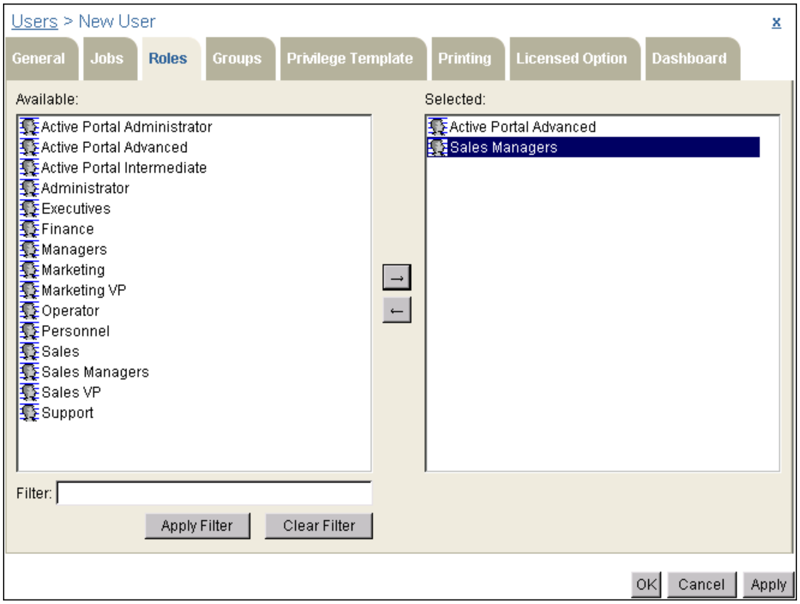
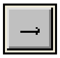


Figure 2-4 Assigning a user to a security role in New User—Roles

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 choose the right arrow to move the group to Selected. For example, to assign Eriza Senoadi to the Sales group, in Available, select Sales and move it to Selected, as shown in Figure 2-5.

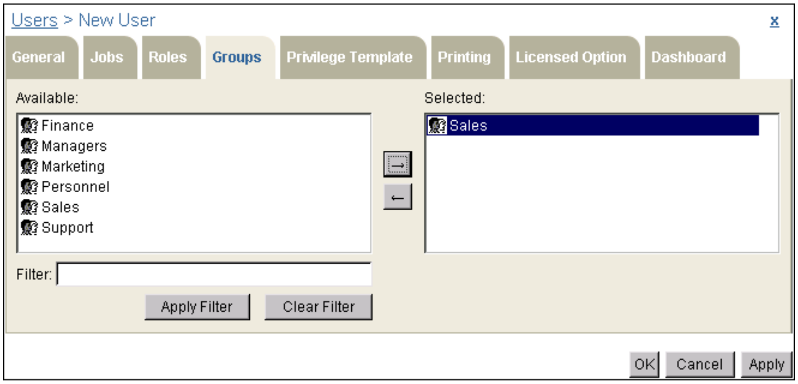
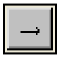


Figure 2-5 Assigning a user to a notification group in New User—Groups

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. Display the list of roles in Available by selecting Roles. Display the list of users by selecting Users.
2. Select one or more security roles from Available and move the role or roles to Selected.
3. Assign privileges by selecting the role or roles in Selected and choosing privileges from the list of privileges below Selected.

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

- Sales
- Sales Managers
- Sales VP

Assign visible and secure read privileges to the Sales role. Assign visible and read privileges to the Sales Managers role. Assign visible, read, and execute privileges to the Sales VP role, as shown in Figure 2-6.

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

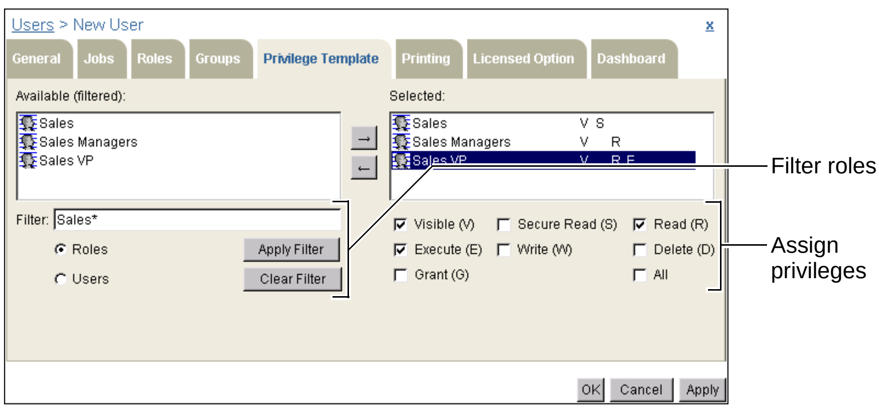


Figure 2-6 Assigning privileges on New User—Privilege Template

Choose Printing.

7 On 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 named Microsoft XPS Document Writer 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
- 1-sided or 2-sided printing
- Page size
- Paper tray

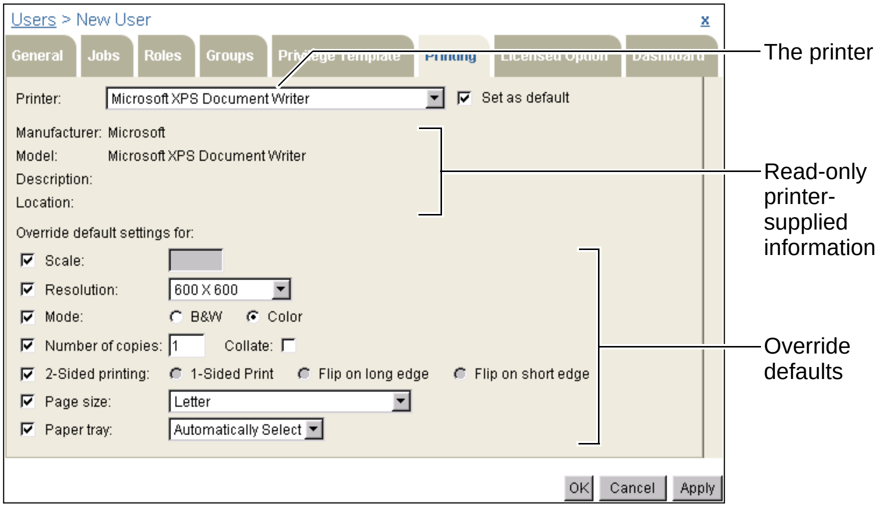


Figure 2-7 Selecting printing options on New User—Printing

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. For example, to support a user executing a BIRT design executable (.rptdesign), assign the BIRT option, as shown in Figure 2-8.
- 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.

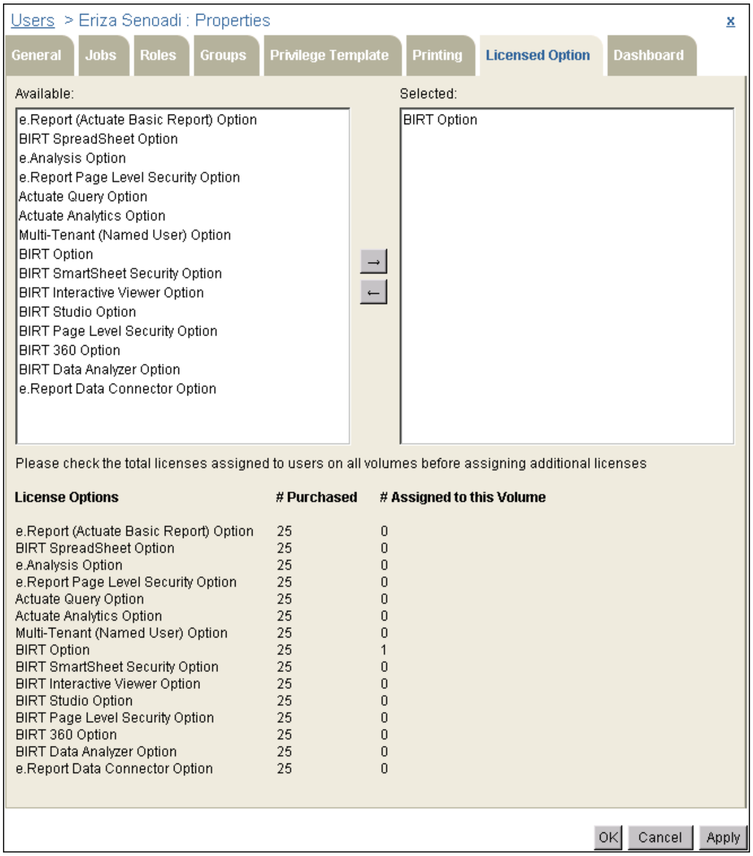


Figure 2-8 Assigning license options on New User—Licensed Option

Choose Dashboard.

9 On Dashboard, specify default Information Console dashboard settings for a user. You can configure the default dashboard template and the default dashboard layout. The default template can be a blank dashboard, the system default dashboard, or you can assign an existing dashboard to the user. You can configure the default layout to show one, two, or three columns. Alternatively, you can select a free form dashboard layout, and specify grid settings for it.

Configuring dashboard settings for a new user supports the user being able to use a dashboard in Information Console immediately, using a pre-determined dashboard configuration.

Figure 2-9 shows the default dashboard settings.

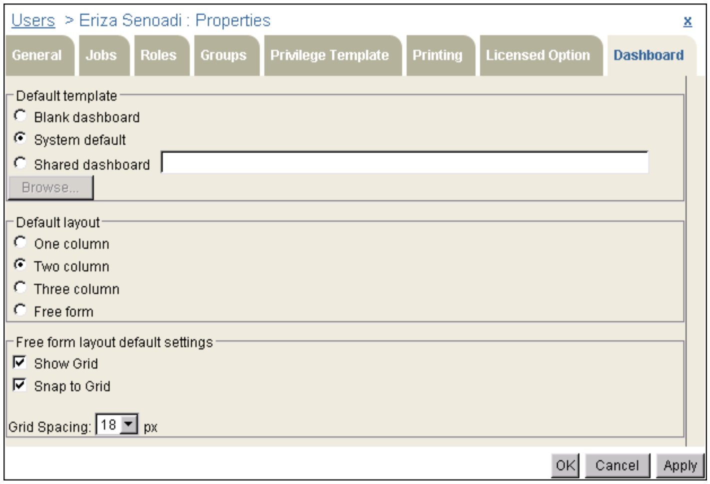


Figure 2-9 Configuring default dashboard property settings

Modifying user properties

The administrator 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 2-10.

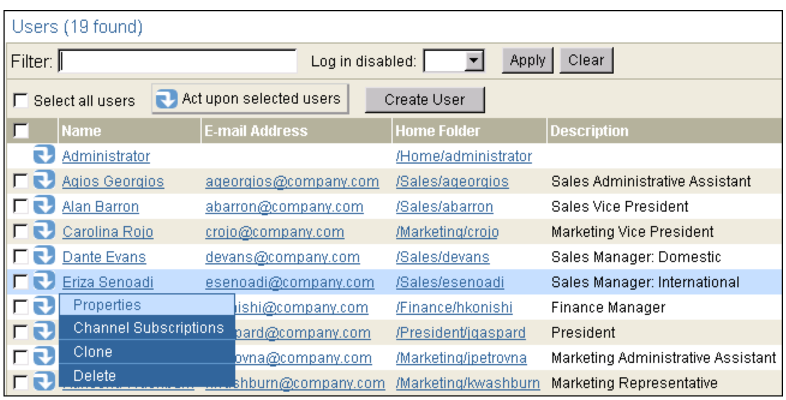


Figure 2-10 Accessing Users—Properties

2 Users—Properties displays the same properties as Users—New User, as shown in Figure 2-11:

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

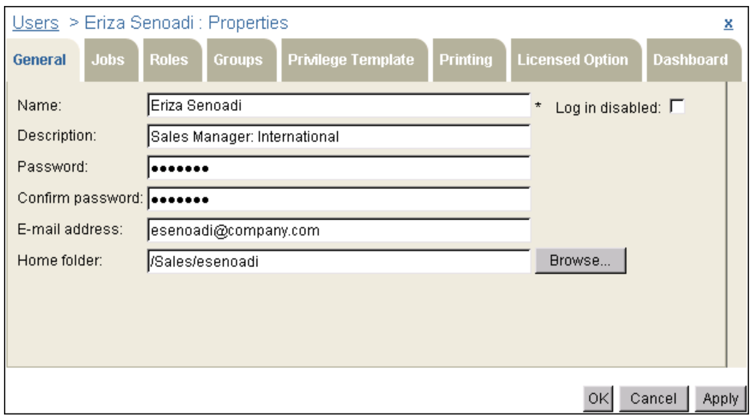


Figure 2-11 Viewing Users—Properties

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, iHub 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 2-12.

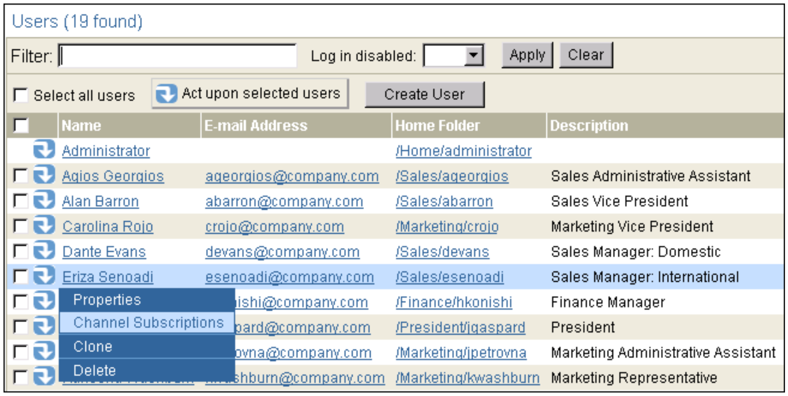


Figure 2-12 Accessing Users—Channel Subscriptions

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 Eriza Senoadi to the Managers channel, select the Managers channel in Available and move it to Selected, as shown in Figure 2-13.

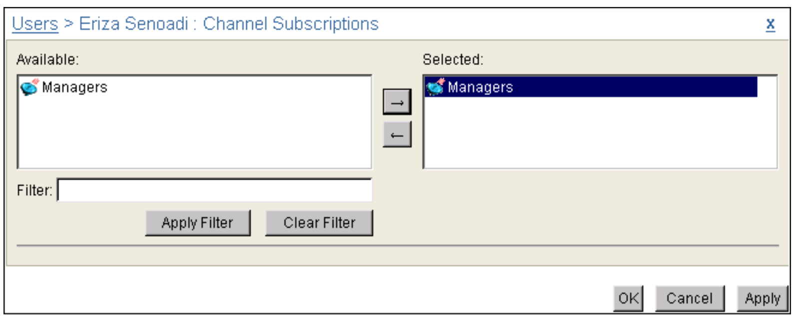


Figure 2-13 Subscribing a user to a channel

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 2-14 shows all management personnel 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 2-14.

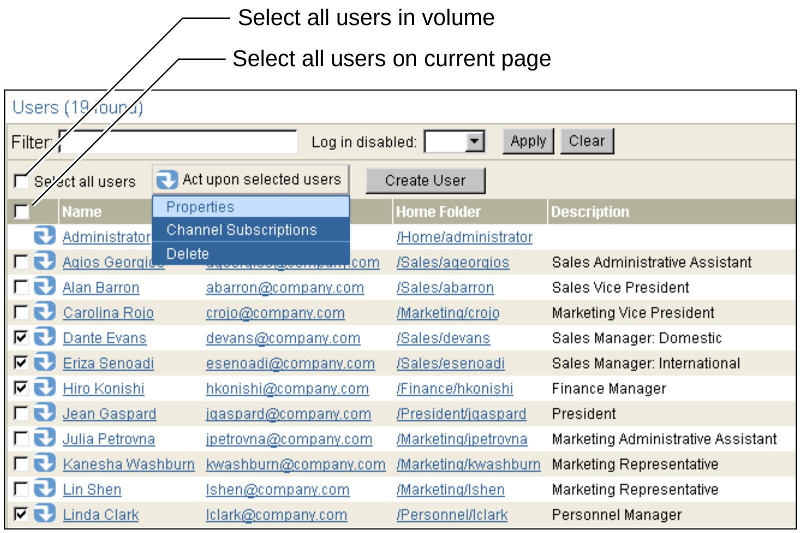


Figure 2-14 Select the properties for multiple users

2 On Users—Properties, make the following changes:

1 On General, enable or disable the user logins and change the description and home folder. Figure 2-15 shows general properties for multiple users.

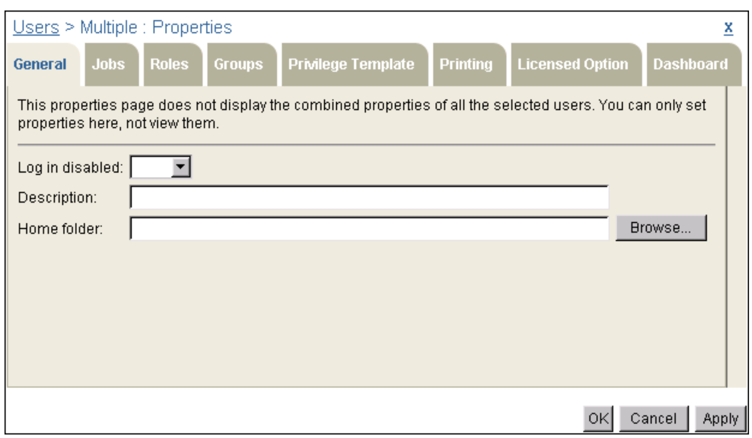


Figure 2-15 Modifying general properties for multiple users

2 On Jobs, set the maximum job priority for the selected users and set notification preferences for jobs that succeed or fail, as shown in Figure 2-16.

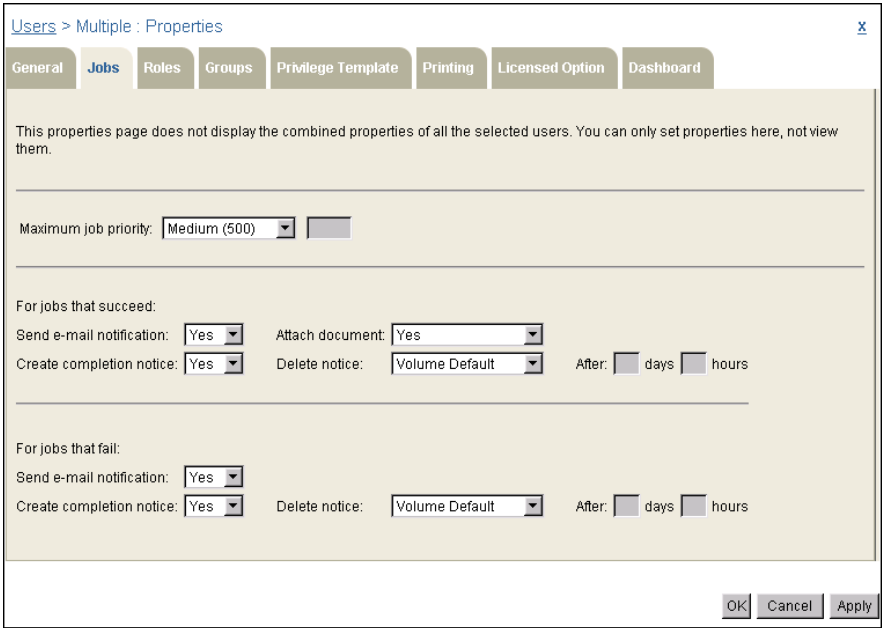


Figure 2-16 Modifying job properties for multiple users

3 On Roles, remove roles from or add roles to selected users by moving the security roles in Available either to Remove these roles or Add these roles. For example, to assign the Managers role to the selected management personnel, move Managers from Available to Add these roles, as shown in Figure 2-17.

To remove all roles from the selected users, except roles you assign in Add these roles, select Remove all.

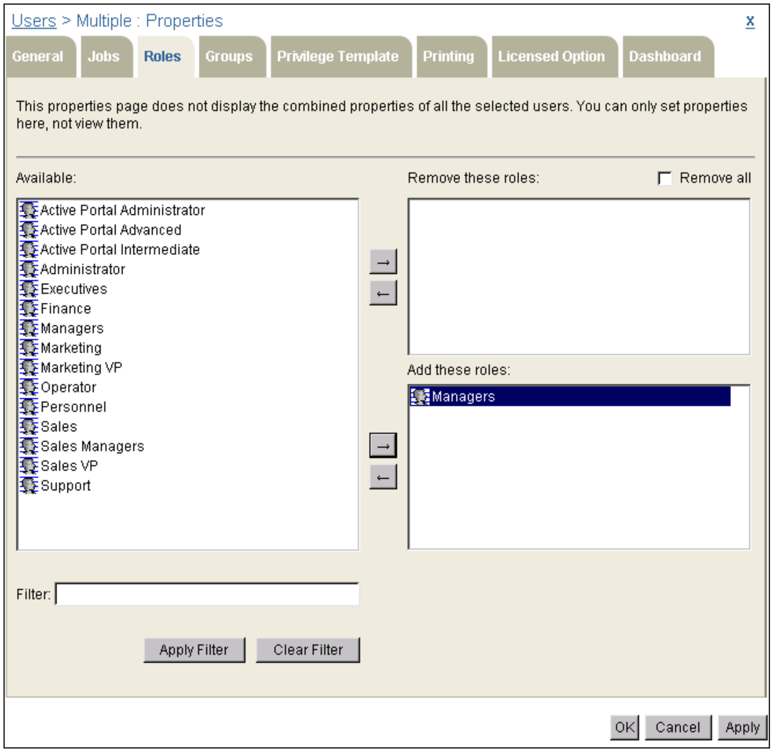


Figure 2-17 Modifying role properties for multiple users

4 On Groups, remove notification groups from or add notification groups to selected users by moving the groups in Available either to Remove these groups or Add these groups. For example, to assign the Managers group to the selected management personnel, move Managers from Available to Add these groups, as shown in Figure 2-18.

To remove all groups from the selected users, except groups you assign in Add these groups, select Remove all.

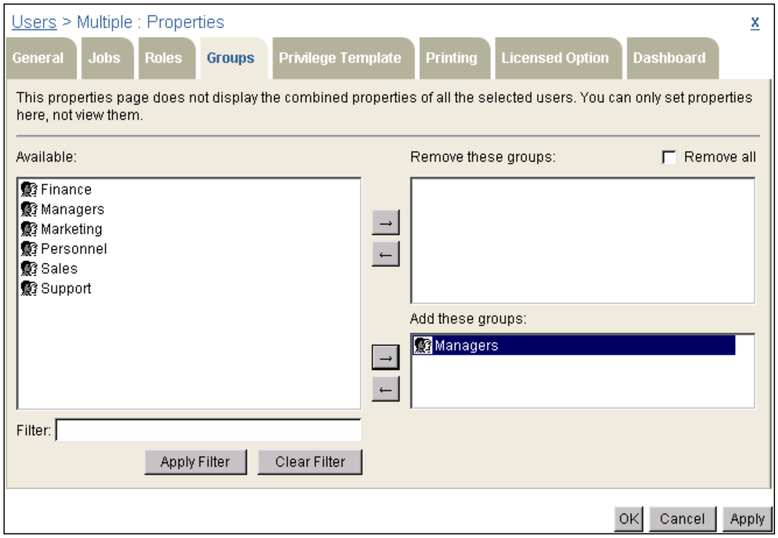


Figure 2-18 Modifying group properties for multiple users

5 On Privilege Template, assign privileges to or remove privileges from other users and security roles on items that the selected users create by performing the following tasks:

1 To display the list of roles in Available, select Roles. To display the list of users, select Users.

2 To remove privileges, move one or more roles or users from Available to Remove these privileges. iHub assigns all privileges to a role or user you move to Remove these privileges. Deselect the privileges that you want the role or user to keep.

3 To add privileges, move one or more roles or users from Available to Add these privileges. With the role or user selected, assign privileges from the list of privileges.

4 To remove all privileges any user or role has on items the selected users create, except privileges you assign in Add these privileges, select Remove all.

For example, assign visible and read privileges to the Executives role on any item a selected manager creates by moving Executives from Available to Add these privileges. With Executives selected, assign privileges from the list of privileges, as shown in Figure 2-19.

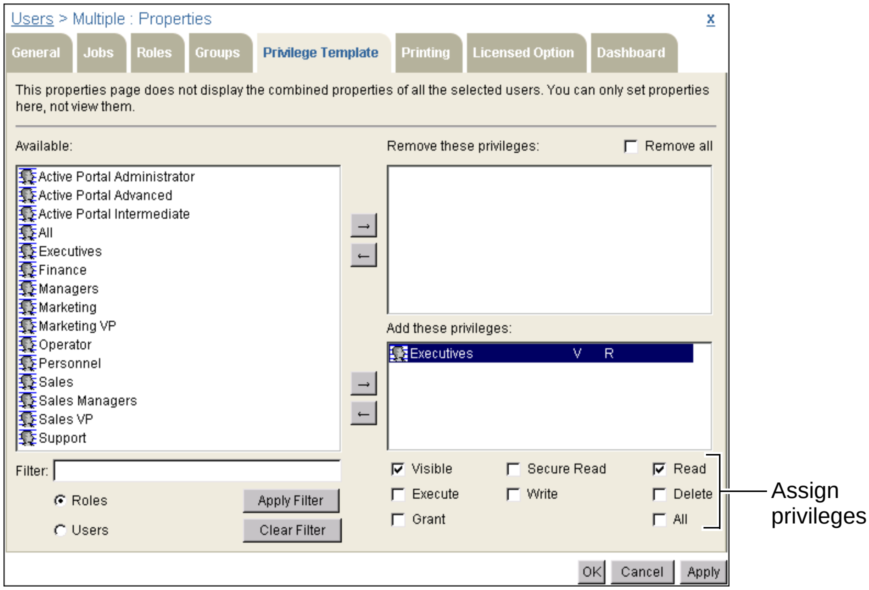


Figure 2-19 Modifying the privilege template properties for multiple users

6 On Printing, specify the printer you send the document to, and choose whether it is the default printer. Use default printer settings, as shown in Figure 2-20, or selectively override individual printer settings.

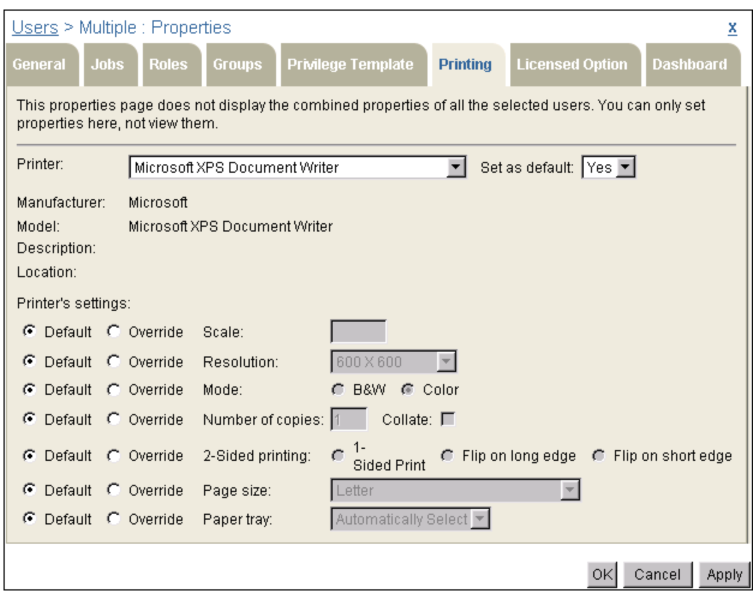


Figure 2-20 Modifying printing properties for multiple users

7 On Licensed Option, shown in Figure 2-21, 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 all licensed options from the selected users except licensed options you assign in Add these licensed options.
- Assign licensed options by moving one or more options from Available to Add these licensed options. For example, assign the BIRT Interactive Viewer option to all management personnel, as shown in Figure 2-21.

License Options lists each licensed option, showing the number of license options purchased as # Purchased and the number of license options assigned to this volume as # Assigned to this Volume.

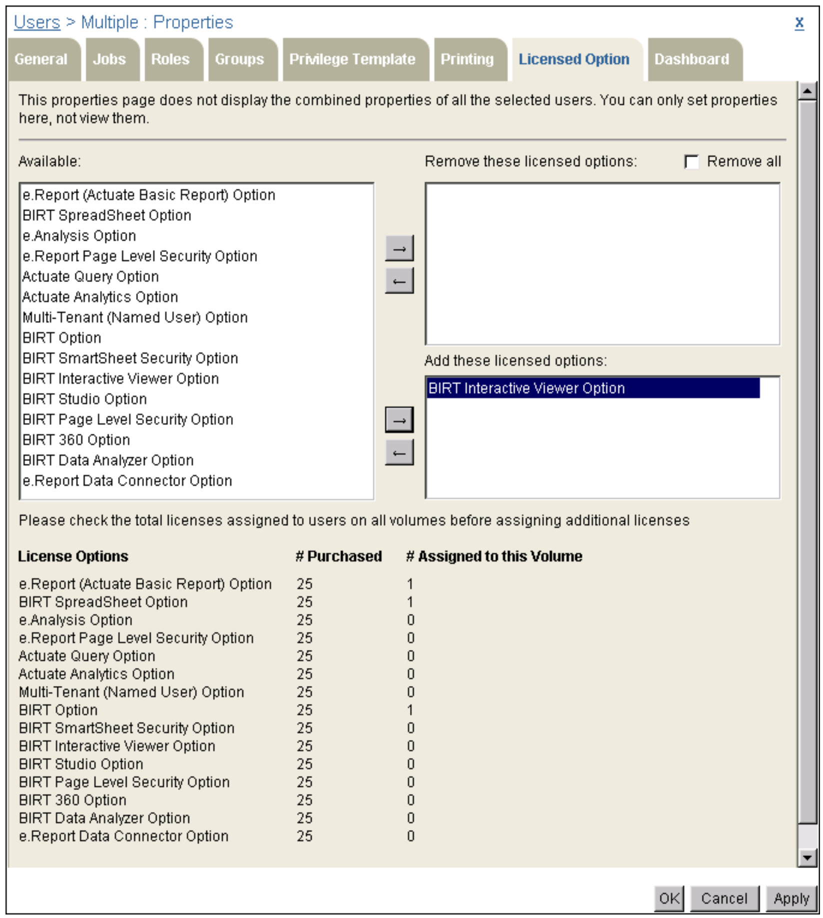


Figure 2-21 Adding and removing licensed options for multiple users

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

8 On Dashboard, shown in Figure 2-22, specify default Information Console dashboard settings for selected users. You can configure the default dashboard template and the default dashboard layout. The default template can be a blank dashboard, the system default dashboard, or you can assign an existing dashboard to the selected users. The default layout can be configured to show one, two, or three columns. Alternatively, you can select a free form dashboard layout, and specify grid settings for it.

A selection you make on Properties—Dashboard overrides the same selection set previously for a selected user.

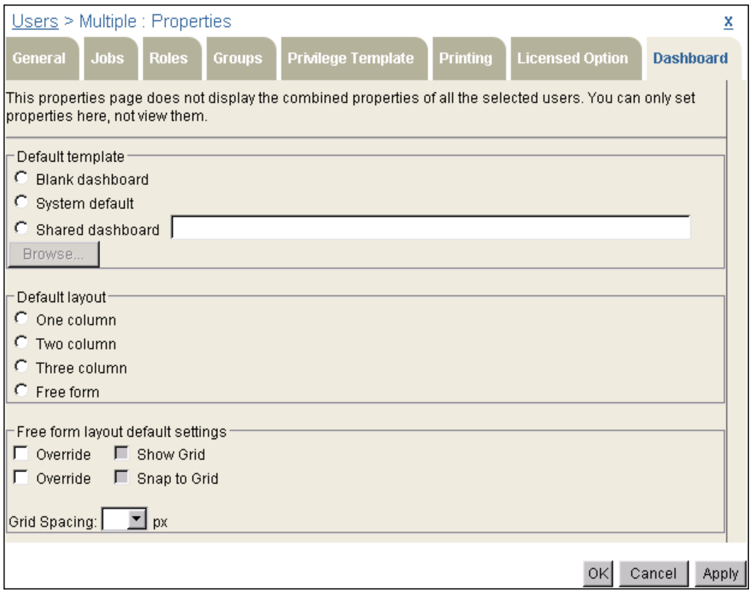


Figure 2-22 Configuring default dashboard property settings

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. For example, after selecting all management personnel on Users, assign the Managers channel to all

management personnel by moving Managers from Available to Selected, as shown in Figure 2-23. To remove all channel subscriptions from the selected users, except subscriptions you assign in Add these subscriptions, select Remove all.

Adding a channel subscription to the selected users requires that each user have read privilege on the channel, either directly or through a security role. If a selected user does not have read privilege on the channel you choose to assign the selected users, Management Console does not assign the channel to the selected user.

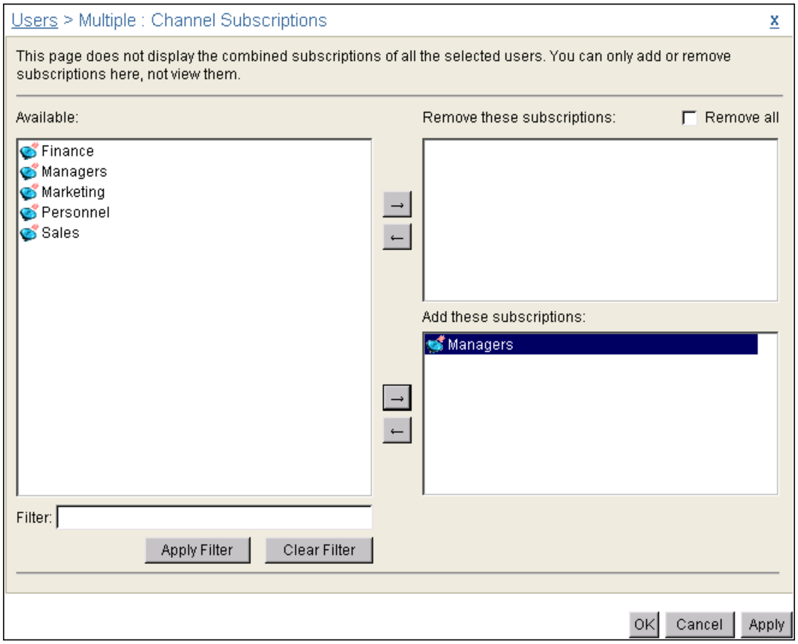


Figure 2-23 Modifying channel subscriptions for multiple users

Choose OK. Management Console returns to Users.

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. For example, to create a new sales manager, clone an existing sales manager. Then, modify the new user properties as needed.

How to clone a user account

1 On Users, point to the arrow next to the user name. Choose Clone, as shown in Figure 2-24.

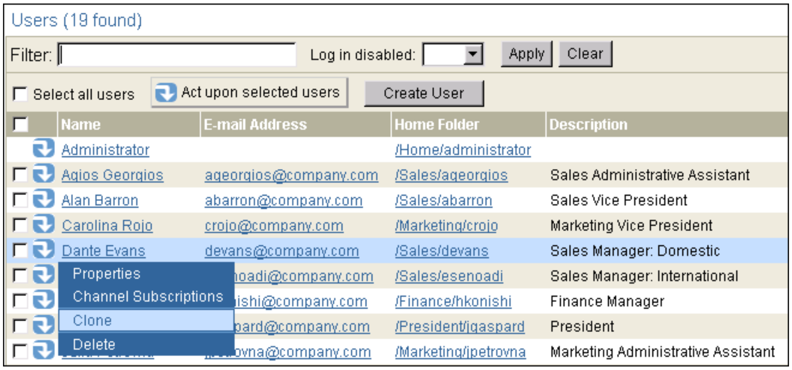


Figure 2-24 Choosing to clone a user

Figure 2-25 shows the properties of the cloned sales manager, Dante Evans, in Users—New User.

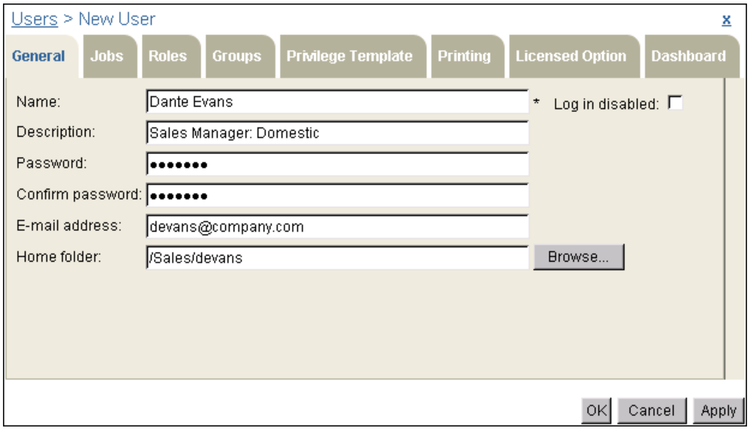


Figure 2-25 Creating a new user account with properties of a cloned user

2 On New User—General, at minimum, change the cloned user's name and password. Change any other properties as needed. For example, to create a new sales manager, Carter Nash, make the necessary new user property changes, as shown in Figure 2-26.

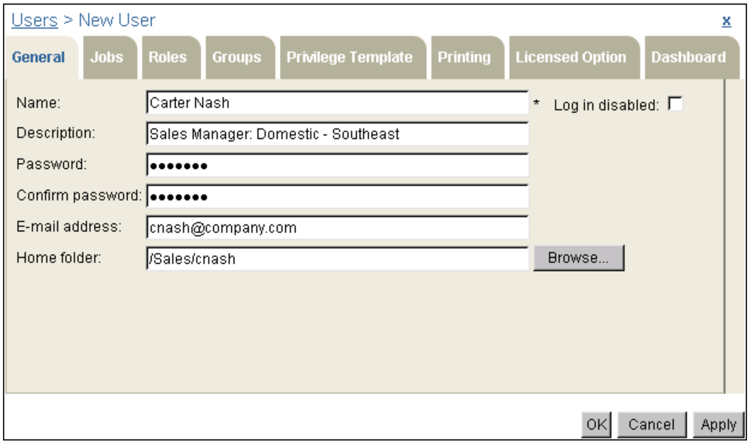


Figure 2-26 Creating a new user from a cloned user

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. iHub 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 2-27.

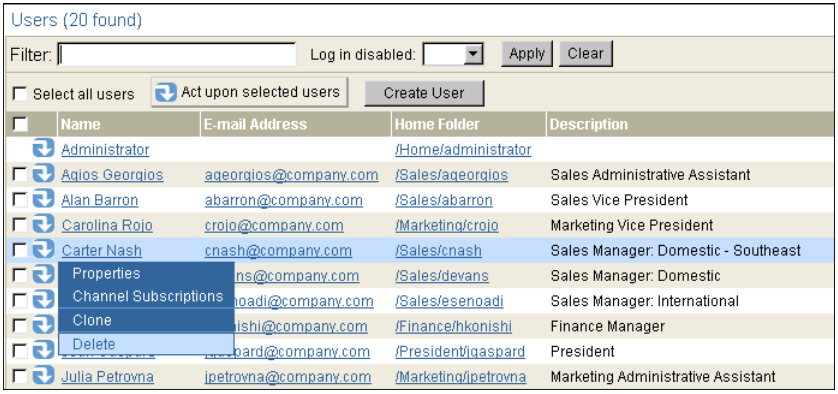


Figure 2-27 Deleting a user account

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 2-28.

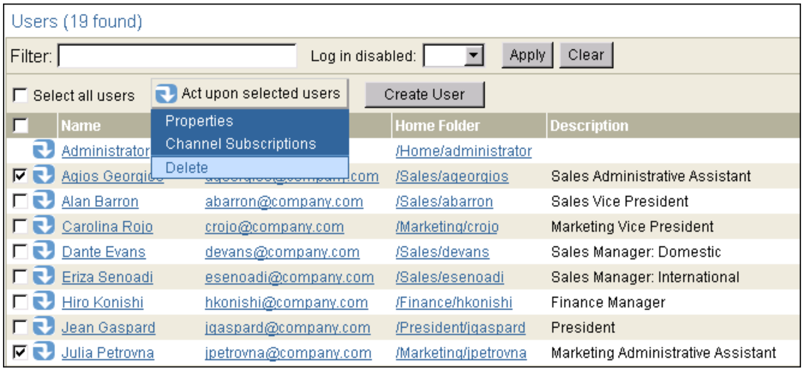


Figure 2-28 Deleting multiple users

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, the Sales Managers role has visible and execute privileges on the Sales Invoice design. Marketing and Finance cannot run the design. Marketing and Finance both can read the document that the Sales Invoice design creates.

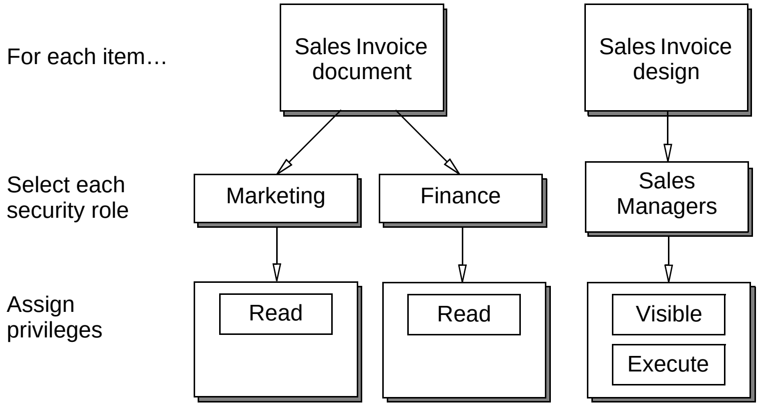


Figure 3-1 Assigning privileges to security roles

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 from a role, the administrator must remove the privilege from every parent role that has the privilege.

iHub 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 Managers, and Sales Managers is the parent role of Sales VP. Sales Managers inherits privileges from Sales. Sales VP inherits privileges from Sales Managers and Sales.

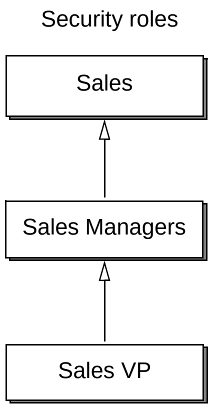


Figure 3-2 Viewing a security roles hierarchy

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

Table 3-1 Privileges assigned to roles on a folder and a file

Security role	/Public/Sales	/Public/Sales/Sales Invoice
Sales	Read	None
Sales Managers	Write	Visible, execute
Sales VP	None	None

As an example, Alan Barron belongs to the Sales VP role. To execute Sales Invoice and write the output to the /Public/Sales/ folder, Alan Barron requires the following privileges:

- Execute and either read, secure read, or visible privilege on Sales Invoice
- Write and either visible, secure read, or read privilege on the /Public/Sales folder

As a member of the Sales VP role, Alan Barron inherits:

- Write privilege on the /Public/Sales folder from the Sales Managers role
- Read privilege on the /Public/Sales folder from the Sales role.
- Visible and execute privileges on Sales Invoice from the Sales Managers role.

Alan Barron inherits all the privileges he needs to execute Sales Invoice and write the output to the /Public/Sales folder.

About system-defined security roles

iHub 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 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. By default, all functionality level features are available to a new user. The Information Console administrator can modify functionality levels and add additional levels by editing the configuration file. The out-of-the-box (OOTB) 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. Management Console assigns this functionality level to a new user by default.
- 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
Set job priority.		X	X
Share and set privileges on a file or folder.		X	X
Subscribe to a channel.	X	X	X
Upload and download files.	X	X	X
Use the interactive viewer, if this option is licensed.	X	X	X

Managing security roles

When creating a new security role or modifying an existing role, the administrator specifies or changes the following properties:

- Security role name and description
- Parent and child roles
- Channel privileges

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 create a security role

The only piece of information that Management Console requires to create a security role is the name of the role. The administrator can optionally configure all the other security role properties after creating the role. To create a security role, perform the following tasks:

1 In Management Console, choose Security Roles from the side menu. Then, choose Create Role, as shown in Figure 3-3.

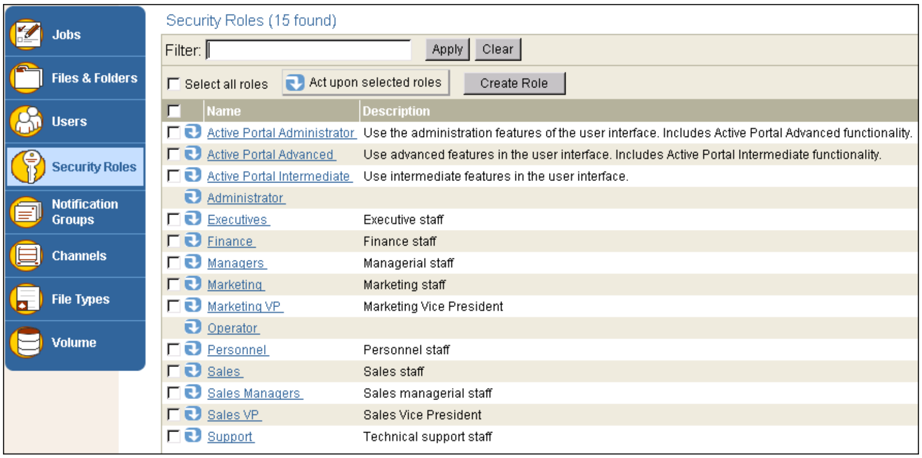


Figure 3-3 Choosing to create a security role

2 In Security Roles—General, type the name of the security role, and optionally, a description, as shown in Figure 3-4.

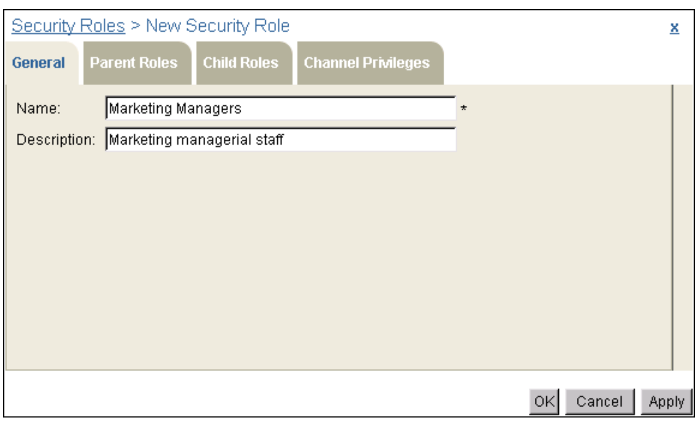


Figure 3-4 Creating a security role

Choose OK.

The new security role appears in the list of security roles, as shown in Figure 3-5.

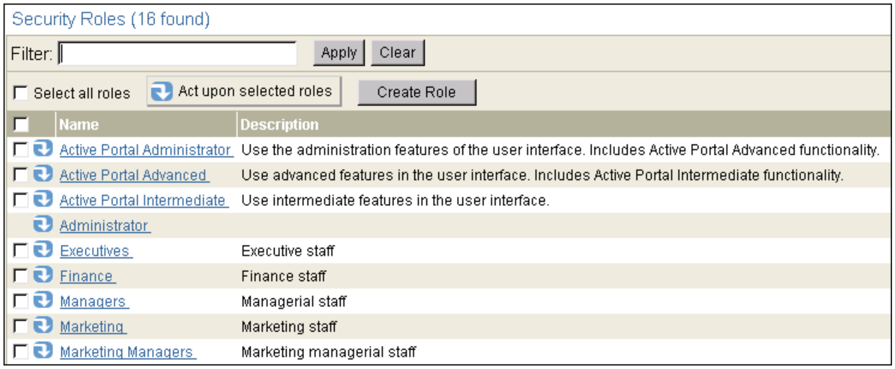


Figure 3-5 Viewing the new security role

How to configure a security role

This section demonstrates how to configure security role properties using the Sales Managers role, an example security role created with only the Name and Description property values defined. The security role properties the administrator configures for an existing role are the same as when creating a new role. To configure a security role, perform the following tasks:

1 Point to the arrow next to the Sales Managers security role, and choose Properties, as shown in Figure 3-6.

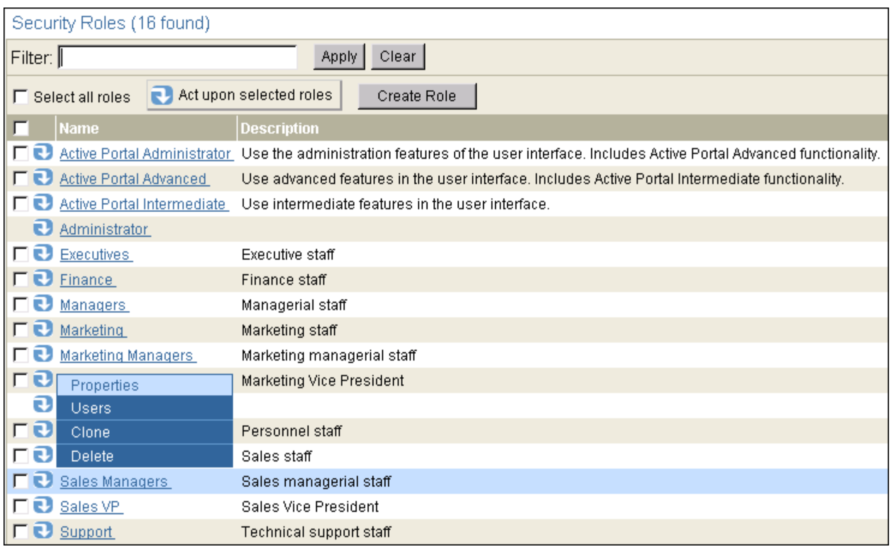


Figure 3-6 Accessing security role properties

Properties—General appears, as shown in Figure 3-7.

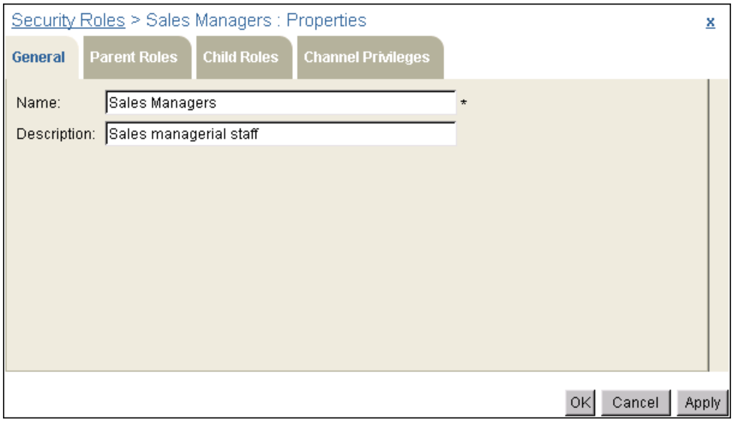
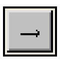


Figure 3-7 Specifying a name and description for a new security role

Choose Parent Roles.



2 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. For example, allow the Sales Managers role to inherit Sales role privileges by moving Sales from Available to Selected, as shown in Figure 3-8.

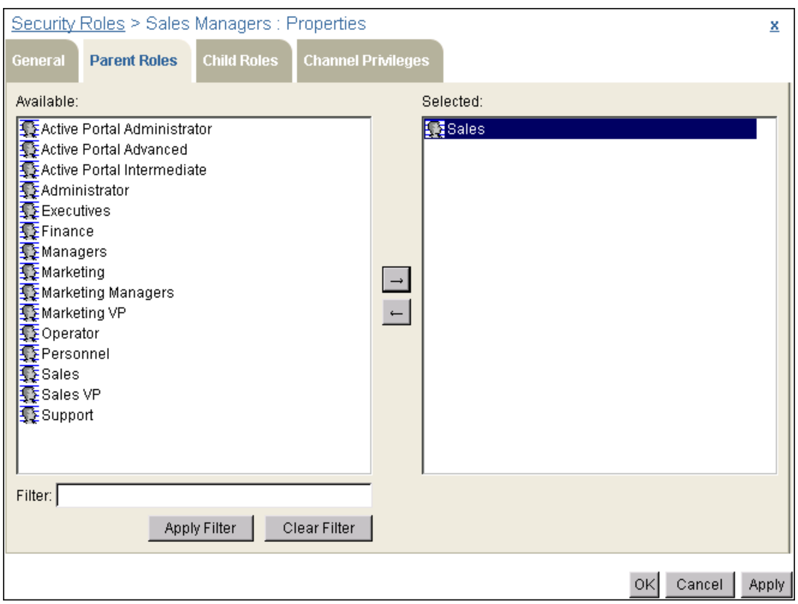


Figure 3-8 Specifying one or more parent roles

Choose Child Roles.

3 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. For example, allow the Sales VP role to inherit Sales Managers role privileges by moving Sales from Available to Selected, as shown in Figure 3-9.

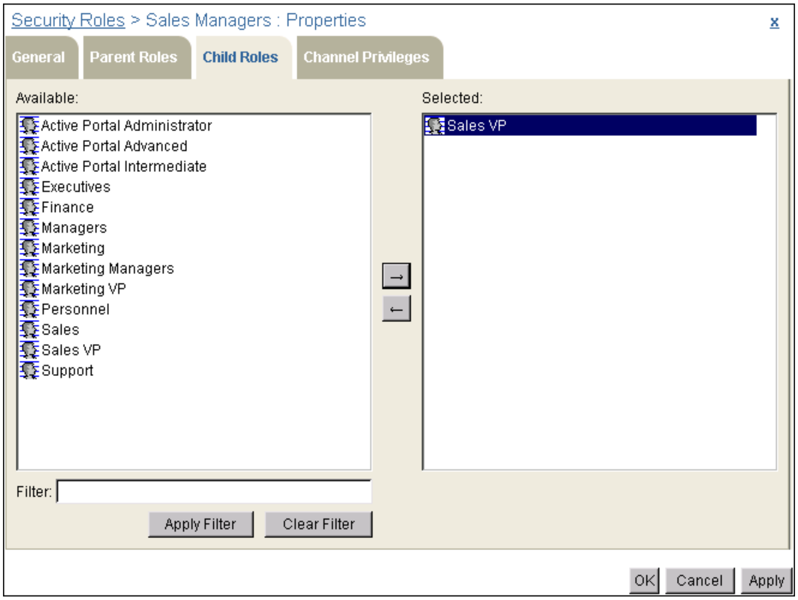


Figure 3-9 Specifying one or more child roles

Choose Channel Privileges.

4 On Channel Privileges, assign channel privileges to this role by moving one or more channels from Available to Selected, and selecting Read, Write, or both privileges for each channel. For example, assign read and write privileges on the Sales channel to the Sales Manager role by moving Sales from Available to Selected, as shown in Figure 3-10.

Alternatively, the administrator can assign channel privileges to a role from Channels after creating the role in Security Roles. Using Figure 3-10 as an example, the administrator could have created the Sales Managers role, then assigned read and write privilege on the Managers channel to the Sales Manager role in Channels—Properties—Privileges instead of in Security Roles—Properties—Channel Privileges.

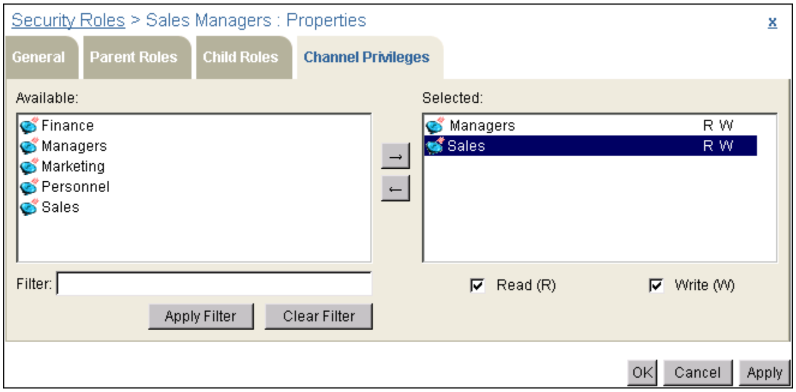


Figure 3-10 Assigning privileges on channels to a security role

Choose OK.

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 3-11.

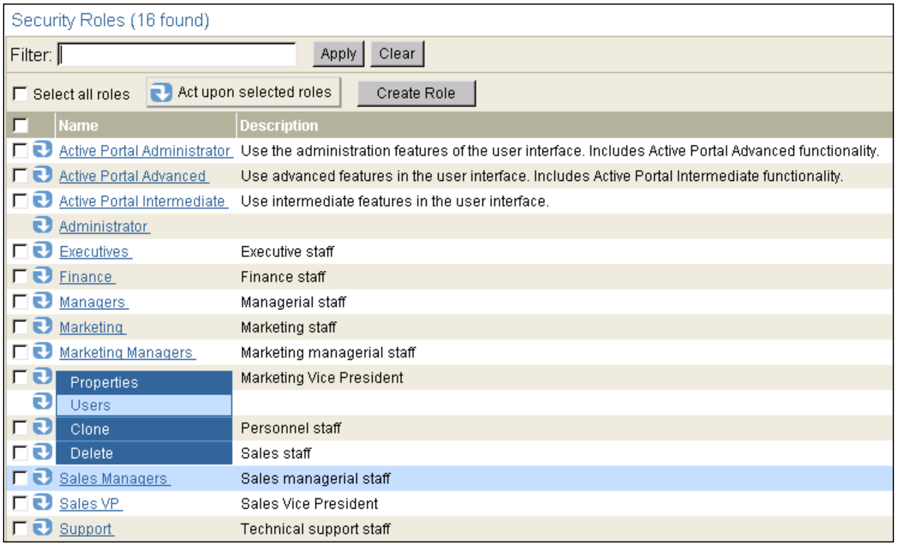


Figure 3-11 Choosing to view a security role membership list

2 On Security Roles—Users, 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. For example, to assign Eriza Senoadi to the Sales Managers security role, move Eriza Senoadi from Available to Add, as shown in Figure 3-12.

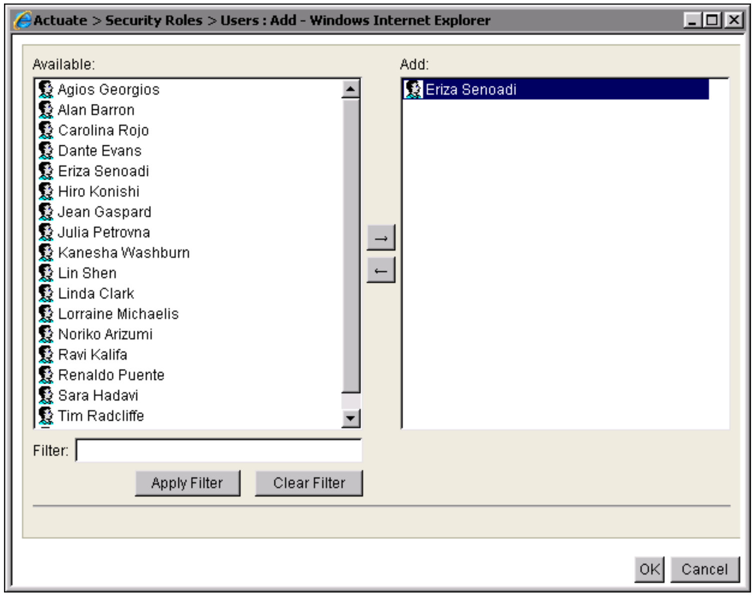


Figure 3-12 Adding a user to a security role

2 Choose OK. Security Roles—Users appears, displaying the list of users assigned to this role, as shown in Figure 3-13.

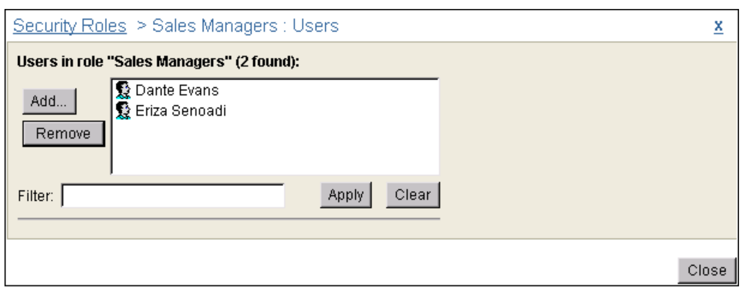


Figure 3-13 Adding and removing security role members

- To remove users:

1 Select the user or users you want to remove.

2 Choose Remove.

3 Confirm the deletion.

Choose Close.

How to clone a security role

The administrator can create a new security role by cloning an existing role. Cloning creates a copy of the role, enabling the administrator 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 3-14.

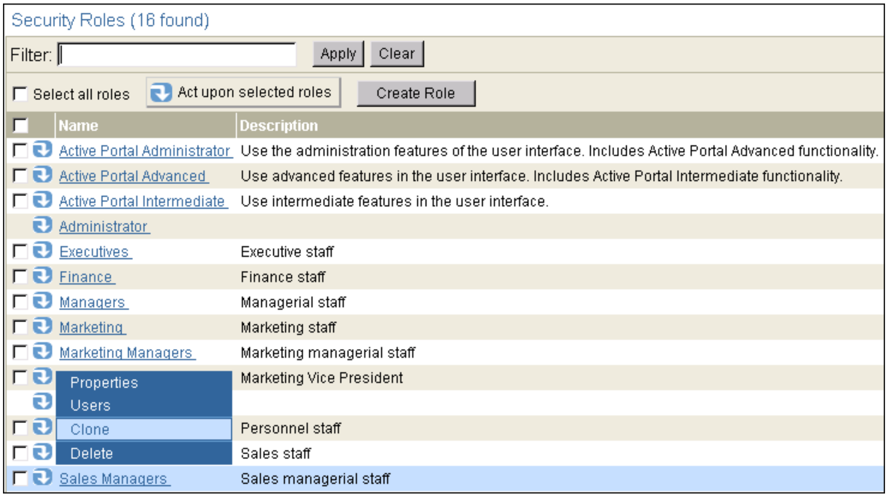


Figure 3-14 Choosing to clone a security role

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 3-15.

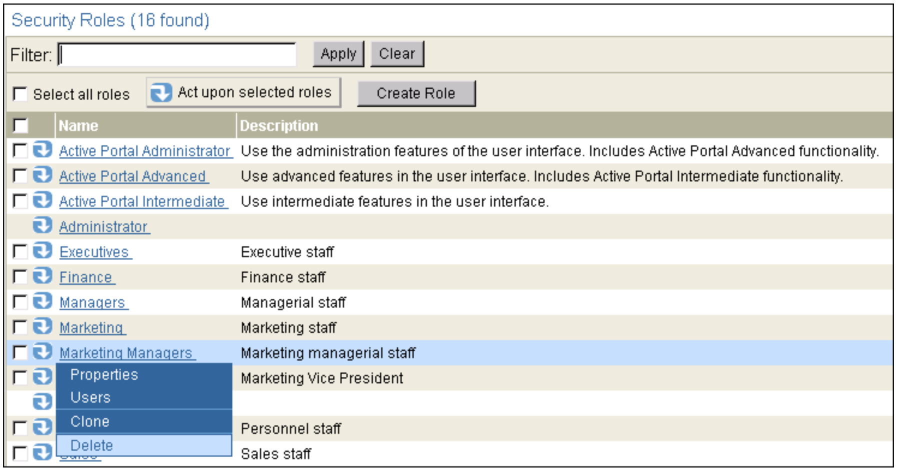


Figure 3-15 Deleting a security role

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 3-16 shows the Marketing VP and the Sales VP roles 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 3-16.

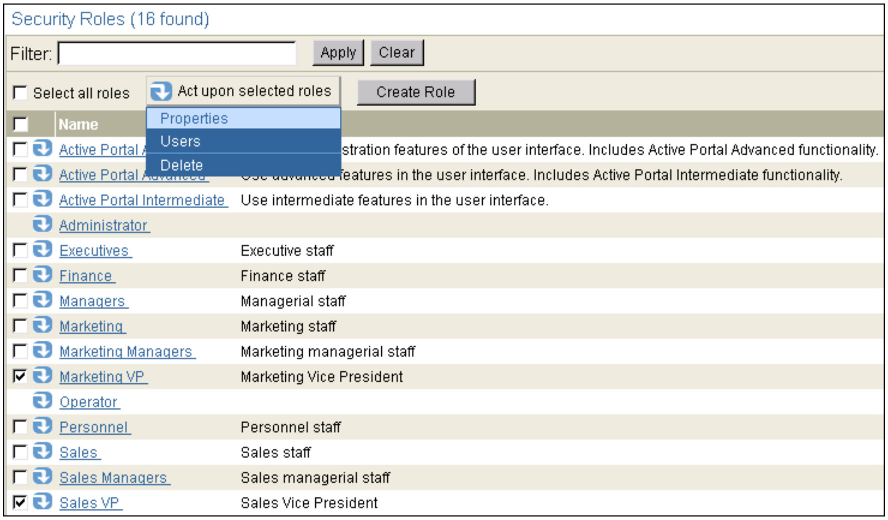


Figure 3-16 Modifying the properties of multiple roles

2 On Security Roles—Properties, perform the following tasks:

1 On General, modify the description field if necessary. Figure 3-17 shows general properties.

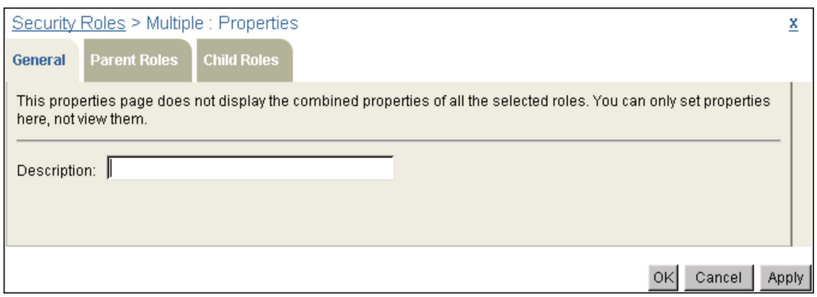


Figure 3-17 Modifying general properties for multiple roles

2 On Parent Roles, select one or more roles from Available, then move the role or roles to Remove these roles or Add these roles. For example, allow the Sales VP and Marketing VP roles to inherit Sales Manager role privileges by moving Sales Manager from Available to Add these roles, as shown in Figure 3-18. To remove all parent roles from the selected roles, except roles you assign in Add these roles, select Remove all.

3 On Child Roles, select one or more roles from Available, then move the role or roles to Remove these roles or Add these roles. For example, allow the Executives role to inherit Sales VP and Marketing VP role privileges by moving Executives from Available to Add these roles, as shown in Figure 3-19.

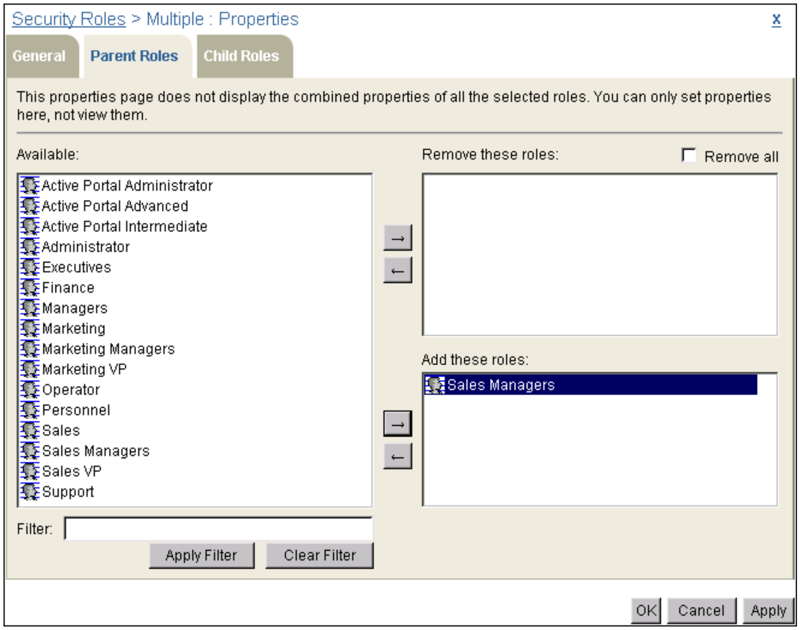


Figure 3-18 Modifying parent role properties for multiple roles

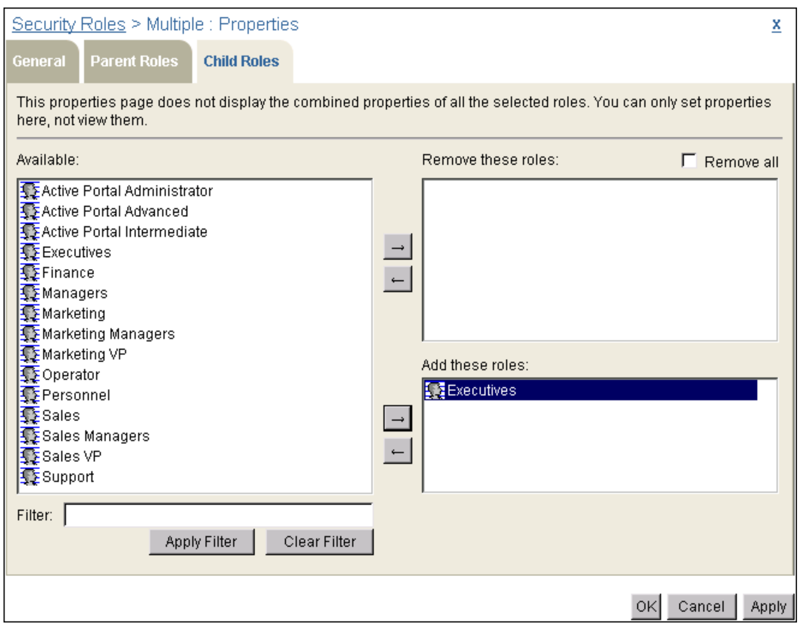


Figure 3-19 Modifying child role properties for multiple roles

To remove all child roles from the selected roles, except roles you assign in Add these roles, select Remove all.

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. Figure 3-20 shows the Executives role and the Finance role selected.

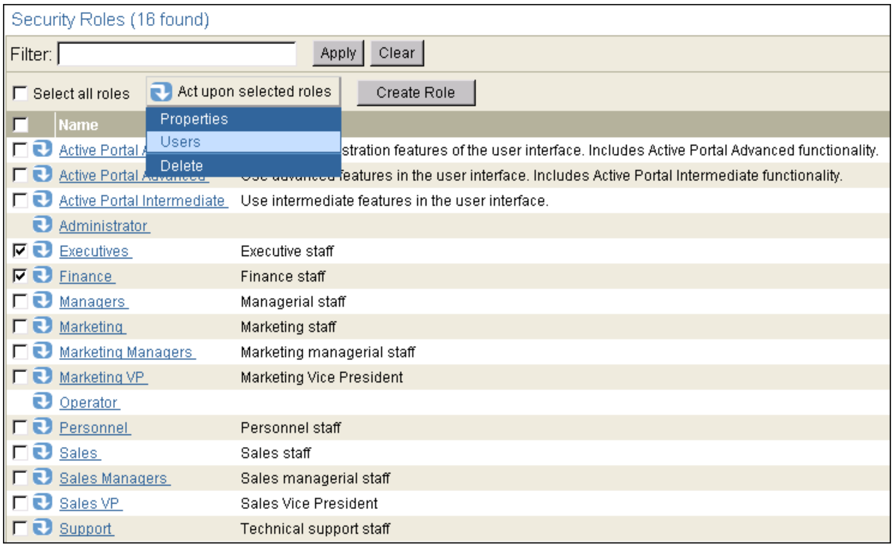


Figure 3-20 Choosing to add and remove users to and from multiple roles

2 On Security Roles—Users, select one or more users from Available, then move the user or users to Remove these users or Add these users. For example, assign the Executives and Finance roles to the company President, Jean Gaspard, by moving Jean Gaspard from Available to Add these roles, as shown in Figure 3-21.

To remove all users from the selected roles, except users you assign in Add these users, select Remove all.

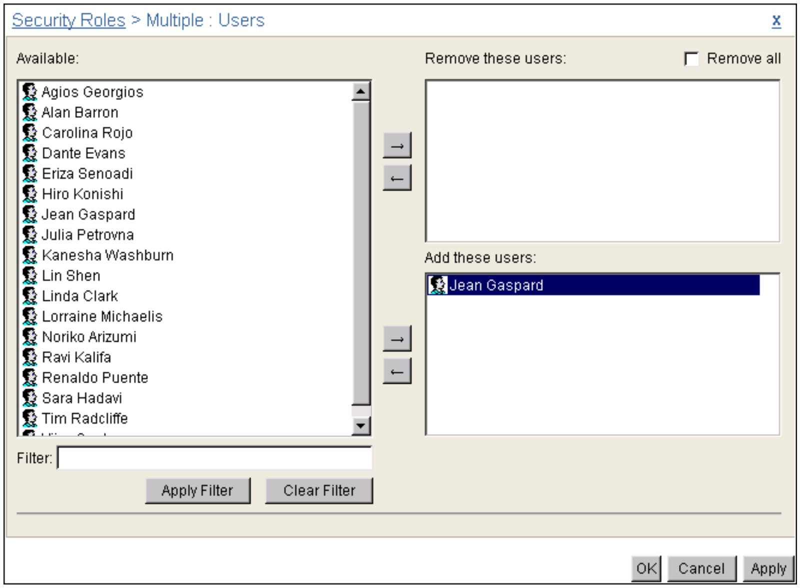


Figure 3-21 Adding and removing users to and from multiple roles

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 3-22.

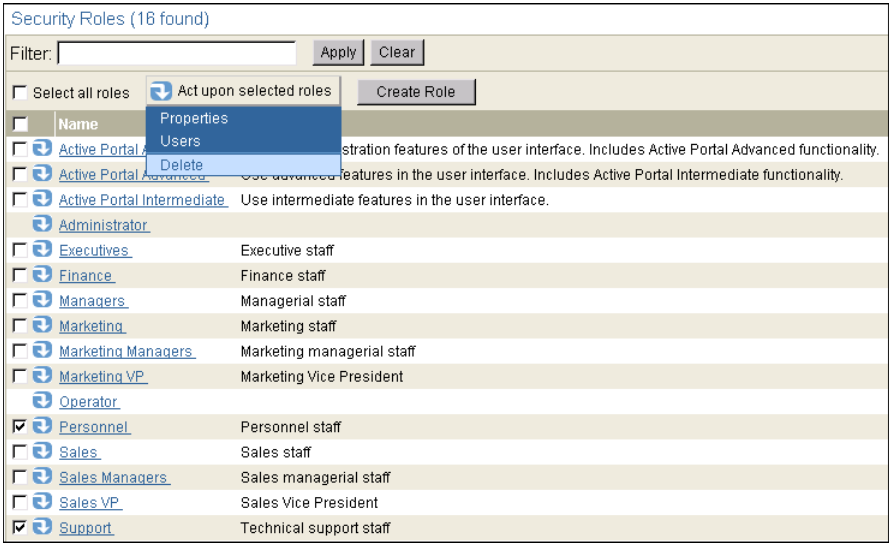


Figure 3-22 Deleting multiple security roles

Confirm the deletion.

Chapter

4

Managing files and folders

This chapter contains the following topics:

- About files and folders
- Understanding file and folder properties
- Adding files and folders to the Encyclopedia volume
- Deleting, copying, moving, and downloading a file or folder

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.

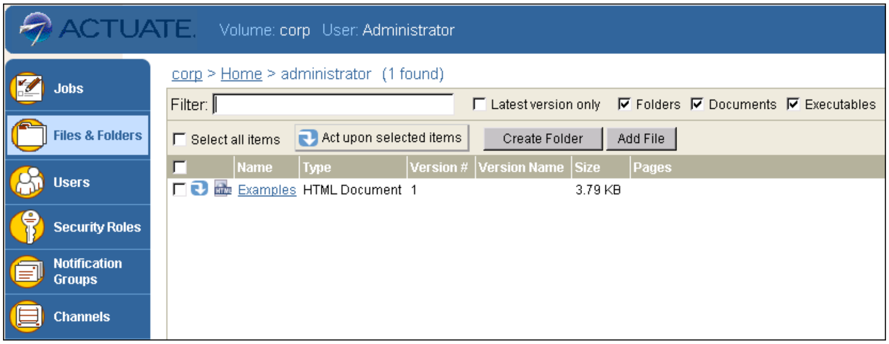


Figure 4-1 Viewing Files and Folders

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.

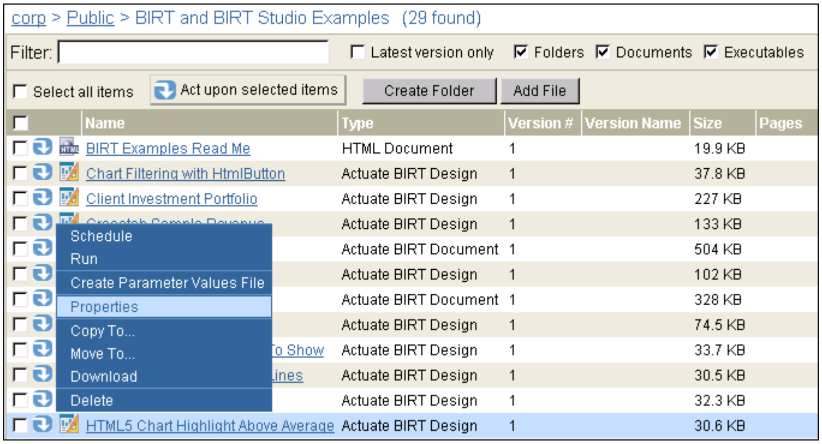


Figure 4-2 Accessing file properties

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 autoarchive 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, HTML5 Chart Highlight Above Average.rptdesign.

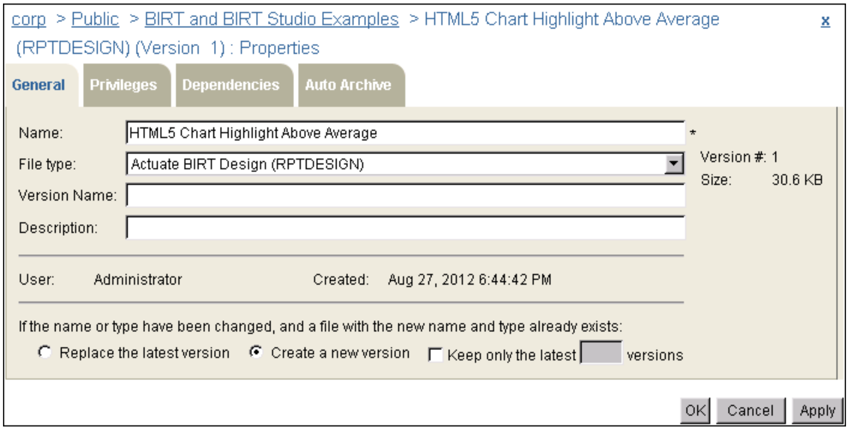


Figure 4-3 Viewing Properties—General for a file

For a folder, Properties—General specifies:

- Name
- Description
- Owner
- Last modified date

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

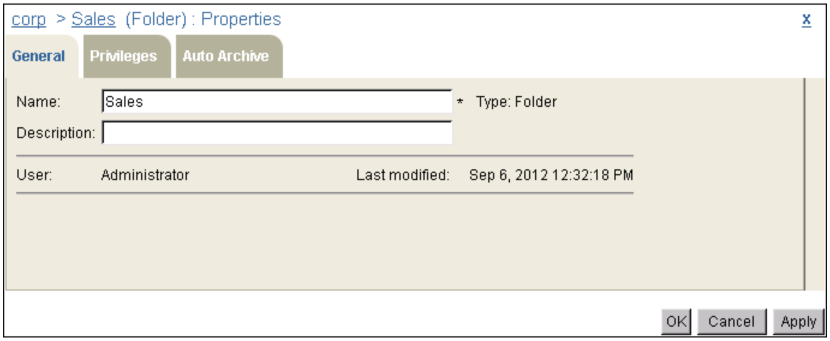


Figure 4-4 Viewing Properties—General for a folder

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.

About folder privileges

The Encyclopedia volume supports the following privileges for a folder:

- Read or visible
  A user can see the folder.
- Write
  A user can create, change, and rename the folder.
- Delete
  A user can delete the folder.
- Grant
  A user can change privileges on the 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 change privileges on the file.
- Read
  A user can open and download the file.
- Execute
  A user can execute a file if the user has both execute and one of the following privileges on the file:
  - Read

  - Secure read
  - Visible

  A user has all privileges on a document the user creates.

- Secure read

  Restricts viewing of a document to DHTML format and prohibits downloading. Typically, the administrator assigns Secure read privilege to a user accessing BIRT documents with the BIRT Page Level Security option.As an example, a design developer creates a design that uses the BIRT Page Level Security option. The administrator assigns a user secure read privilege on the document and the BIRT Page Level Security option. The user's ID determines 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

  A user can see a file in the Files and Folders list, but not open it.

Setting privileges on files and folders

The administrator sets file or folder privileges on Properties—Privileges. Figure 4-5 shows the privileges on the /Sales folder.

If an item has shared access, where an item can be a file or a folder, the owner can assign or remove privileges on the item. A user who is not the owner of an item can assign or remove privileges on the item if it is shared and the user has grant privilege on the item. The administrator can always assign or remove privileges on an item. By default, all items are shared. If the administrator or owner does not want other users to have access to an item, that individual can make the item private by selecting not to share it. Only the owner and Encyclopedia volume administrator can access a file or folder that is not shared.

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.

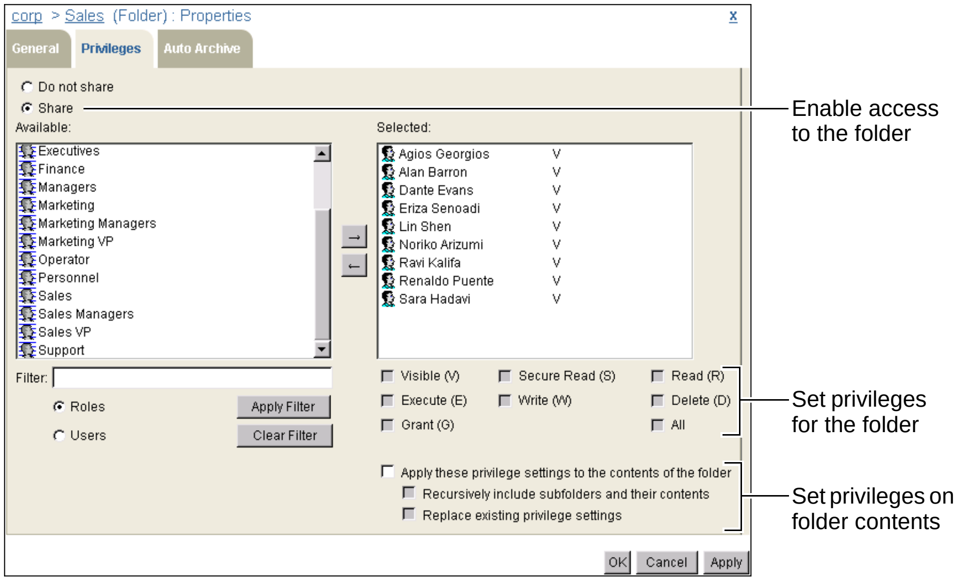


Figure 4-5 Viewing Properties—Privileges for a folder

When setting privileges on a single item or multiple items, the manner in which the administrator sets privileges differs, depending on which of the following single or multiple items the administrator is setting privileges:

- An existing folder
  Add, remove, and replace privileges on the folder and its contents.
- A single file or new folder
  Add and remove privileges on the item.
- Multiple items
  Add and remove privileges on two or more items simultaneously.

How to set privileges on an existing folder

1 On Files and Folders, point to the arrow next to a folder and choose Properties, as shown in Figure 4-6.

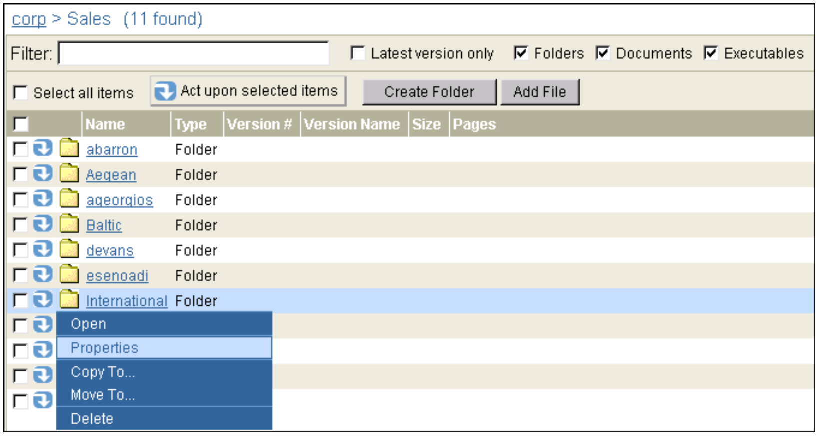


Figure 4-6 Choosing an existing folder

On Properties, choose Privileges.

2 On Privileges, perform the following tasks:

1. Specify whether the folder is shared or private. By default, files and folders are shared. To make the folder private, select Do not share.
2. To assign privileges to one or more users:
    1. Select Users to display the user list in Available.
    2. Select one or more users in Available and move the user or users to Selected.
    3. With the user or users selected, select privileges from the list of privileges below Selected.

To assign privileges to one or more roles, select Roles to display the roles list in Available. Then assign privileges similarly to the way you assign privileges to one or more users.

3. 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. Management Console retains any previously assigned privileges.
    - 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. Management Console retains any previously assigned privileges.

- To replace the existing privilege settings on the folder and contents and specify new privileges, select Replace existing privilege settings.

For example, as shown in Figure 4-7, assign read and write privileges on the /Sales/International folder to Eriza Senoadi. Then, assign read privilege on the folder to the Sales security role. These privileges also apply to the subfolders and files at all levels below /Sales/International and replace any previously assigned privileges.

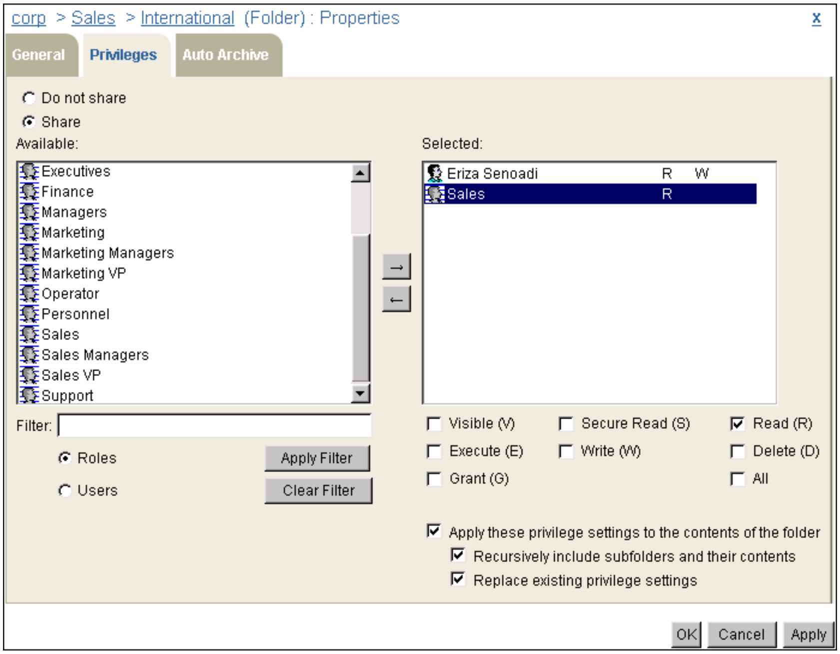


Figure 4-7 Setting privileges on an existing folder

Choose OK.

How to set privileges on a single file or new folder

The tasks for setting privileges on a single file or new folder are the same tasks you perform to set privileges on an existing folder, with the exception that a file or new folder has no contents on which to set privileges.

1 On Files and Folders, choose Create Folder or point to the arrow next to a file and choose Properties, as shown in Figure 4-8. The tasks you perform to set privileges on a single file or a new folder are identical.

On Properties, choose Privileges.

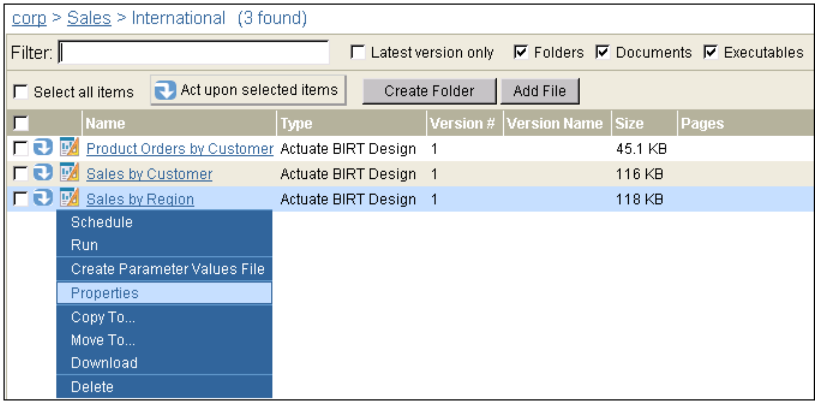


Figure 4-8 Choosing a single file

2 On Privileges, perform the following tasks:

1. Specify whether the file is shared or private by accepting Share or selecting Do not share.
2. Select one or more roles or users in Available and move them to Selected.
3. With the users or roles selected, assign privileges from the list of privileges.

For example, assign read and execute privileges on the Sales by Region BIRT design file to Eriza Senoadi. Then, assign read, execute, and grant privileges on the file to the Sales VP security role, as shown in Figure 4-9.

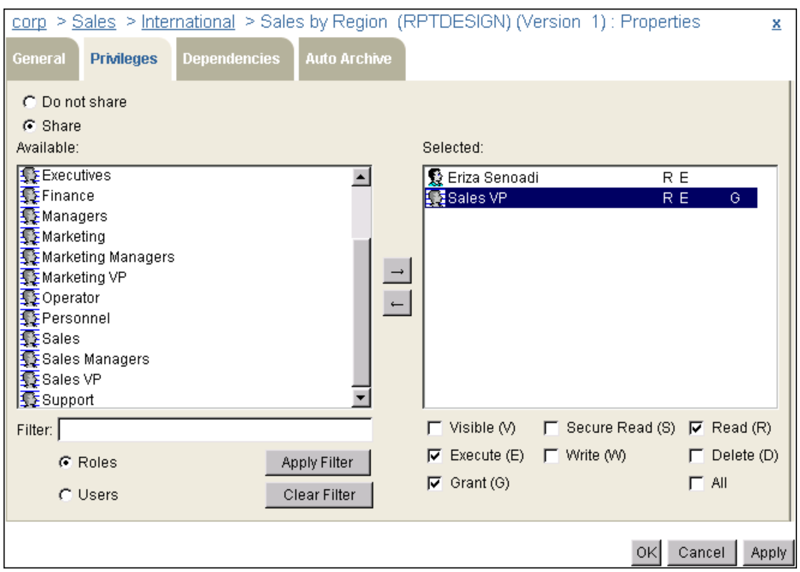


Figure 4-9 Setting privileges on a single item

Choose OK.

How to set privileges on multiple items

1 On Files and Folders, select the individual items on which you want to set privileges. Figure 4-10 shows two files selected. Alternatively, to select all items on the page, select the box next to Name. To select all items in the folder, select Select all items.

Point to Act upon selected items and choose Properties, as shown in Figure 4-10.

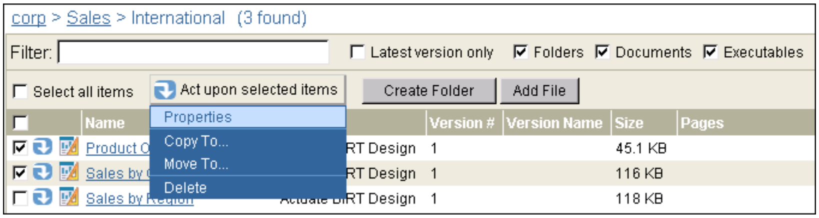


Figure 4-10 Selecting two files

On Properties, choose Privileges.

2 On Privileges, perform the following tasks:

1. To specify whether the selected items are private or shared, select Set file access type. Then, select Do not share or Share.
2. To display the list of roles in Available, select Roles. To display the list of users, select Users.
3. To remove privileges from the selected items, move one or more roles or users from Available to Remove these privileges. iHub assigns all privileges to a role or user you move to Remove these privileges. Deselect the privileges that you want the role or user to keep.
4. To add privileges to the selected items, move one or more roles or users from Available to Add these privileges. With the role or user selected, assign privileges from the privileges list.
5. To remove all privileges from the selected items, except privileges you assign in Add these privileges, select Remove all.

   For example, assign read and execute privilege on the two selected files to Eriza Senoadi. Then, assign read, execute, and grant privileges on the files to the Sales VP security role. Finally, select Remove all to remove all other privileges on the selected files, as shown in Figure 4-11.

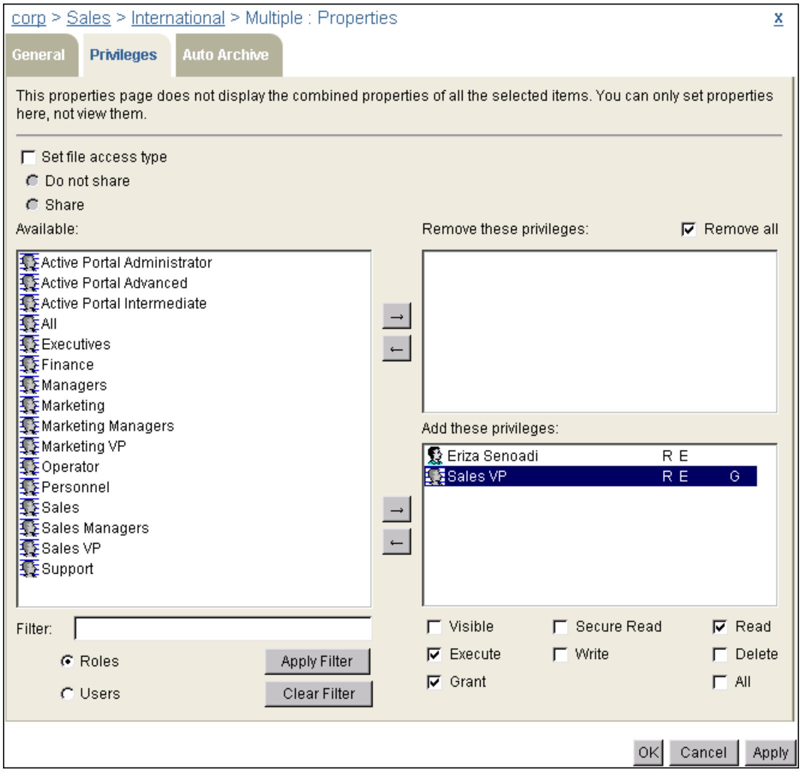


Figure 4-11 Setting privileges on multiple items

Choose OK.

About dependencies

A parameter values file has a dependency on the BIRT design file (.rptdesign) from which a user created the parameter values file. To run a parameter values file, it must have a dependency on the BIRT design file from which a user created the parameter values file. To run a parameter values file, a user must have execute and one of either read, secure read, or visible privileges on the BIRT design file on which the parameter values file depends. iHub updates the dependency information if a user moves the BIRT design to a different location on the Encyclopedia volume.

On Files and Folders, Properties—Dependencies displays the location of the BIRT design executable file, as shown in Figure 4-12.

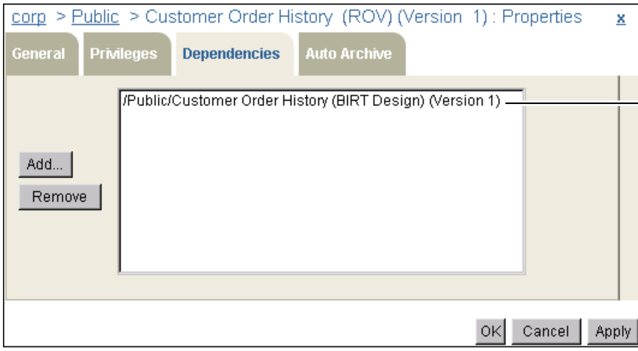


Figure 4-12 Viewing the location of the BIRT design executable

About autoarchiving

Autoarchiving is an iHub 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 iHub can delete the item from the volume. You can specify that iHub archive the item before deleting it. You can also specify that iHub 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 4-13 shows Properties—Auto Archive for a file.

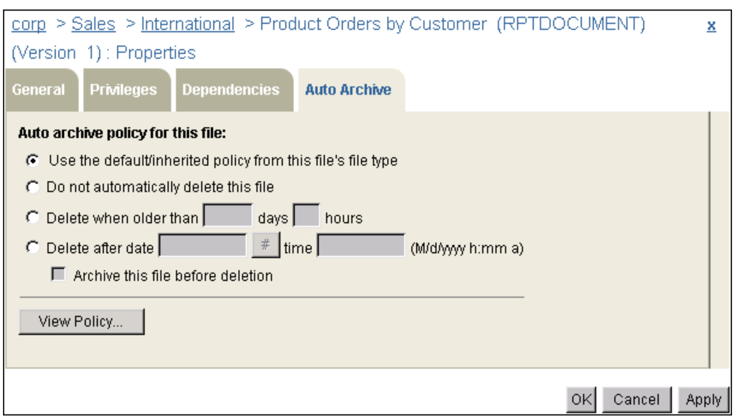


Figure 4-13 Viewing Properties—Auto Archive for a file

Figure 4-14 shows Properties—Auto Archive for a folder.

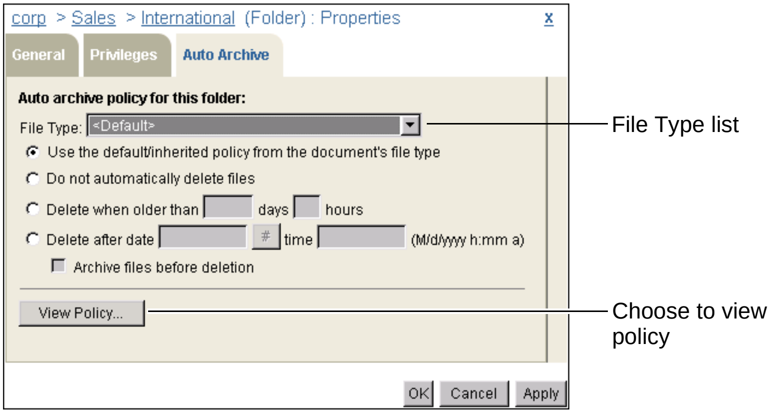


Figure 4-14 Viewing Properties—Auto Archive for a folder

Figure 4-15 shows Properties—Auto Archive for multiple items.

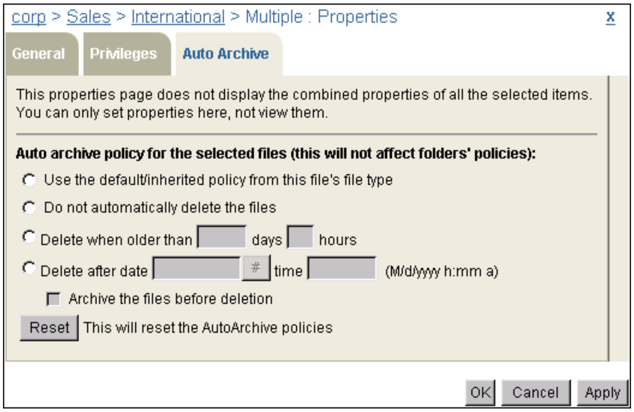


Figure 4-15 Viewing Properties—Auto Archive for multiple items

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 4-16.

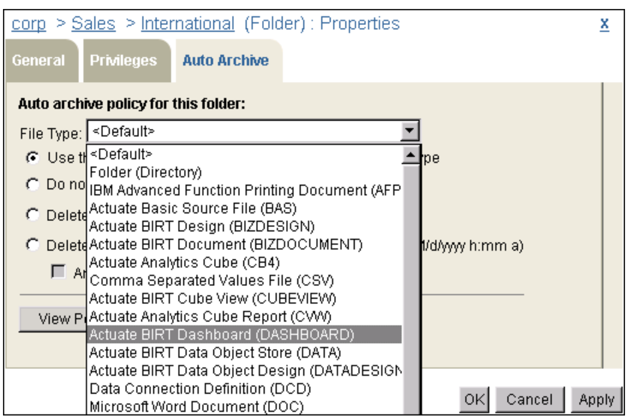


Figure 4-16 Selecting a file type for which to set autoarchive policy

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, iHub 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 iHub

  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. Autoarchive 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 autoarchive without changing the policy for any item from the default policy, iHub 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 autoarchive 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 4-17 shows sample archive policy information for a BIRT Document file.

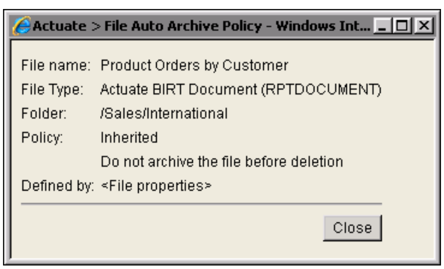


Figure 4-17 Viewing the autoarchive policy

Selecting not to delete automatically

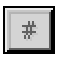
To prevent the autoarchive process from removing a selected folder and its contents, or a selected file or files, select Do not automatically delete files.

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 iHub 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 4-18.

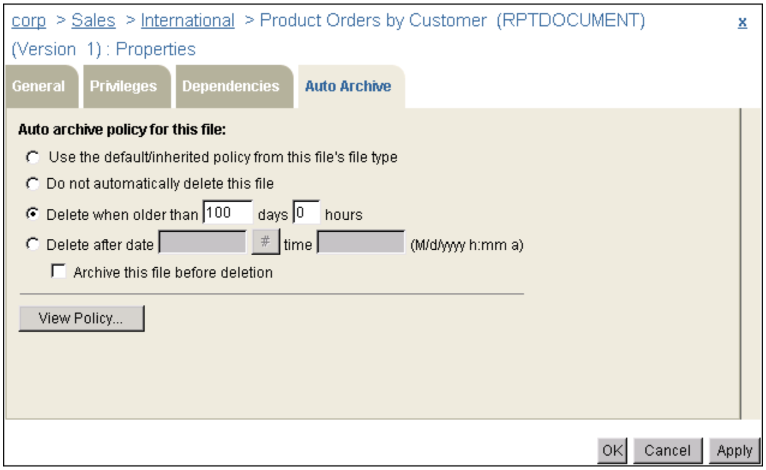


Figure 4-18 Setting autoarchive properties for a file

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 4-19.

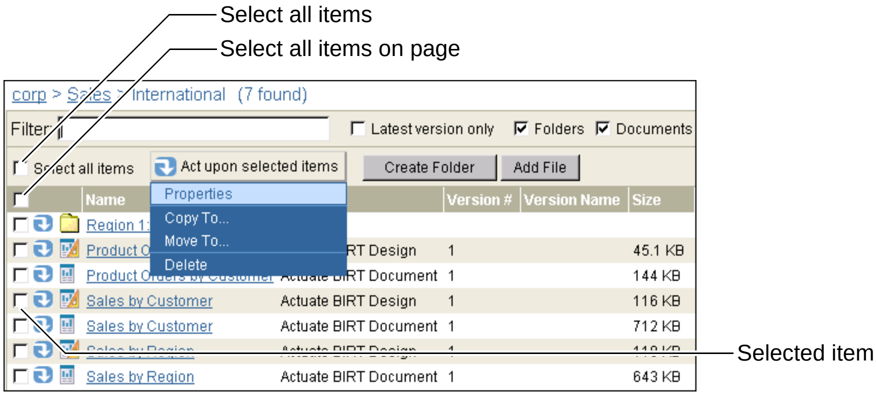


Figure 4-19 Selecting multiple files for which to set archive policy

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, and information object files. Design developers use design tools to create design files to publish to the Encyclopedia volume.

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

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 4-20.

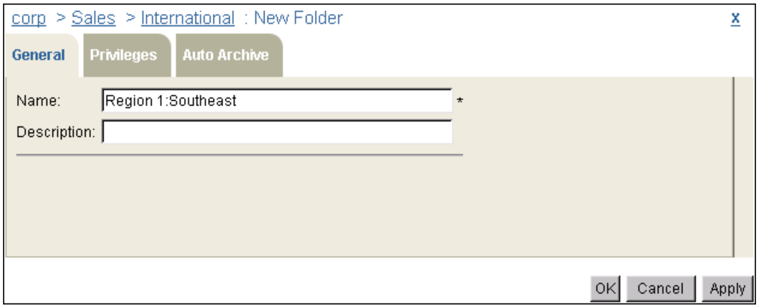


Figure 4-20 Specifying a name and description for a folder

3 On New Folder—Privileges, assign privileges to roles and users, as shown in Figure 4-21.

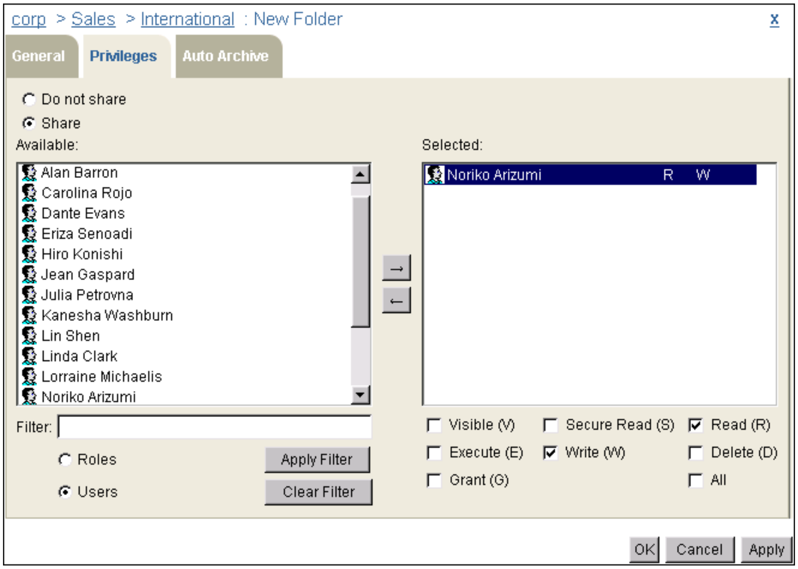
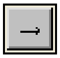


Figure 4-21 Assigning privileges to roles and users

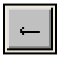
On Privileges, perform the following tasks:

1 Specify whether the folder 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 Read and Write.



4 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 iHub deletes the folder, and whether iHub archives the folder before deleting it, as shown in Figure 4-22.

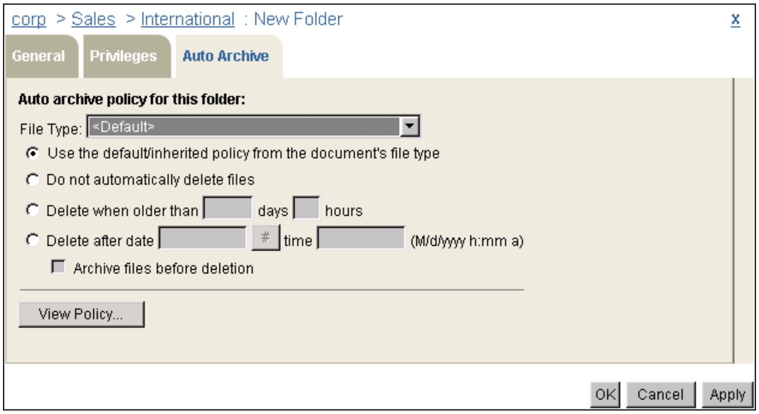


Figure 4-22 Specifying the autoarchiving policy on a folder

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

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, iHub 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 4-23.

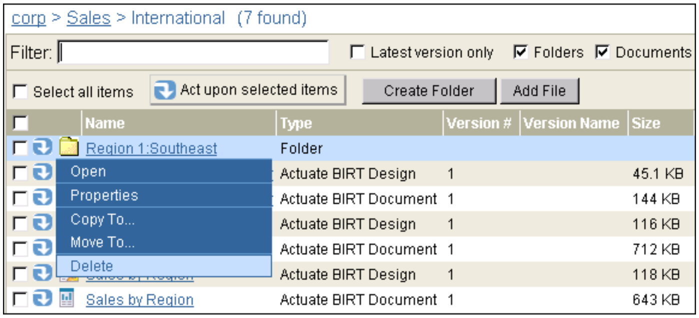


Figure 4-23 Deleting a file or folder

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 4-24.

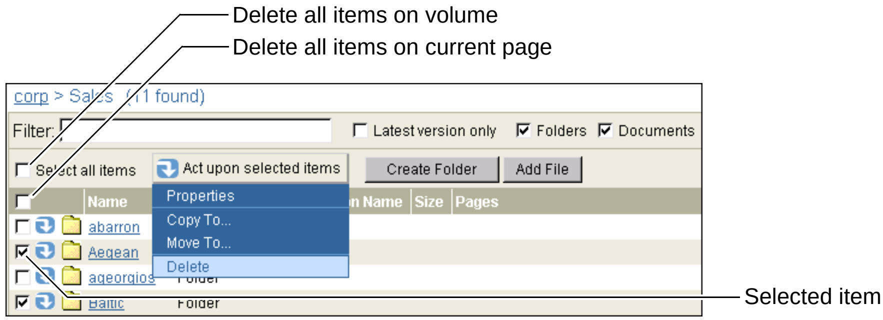


Figure 4-24 Deleting multiple folders

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 4-25.

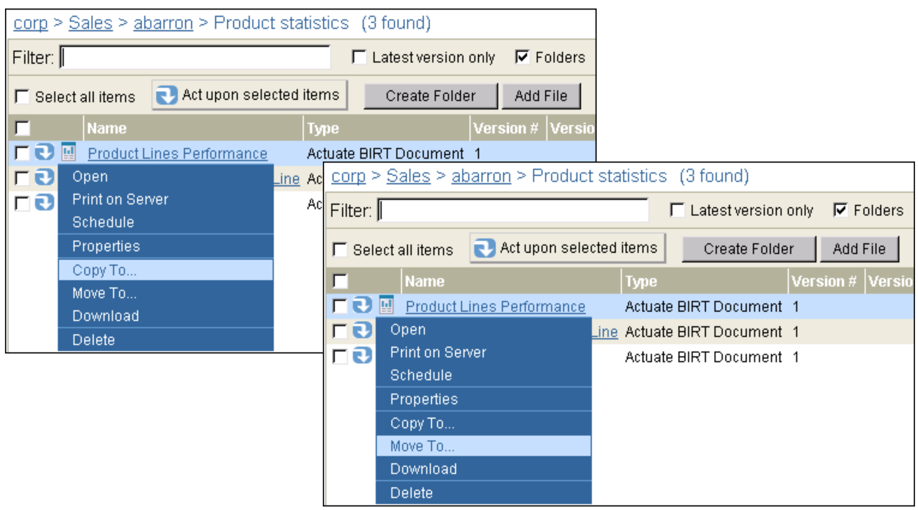


Figure 4-25 Choosing to copy or move a single file or folder

Copy or Move appears. You provide the same information, in the same way, whether copying or moving an item. Figure 4-26 shows Copy.

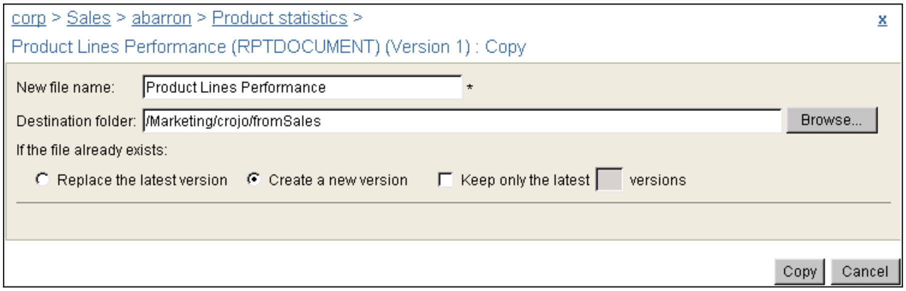


Figure 4-26 Copying or moving a file

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
    iHub replaces the latest version of the file with the new version.
  - Create a new version
    iHub creates a new version of the file.
  - Keep only the latest *n* versions
    Selecting Create a new version enables this option. iHub 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 4-27:
  - Replace the latest versions
    iHub replaces the latest version of any file in the folder or in any subfolder, with the new version.
  - Create new versions
    iHub 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. iHub 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.

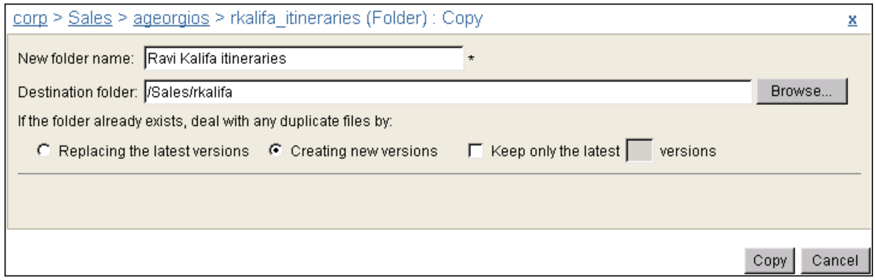


Figure 4-27 Copying or moving a folder

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 4-28.

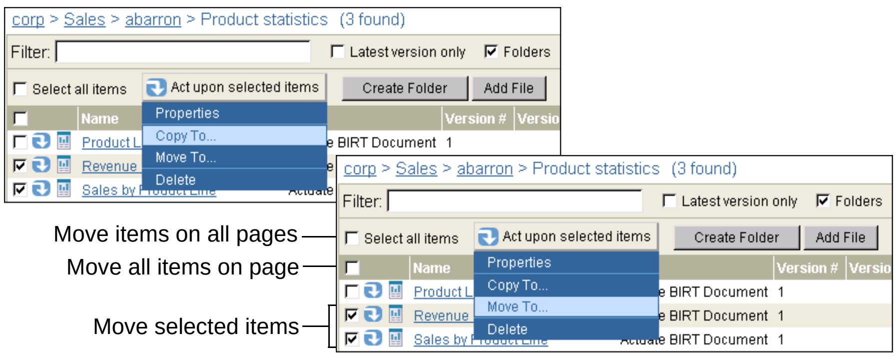


Figure 4-28 Copying and moving files or folders

2 If you are copying or moving multiple items, which can include both files and folders, perform the following tasks, as shown in Figure 4-29:

- 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
    iHub creates a new version of the file.

- Replacing all previous versions
  iHub replaces the latest version of any file with the new version. iHub does not replace all previous versions of a file with the new version.

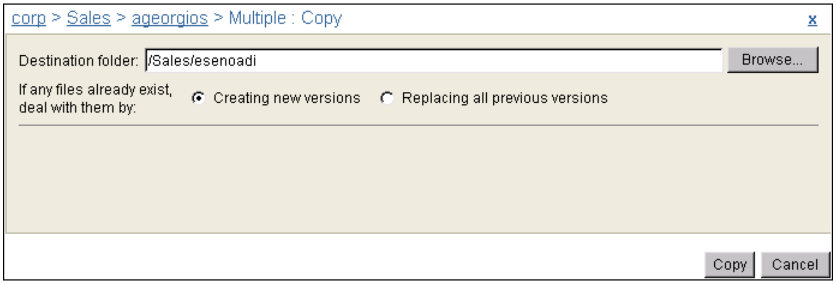


Figure 4-29 Copying or moving multiple items

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 4-30.

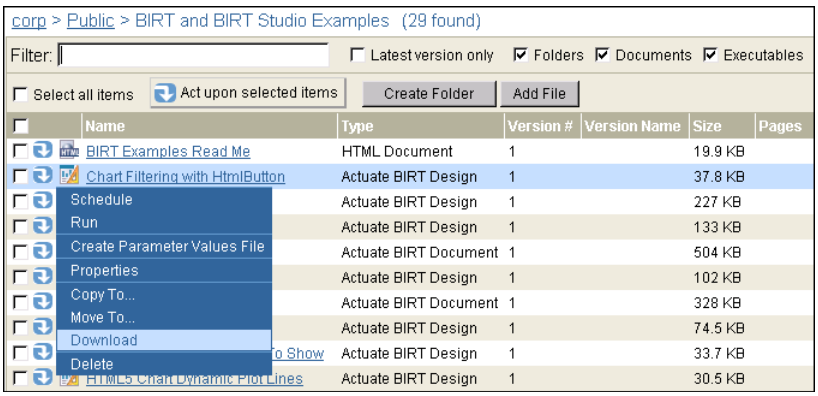


Figure 4-30 Downloading a file

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.

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 or parameter values file. When iHub executes the design, iHub 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, iHub 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.

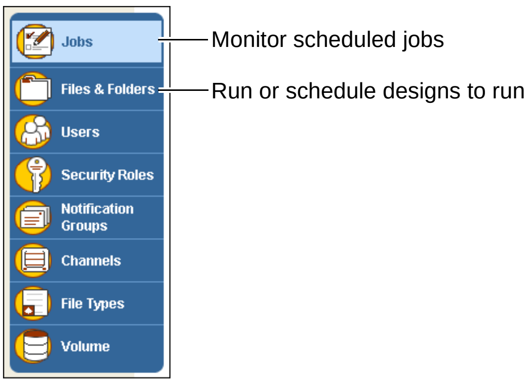


Figure 5-1 Accessing Jobs and Files and Folders from the side menu

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.

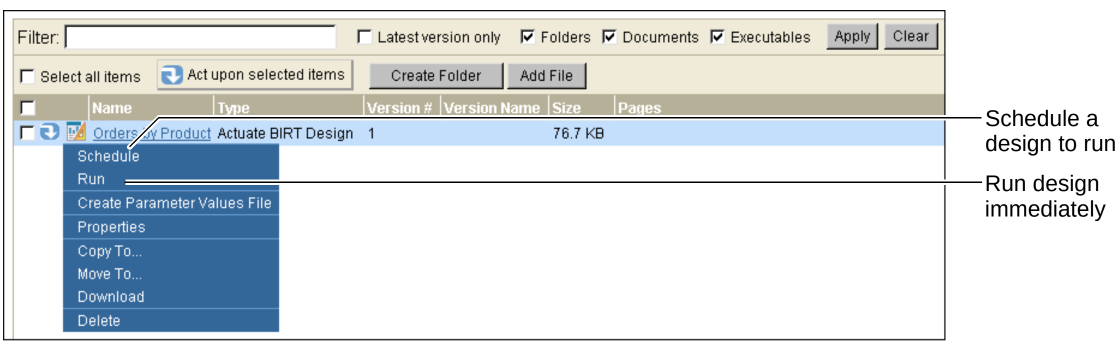


Figure 5-2 Accessing the menu for scheduling or running a design

Running a design

You can run a design using the default execution settings. iHub 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.

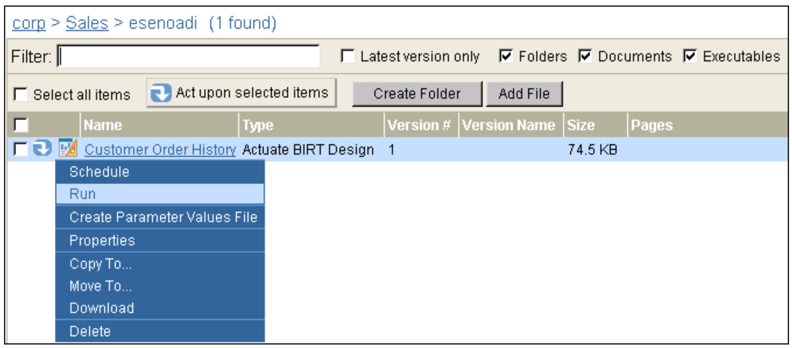


Figure 5-3 Choosing to run a design

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.

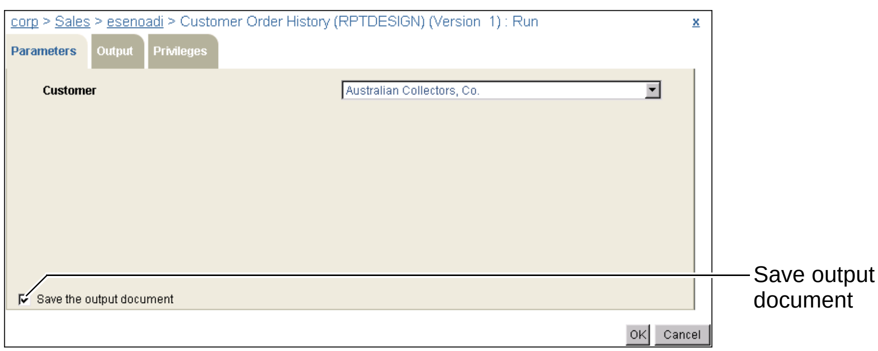


Figure 5-4 Saving the output when running a design

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.

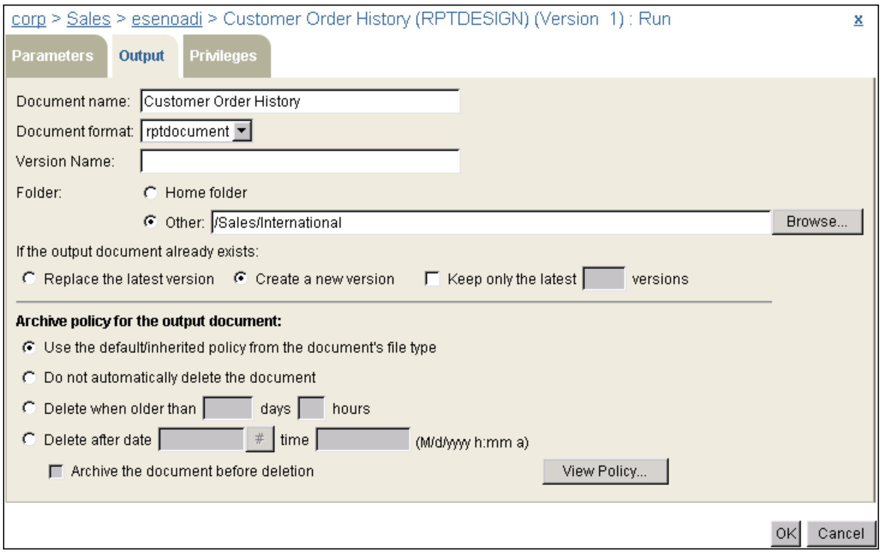
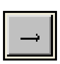


Figure 5-5 Specifying output properties

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.



2. Move roles or users from Available to Selected.
3. Assign privileges on the output document by selecting from the list of privileges such as Visible, Secure Read, or Read. For example, assign read privilege on the Customer Order History output document to the Marketing VP security role, as shown in Figure 5-6.

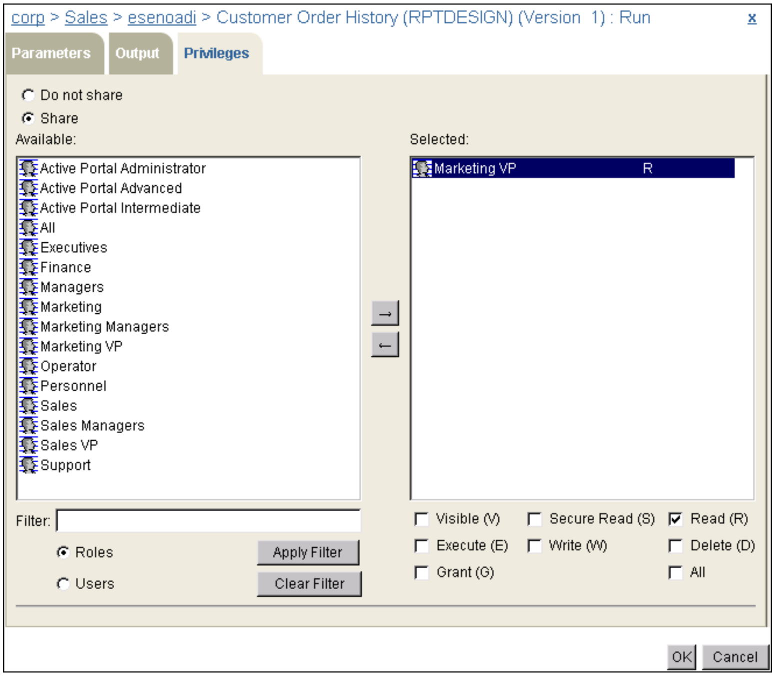


Figure 5-6 Specifying privileges on the output document

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 iHub does not save. This temporary document is sometimes called a transient document.

iHub 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:\Actuate\iHub\data. On a Linux system, it is /<Installation directory>/AcServer/data. The start scripts for iHub on a Linux system set TMPDIR to AC_DATA_HOME/server/tmp. Any iHub operation that creates a temporary file is responsible for deleting that file.

If you deliberately stop and start the iHub service, iHub retains the temporary document files. For example, if the administrator specifies a new transient report cache location, then stops and starts the iHub service, iHub moves any temporary files to the new location. When iHub restarts or stops abnormally, iHub 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

iHub incorporates a flexible job scheduling model for running designs. The term job refers to the following iHub 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

After a scheduled job runs, iHub 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, you can schedule a job to run at 4:00 P.M. on Monday if file \\server2\mydocuments\document.xls exists. If the file does not exist at that time, the job remains scheduled until the file does exist. Then, the job runs. If iHub is down when the conditions by which the job can run are satisfied, the job runs when iHub 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. iHub runs the event-based job when it finds the file or folder. If the item does not exist, iHub 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. iHub 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 iHub scans previously completed, qualifying jobs. For example, if you specify 60 minutes, iHub scans jobs that completed in the preceding 60 minutes. If a job meets the event-based criteria, iHub runs the event-based job.
Custom event	Specify a web service that iHub monitors. iHub communicates with the web service and runs a custom event-based job when the web service returns a signal to iHub. To specify a custom event, you must create a web service application and deploy it in the BIRT iHub 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. iHub waits a fixed amount of time for the generated document, 30 minutes by default. If document generation takes longer than the wait period, iHub 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. iHub saves the output in the Encyclopedia volume, so you can view the output 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. iHub 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 iHub 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 iHub 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 iHub 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 or a parameter values file (.rov).

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

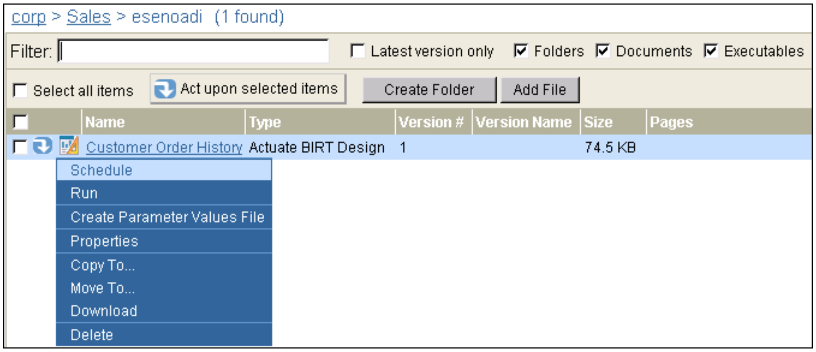


Figure 5-7 Choosing to create a scheduled job

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.

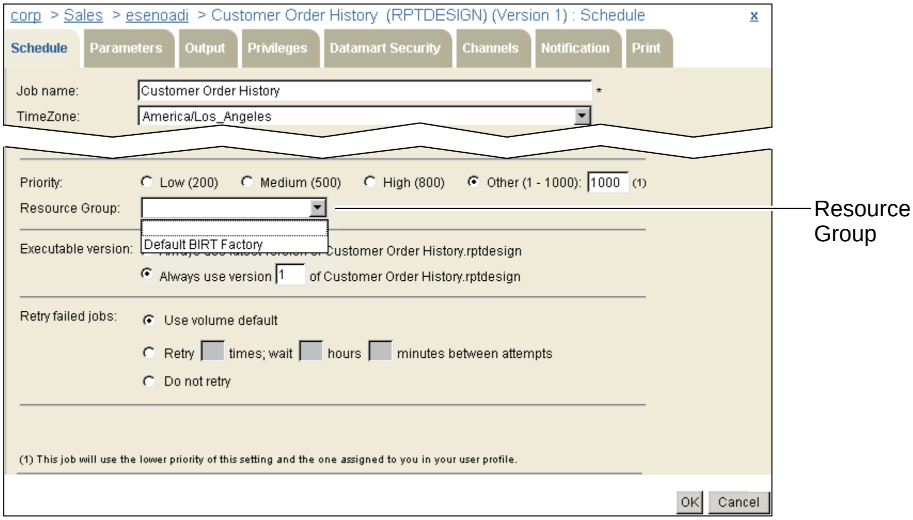


Figure 5-8 Selecting a resource group

- 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 iHub processes for generating documents, or the number of jobs in the queue. iHub saves the resulting document in your Home folder if you have one. Otherwise, iHub 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 iHub 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, iHub 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 iHub instance. The administrator can set minimum and maximum priority levels for an asynchronous resource group to expedite job scheduling.

A job having an assigned resource group has priority over a job having no assigned resource group. 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, iHub assigns the job one of the following default resource groups:

- Default BIRT Factory
  Runs a BIRT design as a scheduled job
- Default BIRT Online
  Runs a BIRT design unscheduled
- Default BIRT Studio
  Used when creating, modifying, and viewing documents using BIRT Studio
- Default BIRT 360
  Runs a BIRT dashboard (.dashboard) or gadget (.gadget) design unscheduled
- Default BIRT Data Analyzer
  Runs a Data Object Store (.data) design 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.

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 iHub 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 iHub should retry running the job and how long the system should wait between tries.

- Do not retry
  Make no retry effort.

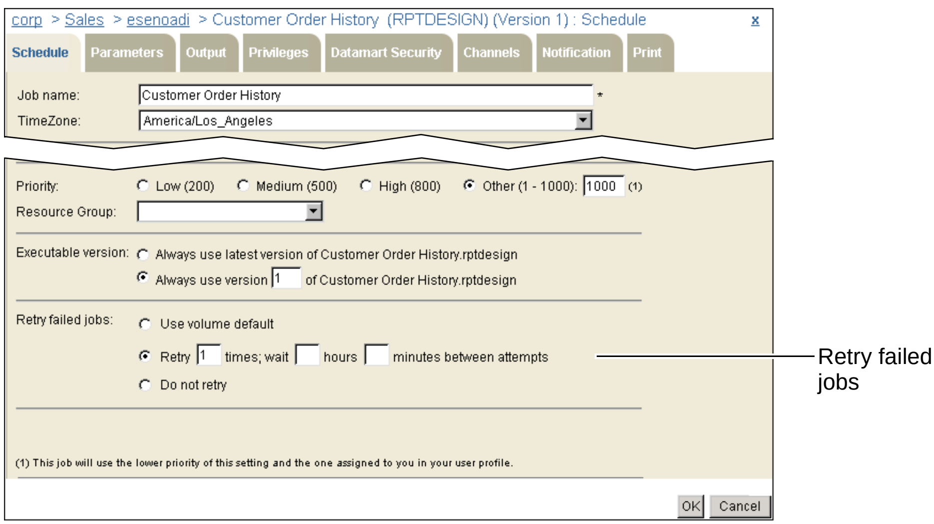


Figure 5-9 Selecting a job retry option

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.

- iHub 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.

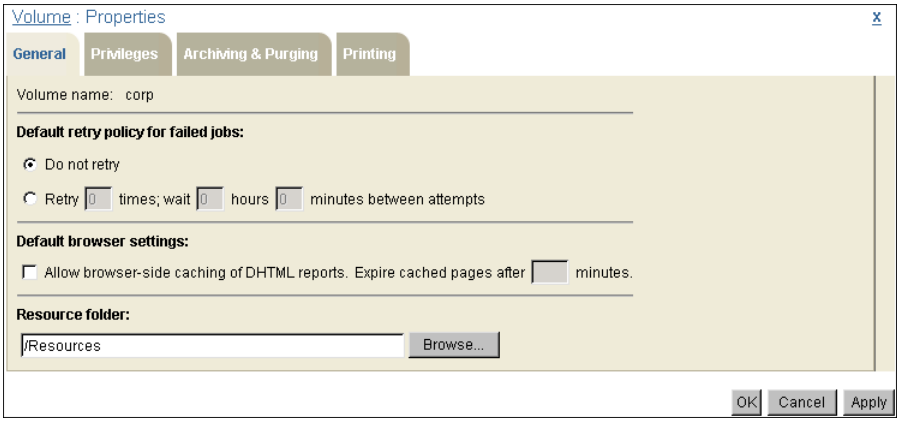


Figure 5-10 Specifying the default job retry policy

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.

If the job retry options are set to retry a job if it fails, the job remains active if the node the job is running on fails. For example, if the node crashes, iHub tries to run the job again when the node restarts.

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.

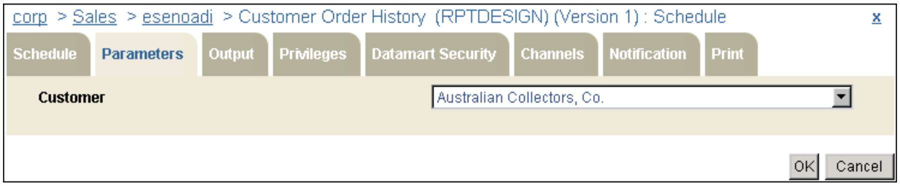


Figure 5-11 Setting parameter values on Schedule—Parameters

Schedule—Parameters does not include the Save option, as Run—Parameters does, because iHub always saves scheduled job output.

Hidden parameters do not appear on Parameters. iHub 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, iHub 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 parameter values.

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.

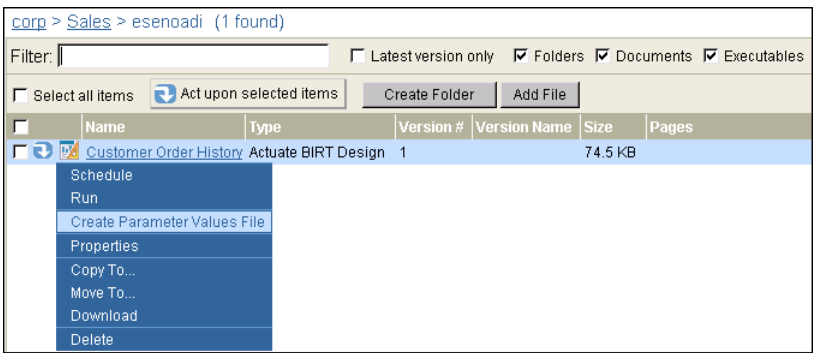


Figure 5-12 Creating a parameter values file

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 and 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 format to which you save the output of a BIRT design or convert a BIRT document.
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 iHub pre-selects, if you have a home folder ■ The folder in which the design resides ■ A folder that you specify

(continues)

Table 5-3 Schedule—Output settings (continued)

Property	Description
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 iHub archive the output document before deleting it.
View policy	View the current autoarchive policy for the output document file type.

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 iHub 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.

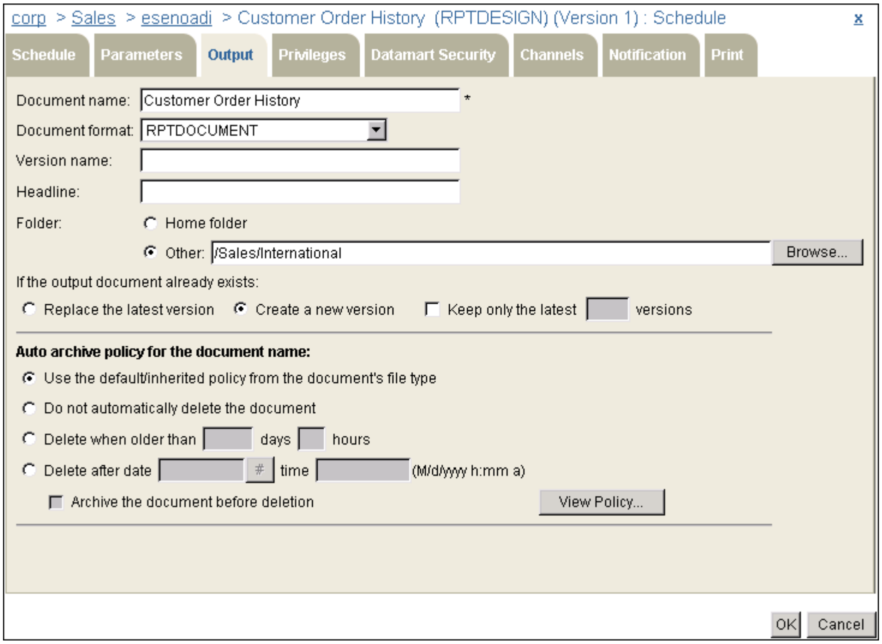


Figure 5-14 Specifying output file properties on Schedule—Output

Specifying a headline

You can specify a headline that becomes a component of the job completion notice that iHub writes to a channel. iHub 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 5-15, to select one of the output formats described in Table 5-4 or Table 5-6.

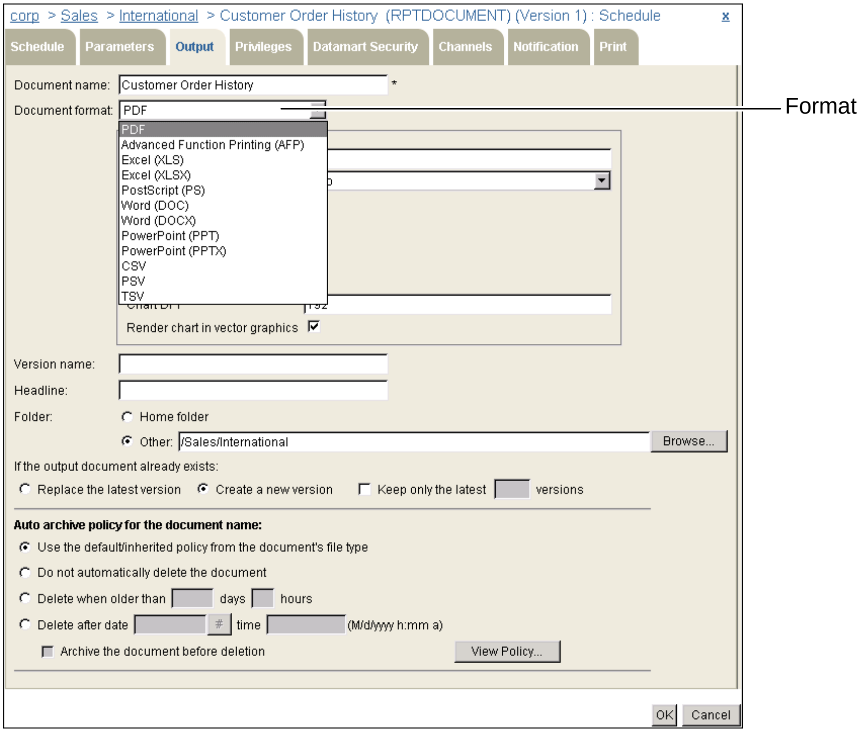


Figure 5-15 Possible file formats for output from a BIRT design

Converting file format of a BIRT document

By default, when you run a BIRT design (.rptdesign), iHub 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. When you schedule a BIRT document (.rptdocument) to run, the document format list contains comma-, pipe-, and tab-separated value (CSV, PSV, or TSV) output formats. When you schedule a BIRT design (.rptdesign) file to run, the Document format list on Schedule—Output does not contain these output formats.

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 (XLS) and Excel (XLSX)	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.

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 Newsfeeds, and choose Schedule, as shown in Figure 5-16.

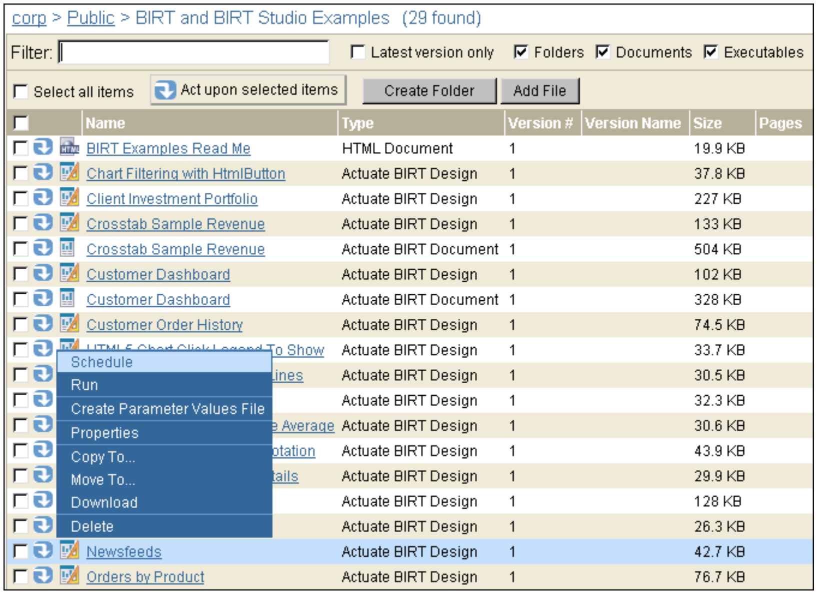


Figure 5-16 Choosing to schedule a BIRT design to run

2 On Schedule, choose OK to accept the default settings and run the design right away.

3 Navigate to your Home folder. The output document, Newsfeeds, appears after the scheduled job runs, as shown in Figure 5-17.

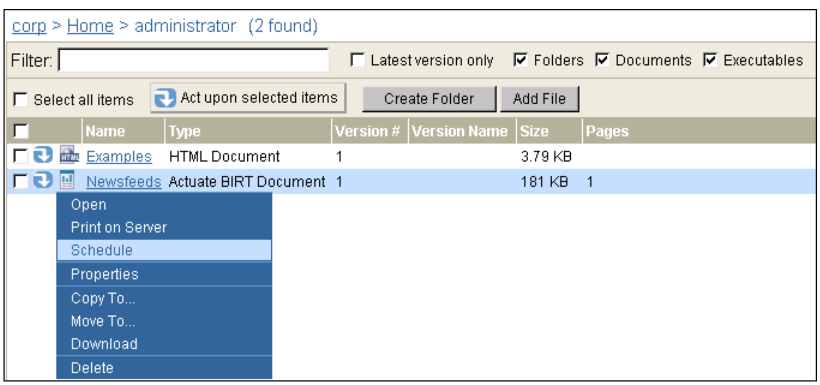


Figure 5-17 Choosing to schedule a format conversion job

Point to the arrow next to Newsfeeds and choose Schedule.

On Schedule, choose Output.

4 On Output, perform the following tasks:

1 In Document format, select CSV, as shown in Figure 5-18.

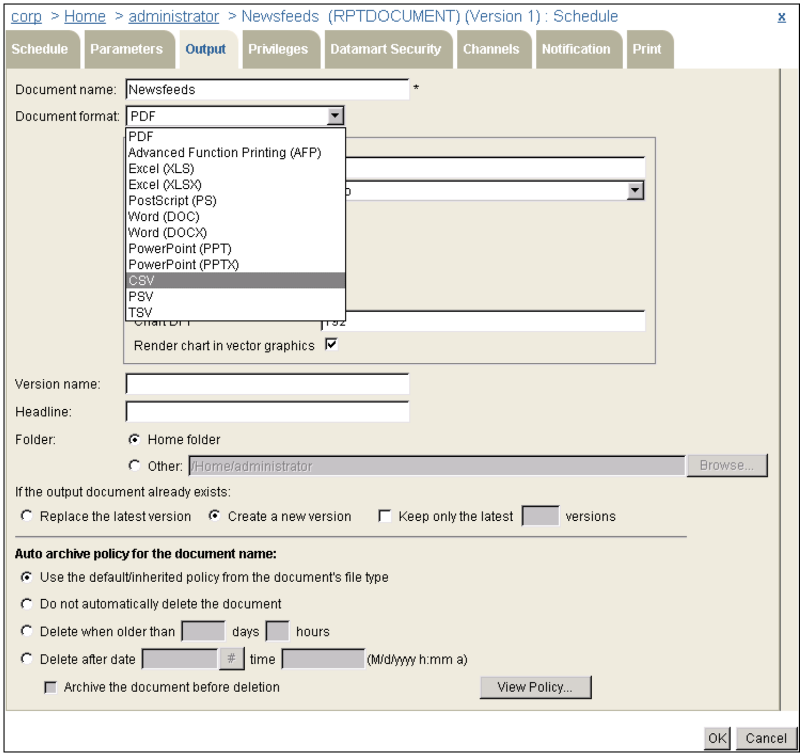


Figure 5-18 Selecting the CSV output format

The conversion options for CSV appear, as shown in Figure 5-19.

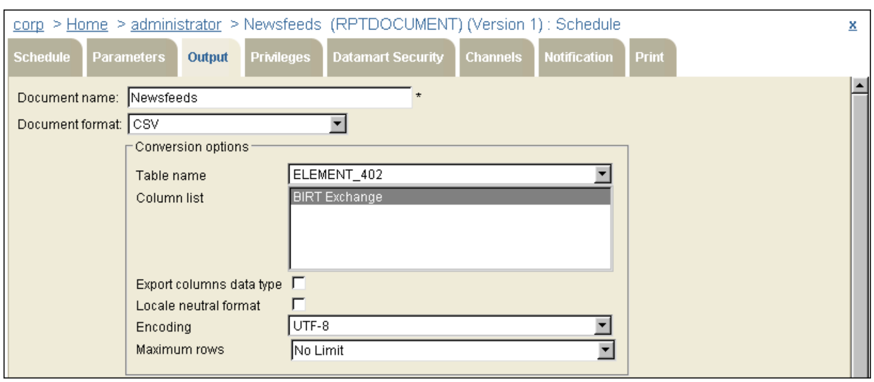


Figure 5-19 Viewing the conversion options for CSV

2 In Table name, select Main Table, as shown in Figure 5-20.

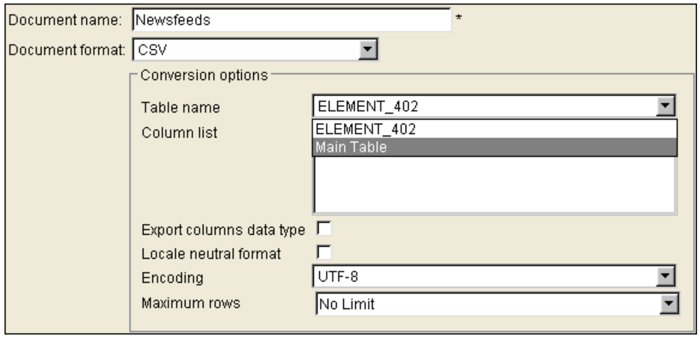


Figure 5-20 Selecting a table name

The list of columns in Main Table appear, as shown in Figure 5-21.

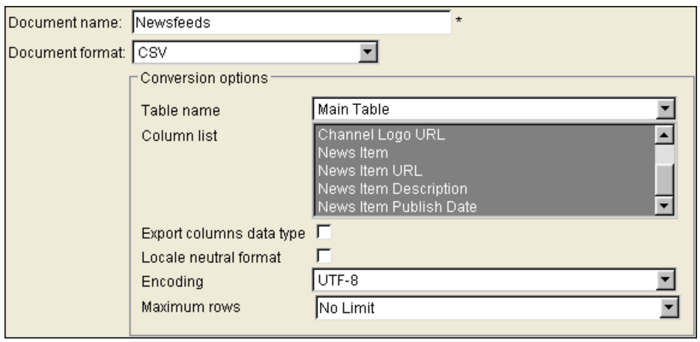


Figure 5-21 Viewing the list of columns in the Managers table

3 Select News Item, hold down the CTRL key and select the News Item URL column. Select Export columns data type, as shown in Figure 5-22. Accept other defaults on Output.

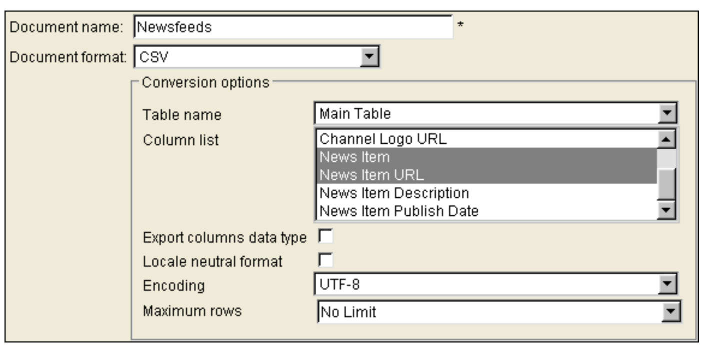


Figure 5-22 Selecting CSV conversion options

Choose OK.

5 Choose Jobs from the side menu, choose Completed, and then select Newsfeeds.CSV, as shown in Figure 5-23, from the list of documents.

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.

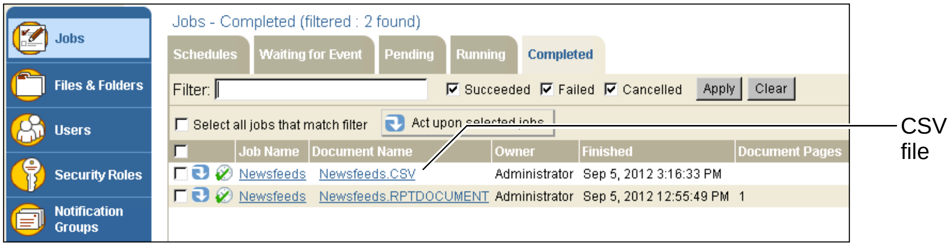


Figure 5-23 Finding the CSV output file

Setting privileges on an output document

Use Schedule—Privileges to assign privileges on the output document.

How to set job privileges

On Schedule—Privileges, perform the following tasks:

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

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. For example, assign read privilege on the Customer Order History output document to Marketing Vice President Carolina Rojo, as shown in Figure 5-24.

If you assign grant or delete privilege on the output document, you must assign visible privilege also.

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

Select Share to reinstate assigned privileges.

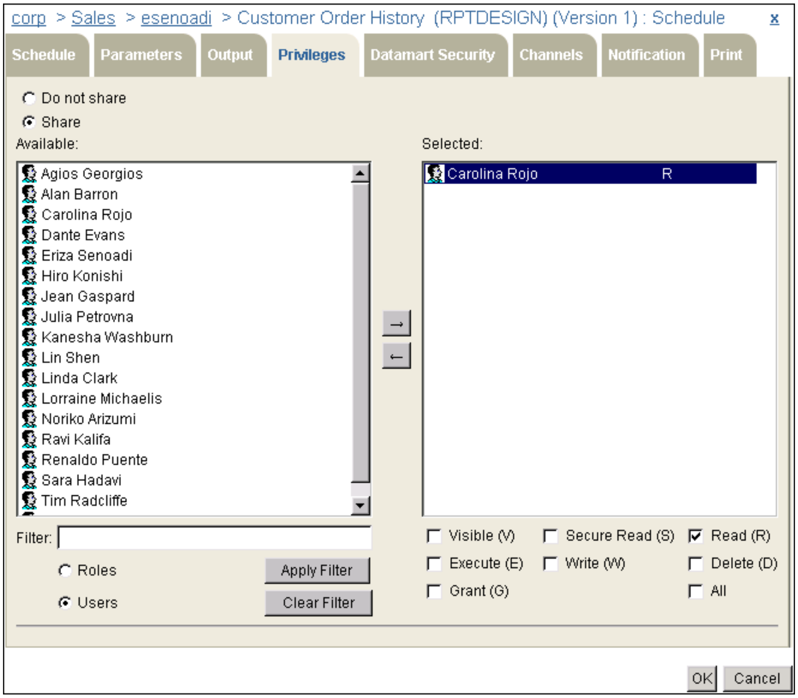


Figure 5-24 Assigning privileges on job output document

About Datamart Security

Datamart Security supports filtering the data a scheduled job generates. Datamart Security is available to the Administrator user or to a user belonging to the Administrator role. 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 iHub 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 5-25.

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

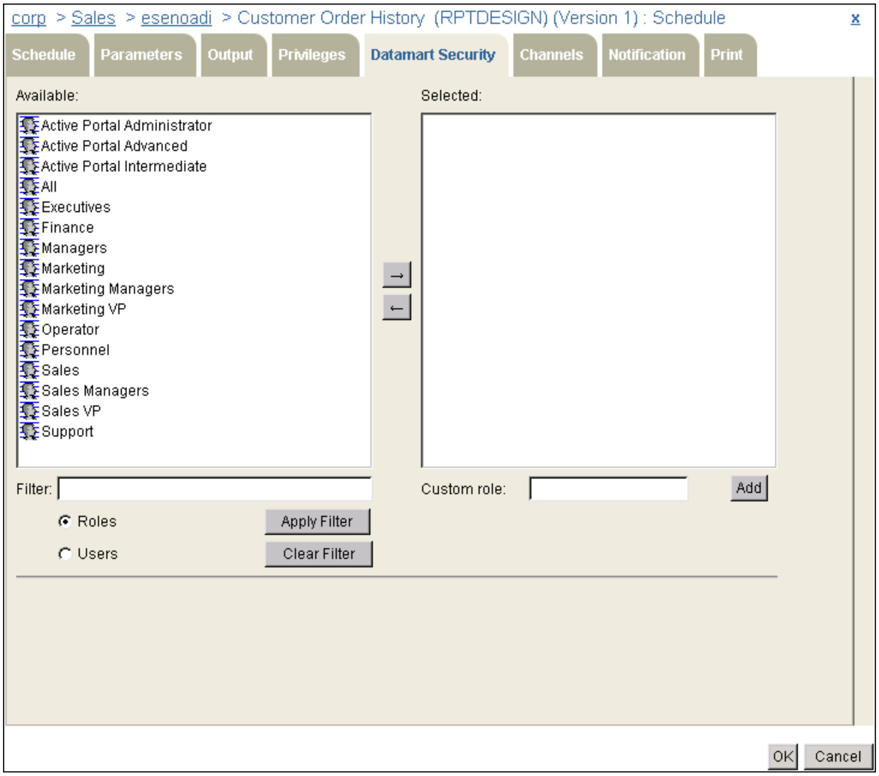


Figure 5-25 Selecting roles or users for which to filter job output

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 5-26. Channels displays only those channels to which the user who initiates the run request has write access.

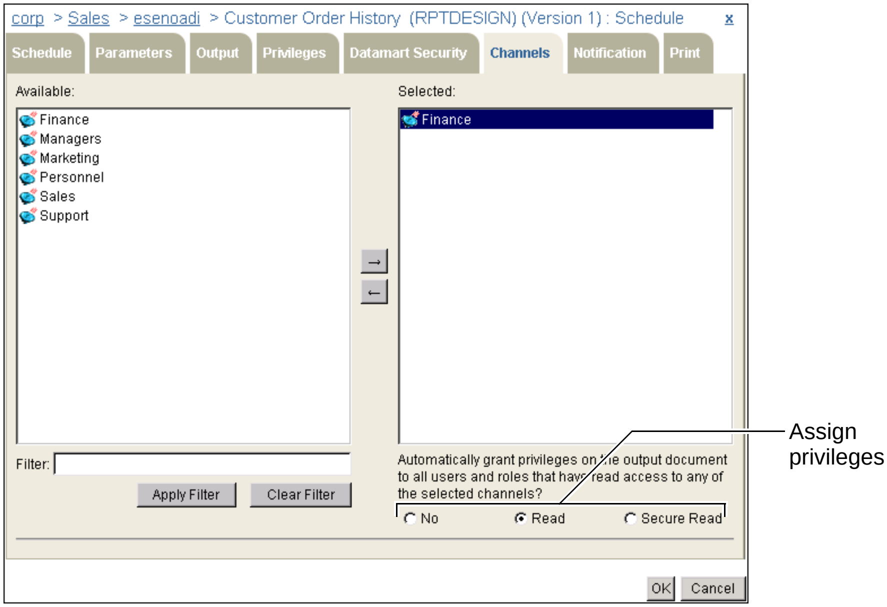


Figure 5-26 Selecting channels on which to view a job notice

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 5-27. iHub sends notification of job completion to the members of the groups and to the individual users that you select.

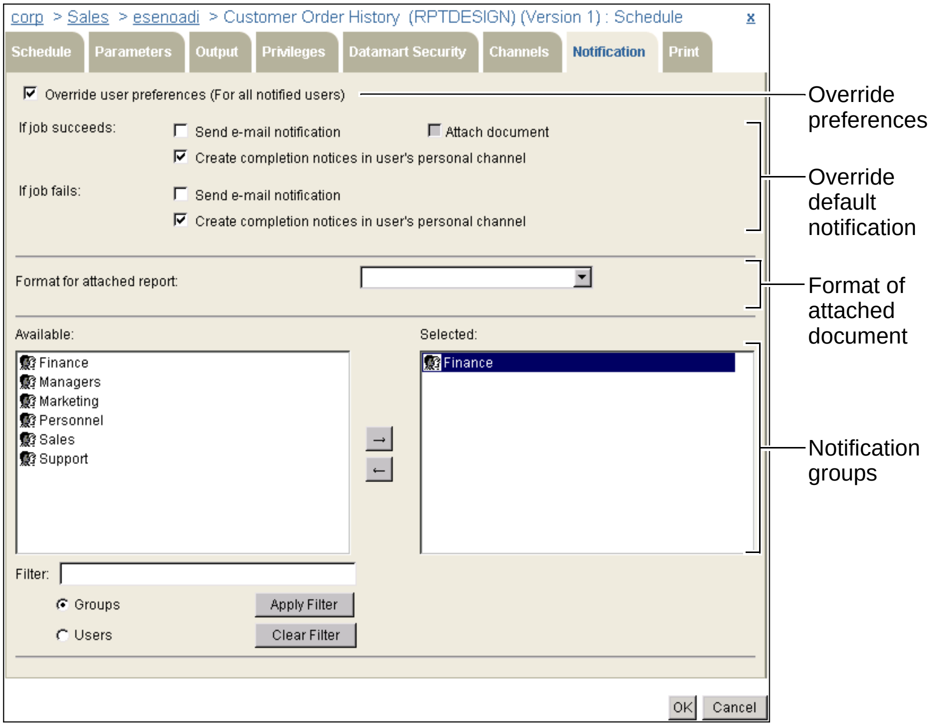


Figure 5-27 Selecting groups and users to notify of job completion

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

  iHub 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 iHub prints the output document after generating it. If you want to print the document, either by sending it to an iHub 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 5-28 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.

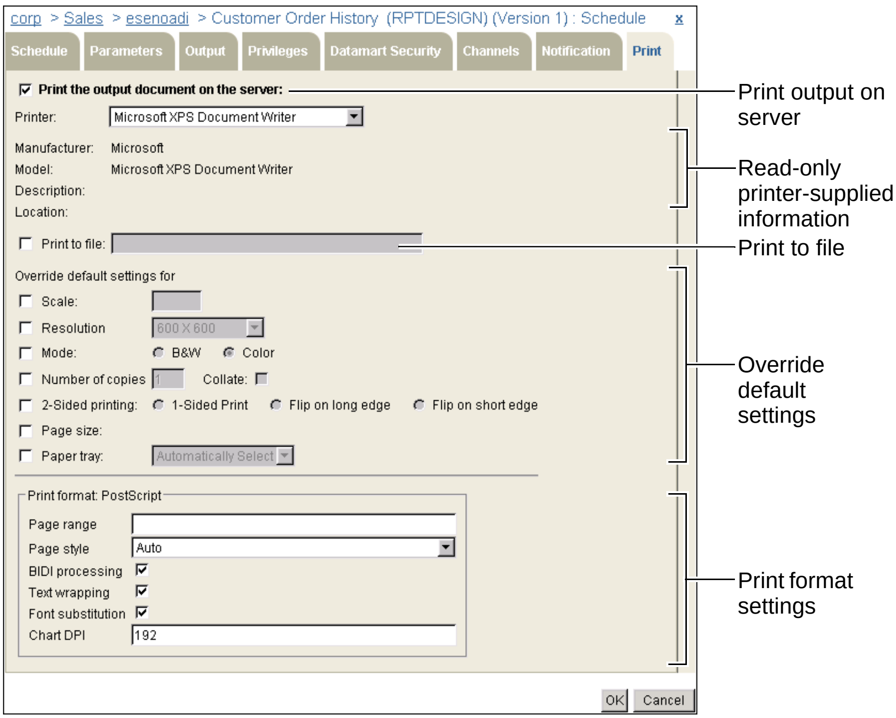


Figure 5-28 Selecting options on Schedule—Print for printing a BIRT document

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

Table 5-5 Schedule—Print properties

Property	Description
Print the output document on the server	Prints the output document.

(continues)

Table 5-5 Schedule—Print properties (continued)

Property	Description
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.
2-Sided printing	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.
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

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 iHub 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

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. You reconfigure some iHub 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 a parameter values file (.rov) does not have a dependency set to the design file from which a user created the ROV, iHub displays the error message shown in Figure 5-29 if you try to schedule a job to run the ROV.

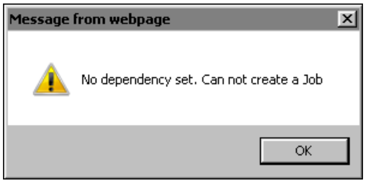


Figure 5-29 Error message when running an ROV file with a missing dependency

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 a BIRT design (.rptdesign) file

1 On Files and Folders, point to the arrow next to a report parameter values file name and choose Properties, as shown in Figure 5-30.

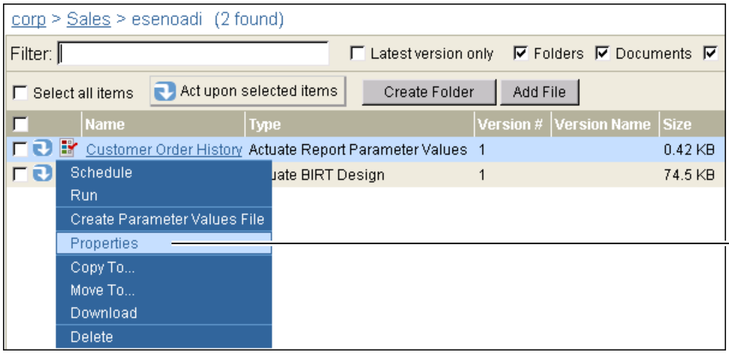


Figure 5-30 Choosing properties for a report parameter values file

On Properties, choose Dependencies.

2 On Dependencies, choose Add.

3 To make the parameter values file dependent on the BIRT design executable, on File Browser, select the BIRT design and choose OK.

Dependencies appears with the added dependency, as shown in Figure 5-31.

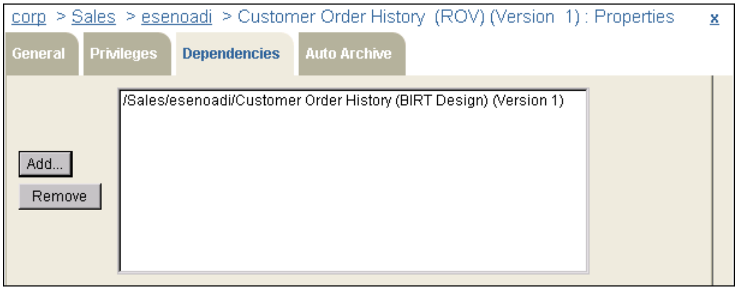


Figure 5-31 Adding a dependency

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 option to the user:

- Execute and either read, secure read, or visible privilege on the design
- The BIRT option for running a BIRT design (.rptdesign).

- To enable a user to run a parameter values file (.rov), you must assign the user the following privileges:
  - Execute and either read, secure read, or visible privileges on the design from which a user creates the ROV or on which the ROV depends
  - Read or secure read privilege on the ROV
- Write privilege on the folder to which iHub writes the document
- Write privilege on the channel to which the user submitting a job sends the job completion notice

The job submitter can cancel a job. A user can get or delete information about a job that the user submits. Only the system administrator can cancel or 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 iHub 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 Management Console and Information Console:

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

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 5-6 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 5-6 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. iHub 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, iHub uses the default locale's value meaning for that field. If no default locale exists in the file, iHub uses a hard-coded value from the C locale.

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

Table 5-7 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 5-7 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

(continues)

Table 5-7 Date format variables (continued)

Symbol	Description	Example	Result
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>
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. iHub formats times according to specifications in the locale map for Management Console. Table 5-8 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 5-8 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.<document extension>
hh	Returns the hour of the day with the leading zero (00-23).	Hour {hh}.<document extension>	Hour 09.<document extension>
n	Returns the minute without the leading zero (0-59).	Minute {n}.<document extension>	Minute 5.<document extension>
nn	Returns the minute with the leading zero (00-59).	Minute {nn}.<document extension>	Minute 05.<document extension>
s	Returns the second without the leading zero (0-59).	Second {s}.<document extension>	Second 1.<document extension>
ss	Returns the second with the leading zero (00-59).	Second {ss}.<document extension>	Second 01.<document extension>
tttt	This setting uses formats that are in the Management Console's locale map.	{tttt}	8:45:00 PM

(continues)

Table 5-8 Time format variables (continued)

Symbol	Description	Example	Result
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 from the Management Console locale map.	{h:n:s AMPM}	8:45:3 PM

iHub 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.

iHub 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 5-9 describes these Jobs properties.

Table 5-9 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

iHub sends a job completion notice to Jobs—Completed after a scheduled job runs. A user or the administrator selects whether iHub sends a notice to a user's personal channel. If the job is successful, iHub includes a link to the output document in the completion notice, as shown in Figure 5-32. If the user deletes the output document from the folder to which the scheduled job wrote the document, iHub also deletes the link to the document from the completion notice on Jobs—Completed, but iHub does not delete any other part of the completion notice.

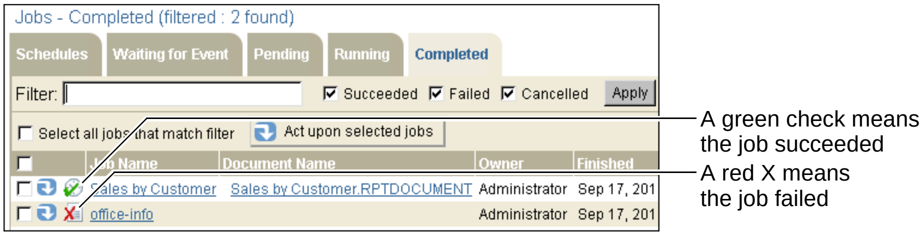


Figure 5-32 Viewing Jobs—Completed

iHub 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 iHub sends a notice to a user and when iHub 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 5-33. 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
    iHub deletes the notice after the time that the job completion notice deletion policy for the volume specifies.
  - Delete notice after *n* days *n* hours
    iHub deletes the notice after the number of days and hours you specify.
  - Do not automatically delete notice
    iHub does not delete the notice from the user's personal channel.

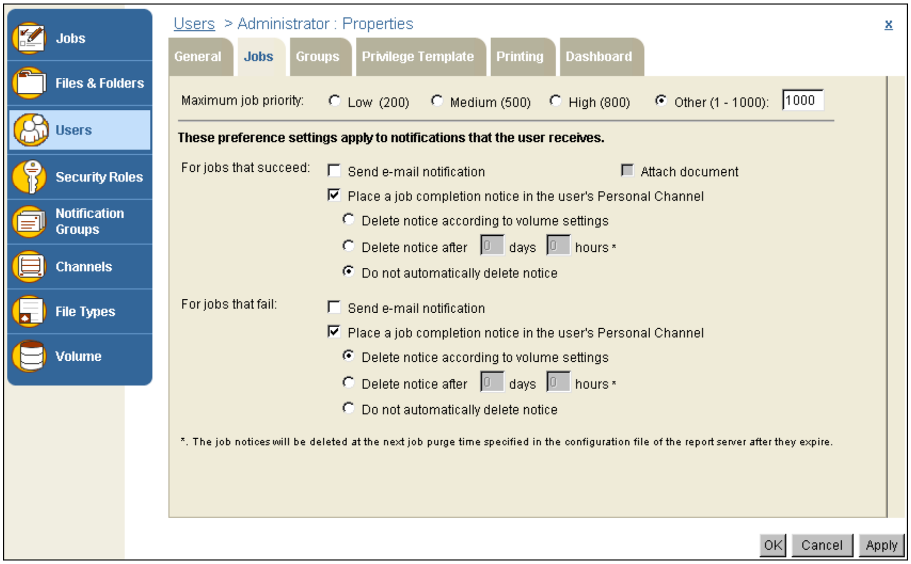


Figure 5-33 Setting completion notice properties on Users—Properties—Jobs

- 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 5-34. iHub does not purge notices if you specify 0 days 0 hours or if you do not select the property.

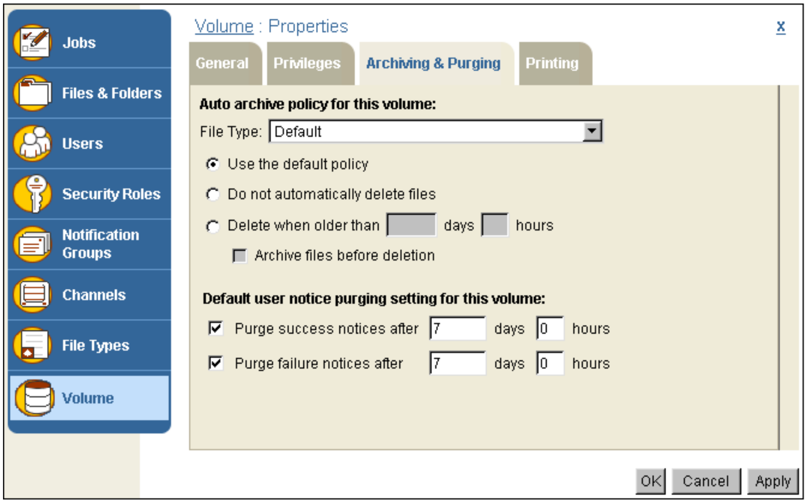


Figure 5-34 Volume—Properties—Archiving and Purging

As shown in Figure 5-35, after logging in to Configuration Console and choosing Advanced view, the administrator can set the job completion notice expiration properties by choosing Volumes—Properties—Advanced—Archiving and Purging.

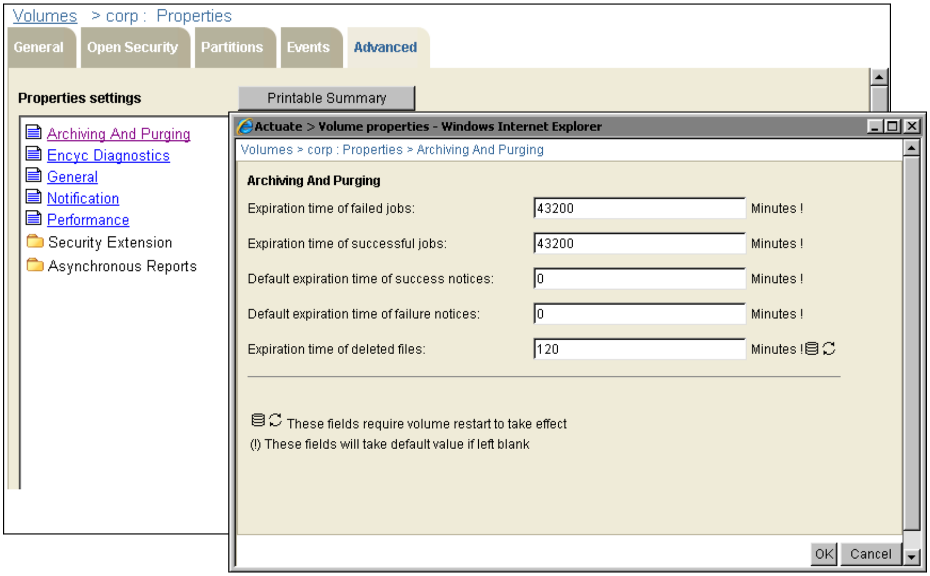


Figure 5-35 Setting properties on Archiving and Purging in Configuration Console

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, iHub 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 iHub 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, iHub deletes the notice according to the notified user's existing deletion policy.

iHub 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 5-36. By default, this time is 2:15 A.M.

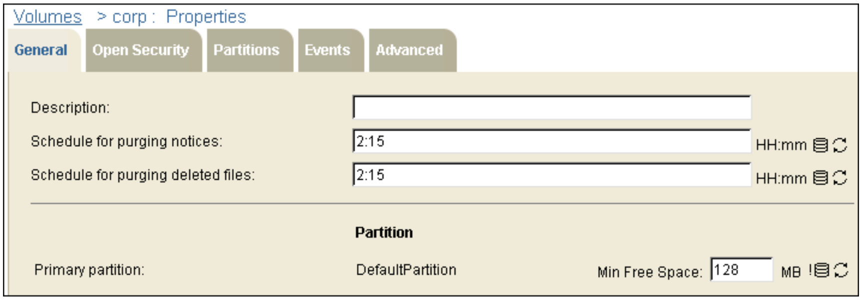


Figure 5-36 Setting Schedule for purging notices in Configuration Console

iHub deletes a job completion notice from a user's personal channel according to the deletion policy in effect when iHub ran the job. A user typically views a document and a job completion notice in Information Console. iHub 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, iHub 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, iHub deletes that notice after that time period expires. iHub 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, iHub does not delete the notice from the user's personal channel or from Jobs—Completed. iHub 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, iHub 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 5-10 lists the default information that appears on each property listing. On Options, you can modify these column settings.

Table 5-10 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
Completed	Job name
	Document name
	Owner of the job
	Date and time iHub 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 5-11 describes the possible event states.

Table 5-11 Event states

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

iHub maintains status information for scheduled jobs, but not documents that iHub 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 5-37.

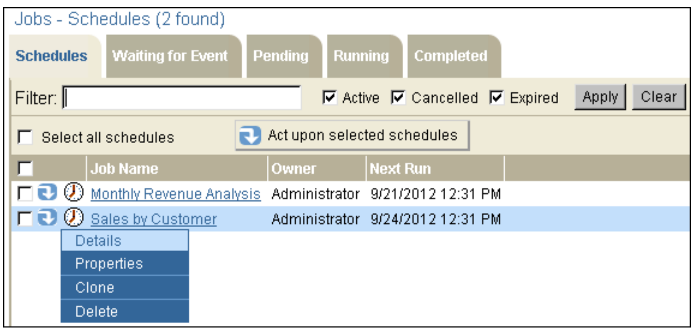


Figure 5-37 Getting detailed information about a job

Details—Summary displays by default. Summary lists basic information about the job, the executable file, and the output document, as shown in Figure 5-38.

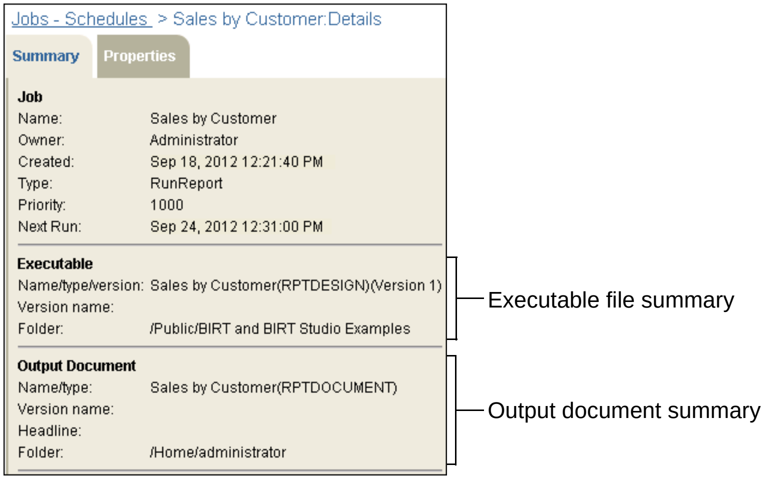


Figure 5-38 Viewing the Details—Summary page

To display additional job details, choose Properties. Figure 5-39 shows a partial view of Details—Properties.

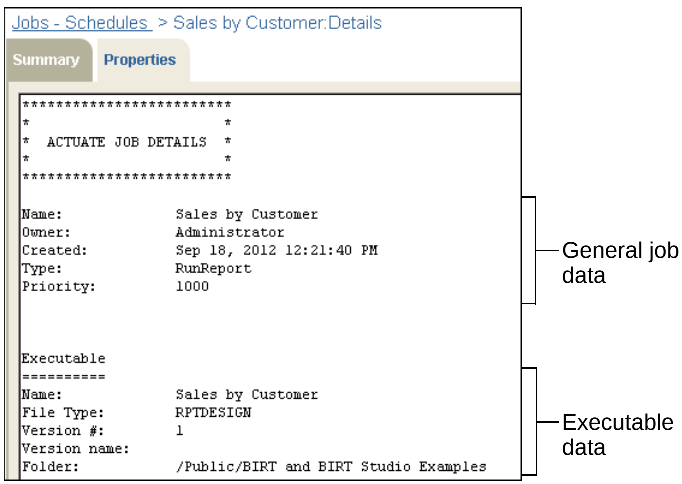


Figure 5-39 Viewing Details—Properties

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 5-40 shows a partial view of Details—Status.

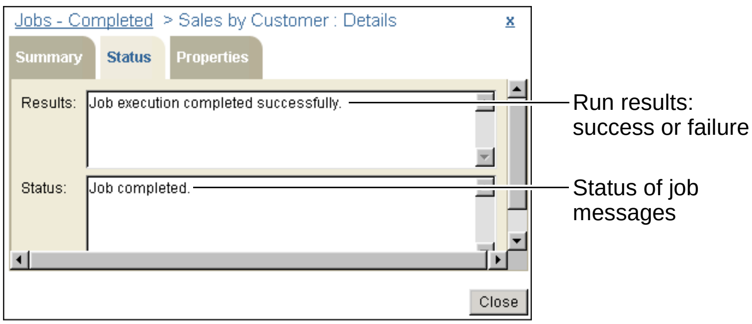


Figure 5-40 Viewing Details—Status

Editing a scheduled job

You can change the settings for any scheduled job before iHub 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 5-41.

Figure 5-41 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 iHub processes it. You cannot recover a deleted job. After iHub processes a job, iHub 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 5-42.

Figure 5-42 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 iHub 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.

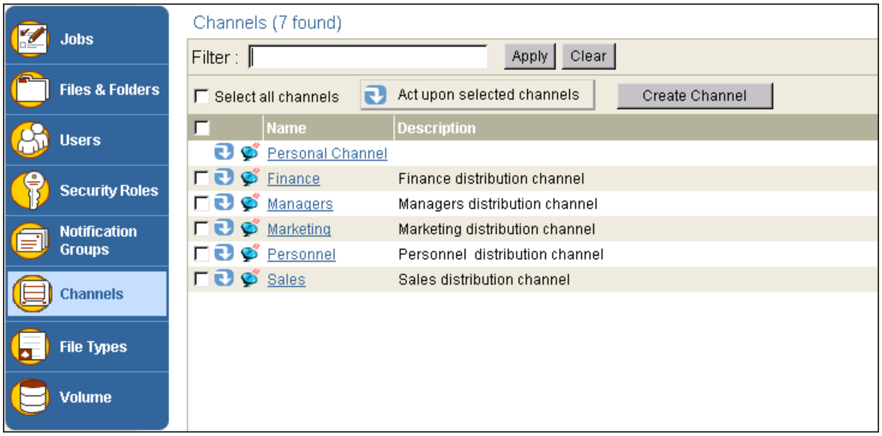


Figure 6-1 Viewing Channels

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 iHub sends job completion notices to a user's personal channel by default, and if so, under what conditions iHub deletes notices. The user can also set these options, on Personal Settings—Jobs. A user scheduling a job can also control whether iHub 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 staff. You create a security role, to which you assign the marketing and finance staff, 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 personnel and support. 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 iHub 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 32x32 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.

iHub requires these properties.

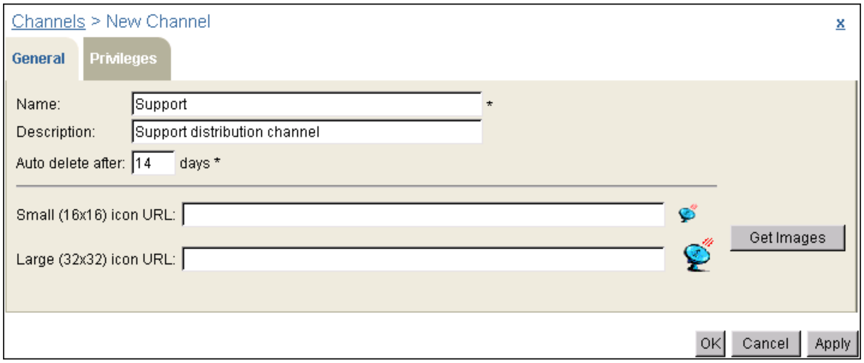


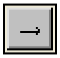
Figure 6-2 Specifying values for properties on New Channel—General

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 privileges. For example, assign read and write privileges on the new Support channel to the Support role, as shown in Figure 6-3.

Choose OK.

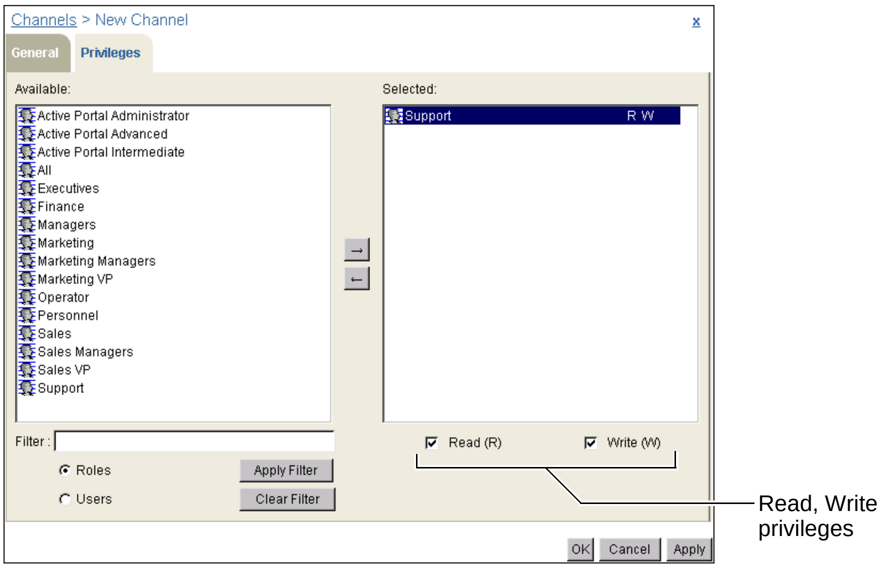


Figure 6-3 Assigning privileges on a new channel

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 properties 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 properties 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.

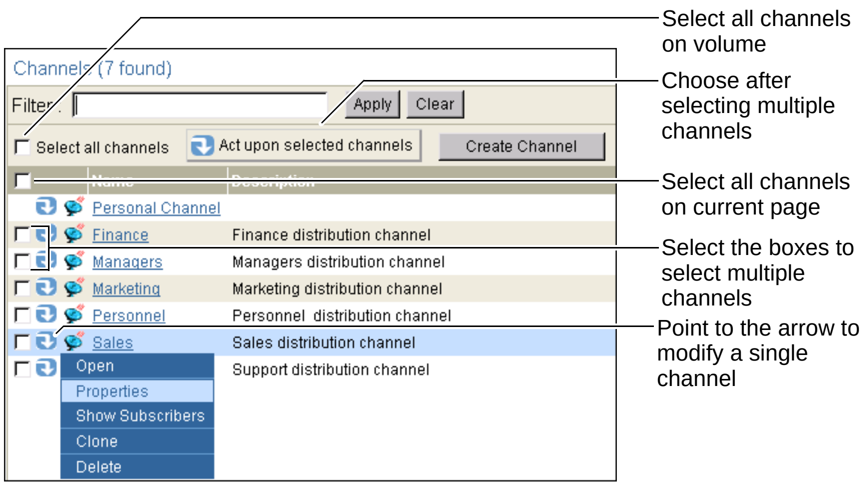
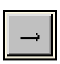


Figure 6-4 Accessing Channels—Properties

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 two or more channels you want to modify. For example, select the Marketing and Sales channel. Then, point to Act upon selected channels and choose Properties, as shown in Figure 6-5.

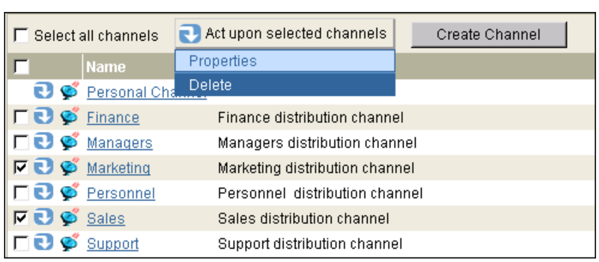


Figure 6-5 Choosing to modify two channels

On Properties, choose Privileges.

2 On Privileges, assign or remove privileges on the selected channels to roles or users by performing the following tasks:

   1 To display the list of roles or users in Available, select Roles or Users.

   2 To remove privileges on the selected channels, move one or more roles or users from Available to Remove these privileges. iHub assigns read and write privileges to a role or user you move to Remove these privileges. Deselect the privileges that you want the role or user to keep.

   3 To add privileges, move one or more roles or users from Available to Add these privileges. With the role or user selected, assign read, write, or both privileges.

   4 To remove all privileges on the selected channels, except privileges you assign in Add these privileges, select Remove all.

For example, assign read privilege on the Marketing and Sales channels to Administrative assistants Agios Georgios and Julia Petrovna, as shown in Figure 6-6.

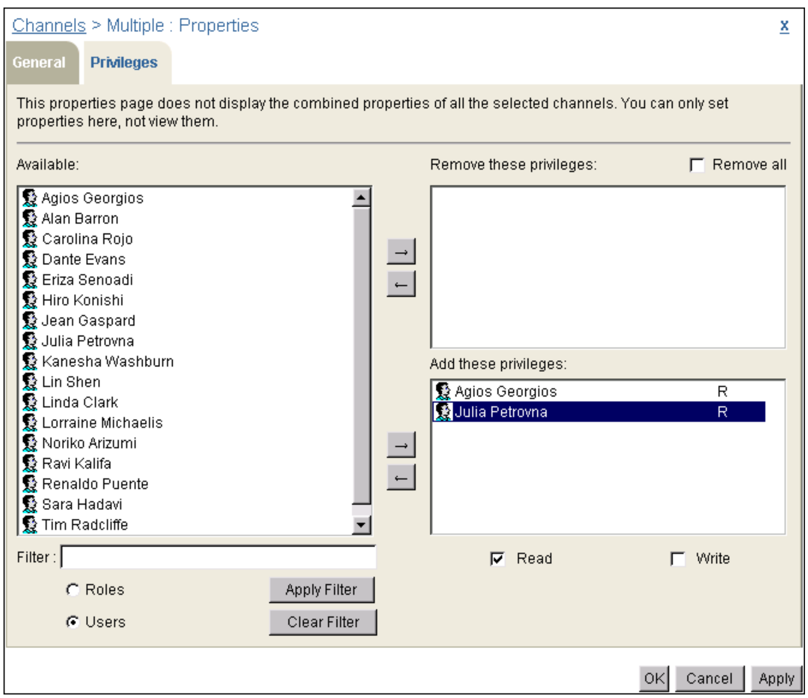


Figure 6-6 Removing and adding privileges on multiple channels

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 6-7.

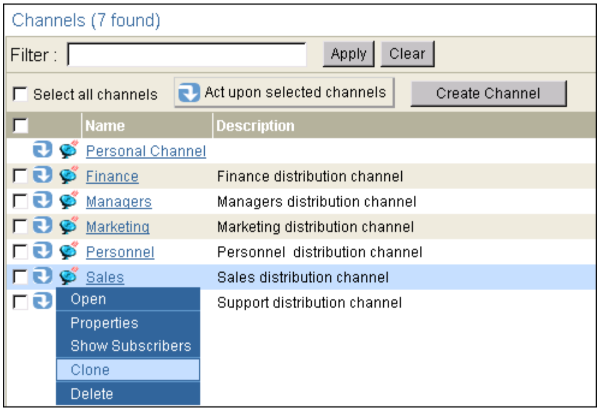


Figure 6-7 Choosing to clone a channel

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, 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 6-8.

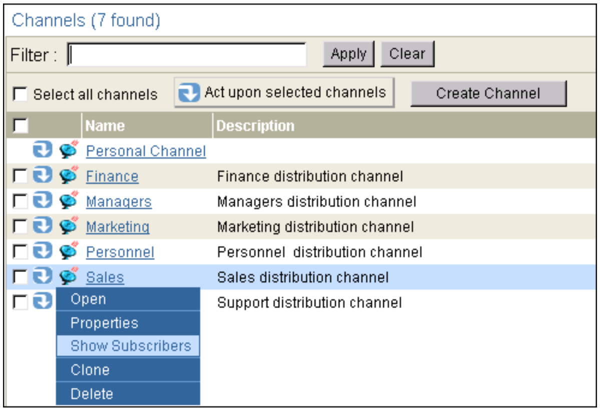


Figure 6-8 Choosing to show subscribers to a channel

Channels—Subscribers displays a list of current subscribers to the specified channel, as shown in Figure 6-9. You cannot add or remove subscribers on Subscribers.

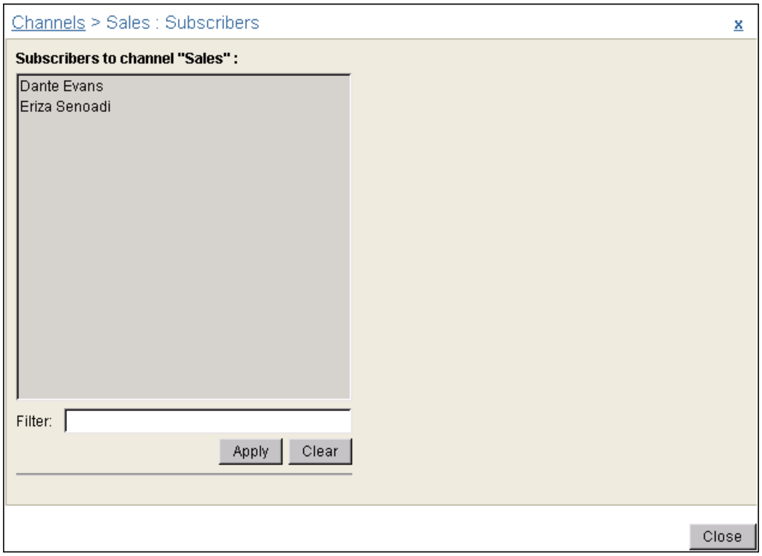


Figure 6-9 Viewing the list of channel subscribers

2 To return to Channels, choose Close.

How to specify a channel icon

You can specify an icon that both iHub and Information Console display next to the name of a channel, as shown in Figure 6-10.

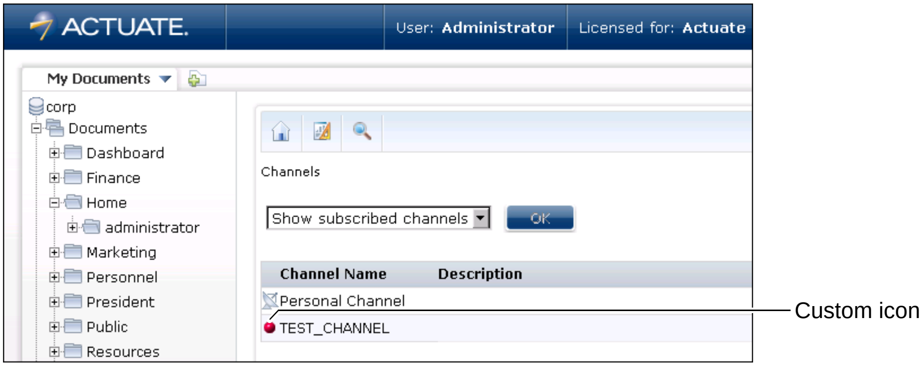


Figure 6-10 Custom channel icon

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

   To create a new channel, choose Create Channel.
4. In Channels—Properties, in Small icon URL, type the URL of the icon. For example, use the following URL as shown in Figure 6-11:

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

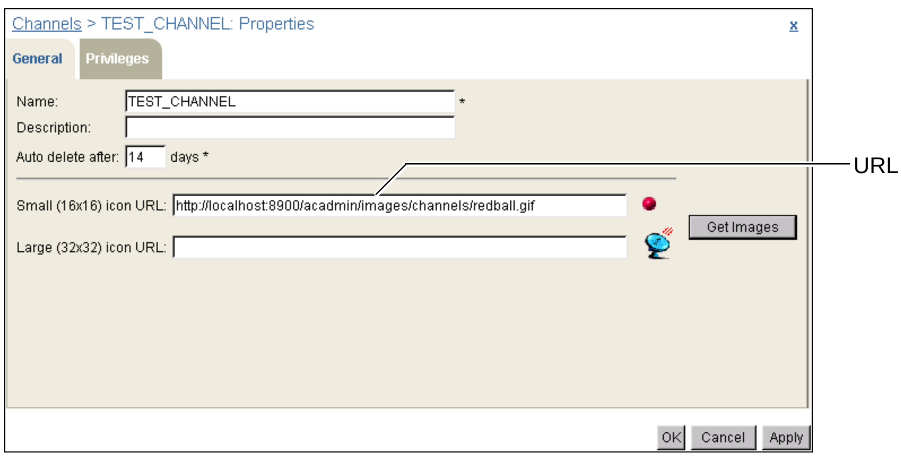


Figure 6-11 Specifying the URL to the icon

5. Choose Get Images. Then, choose OK.

Viewing a document

When iHub generates a document, iHub 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 6-12.

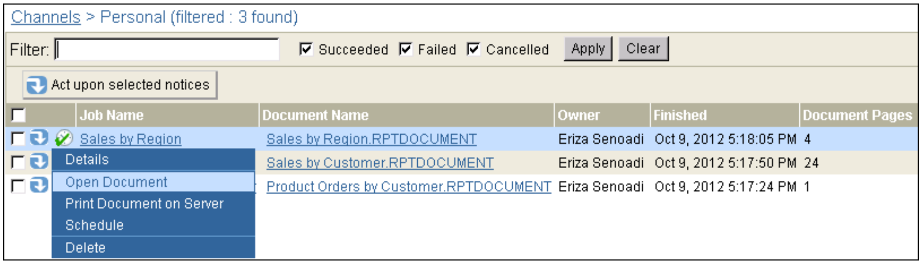


Figure 6-12 Opening a document from a channel

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 the member's 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 6-13.

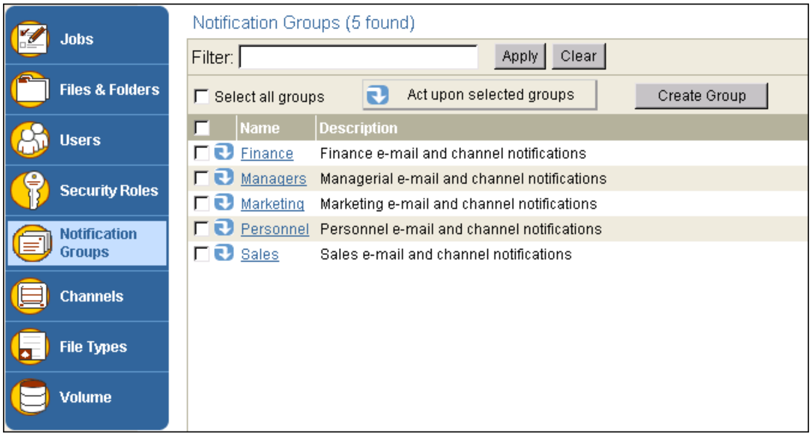


Figure 6-13 Viewing Notification Groups

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 6-14. Optionally, you can type a description.

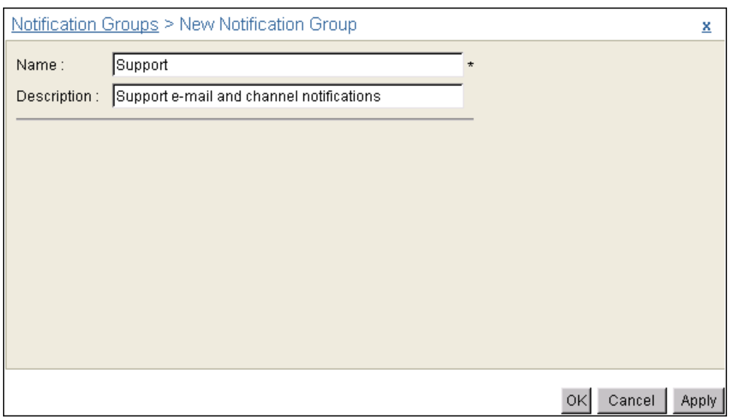


Figure 6-14 Creating a new notification group

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 6-15.

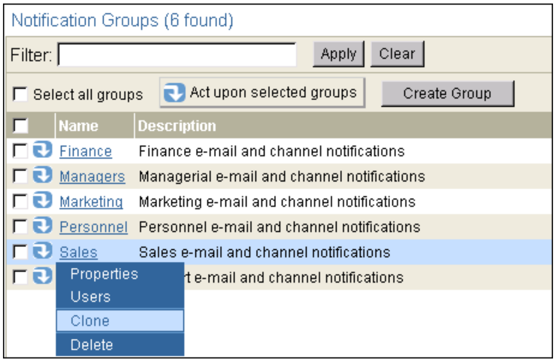


Figure 6-15 Choosing to clone a notification group

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 6-16.

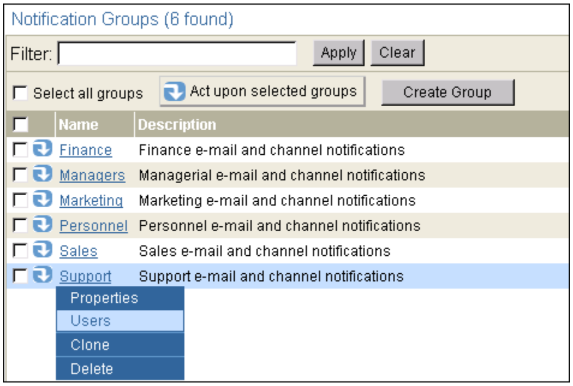


Figure 6-16 Choosing to add or remove users to or from a notification group

2 On Notification Groups—Users, you can add and remove members of the selected group, as shown in Figure 6-17.

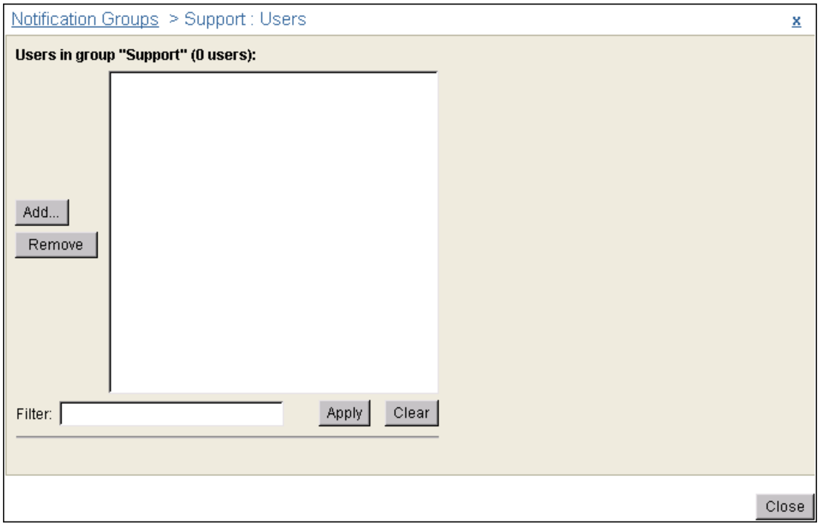


Figure 6-17 Adding or removing users to or from a notification group

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 6-18.

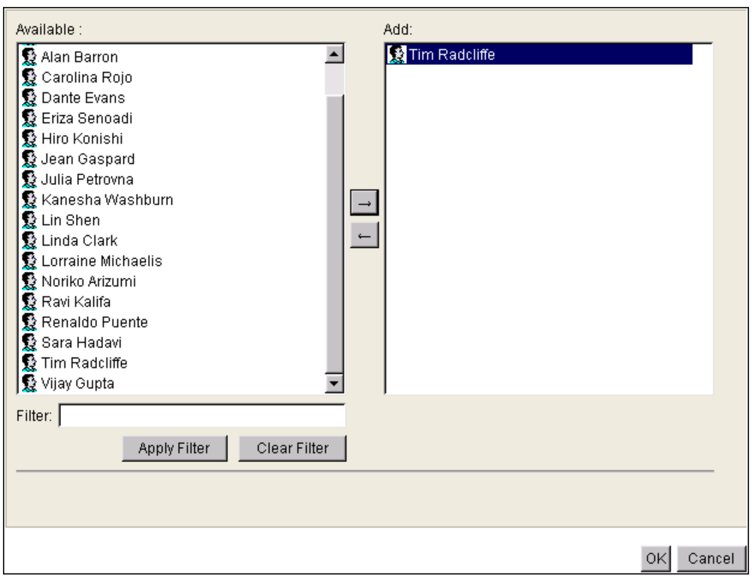


Figure 6-18 Adding users to a group

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 for which you want to add or remove users. For example, select the Marketing and Sales groups, as shown in Figure 6-19. 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.

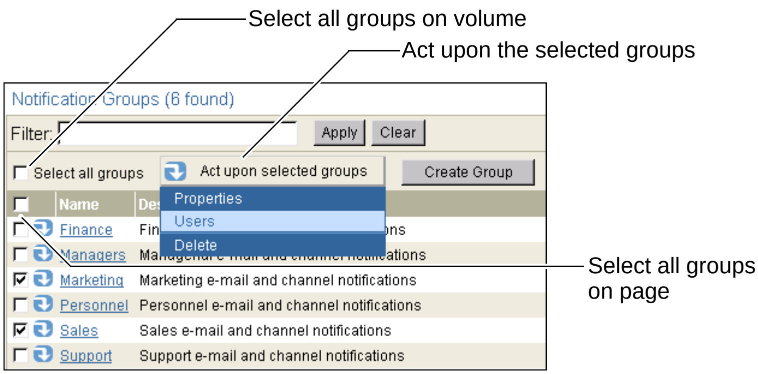


Figure 6-19 Choosing to add and remove users from multiple groups

2 On Notification Groups—Users, perform the following tasks:

- To remove one or more users from the selected groups, move the user or users from Available to Remove these users.
- To add one or more users to the selected groups, move the user or user from Available to Add these users.
- To remove all users from the selected notification groups, except users you add in Add these users, select Remove all.

  For example, add users Agios Georgios and Julia Petrovna to the Sales and Marketing groups, as shown in Figure 6-20.

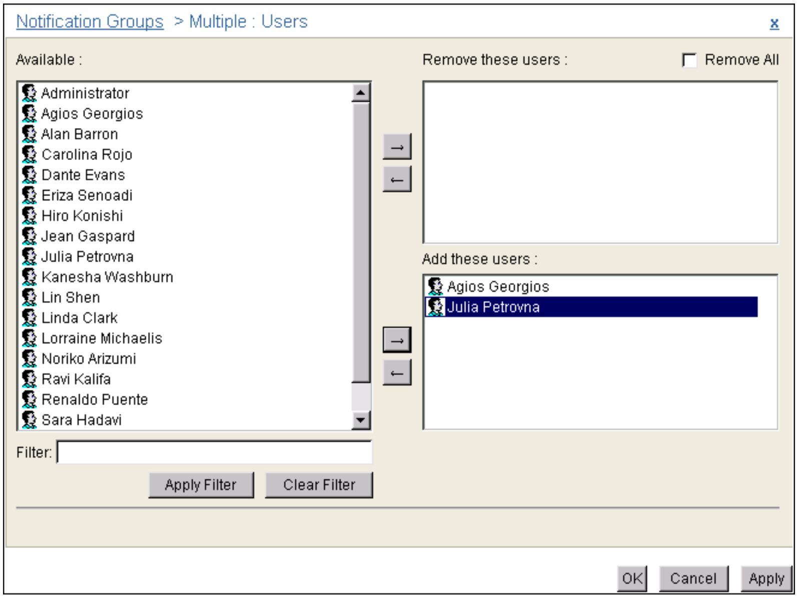


Figure 6-20 Adding and removing users to and from multiple groups

Choose OK.

How to rename a notification group

iHub 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 6-21.

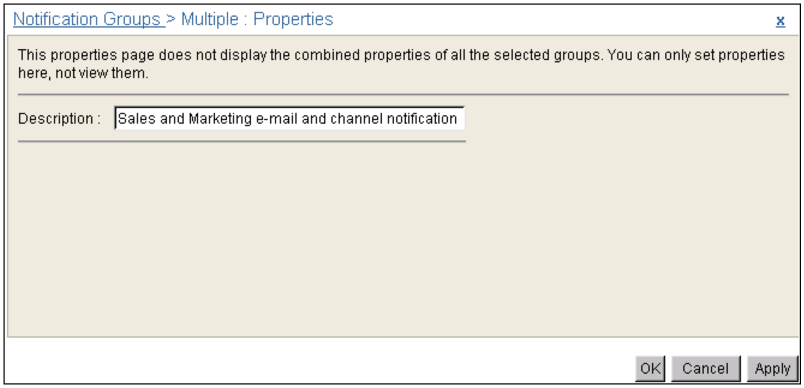


Figure 6-21 Properties for multiple notification groups

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 6-22.
- 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 6-22.

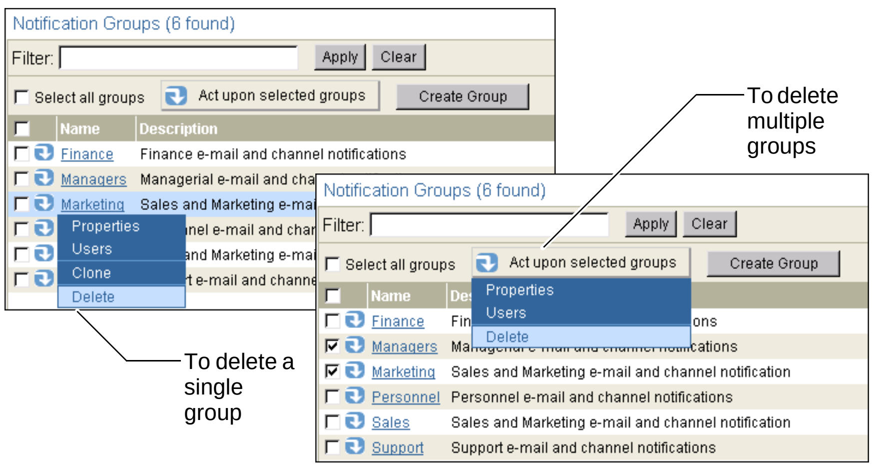


Figure 6-22 Deleting a group

2 Confirm the deletion.

Chapter

7

Managing volume-level operations

This chapter contains the following topics:

- Working at the volume level
- Archiving files and removing empty folders
- Setting web browser defaults
- Setting volume privileges
- Setting volume-level printer options

Working at the volume level

To access the Volume pages of Management Console, choose Volume from the side menu, as shown in Figure 7-1.

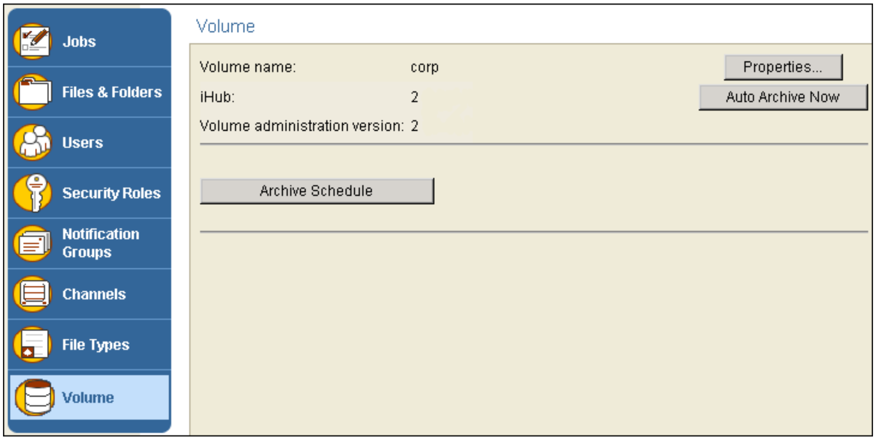


Figure 7-1 Viewing Volume

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.

Figure 7-2 shows Volume—Properties—General as well as the other properties for Volume.

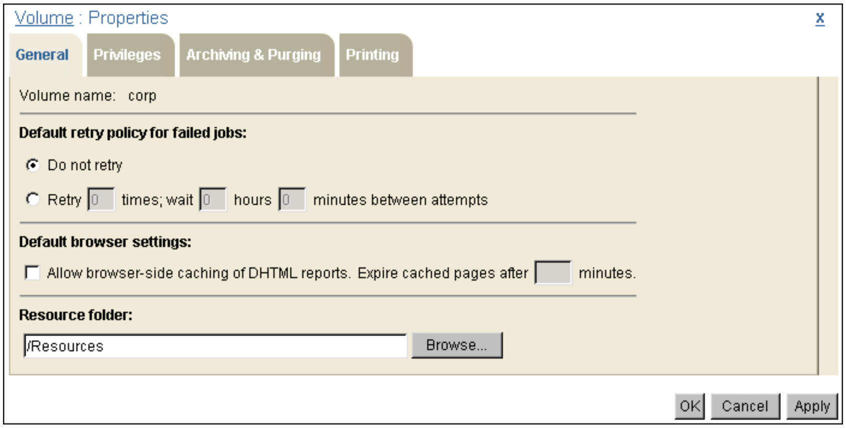


Figure 7-2 Volume—Properties—General

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 7-1 shows the limits for the Encyclopedia volume.

Table 7-1 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 7-1 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 iHub 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 files and folders.
- 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, iHub 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>.

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 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, iHub performs an autoarchive sweep once daily. You can specify when and how many times to perform an autoarchive sweep in a day.

When iHub performs autoarchiving, it starts from the Encyclopedia volume's root folder. For each file whose age has expired, iHub deletes the file. If the Archive files before deletion option is selected, iHub calls the archive application for the Encyclopedia volume, then deletes the file if the archive process succeeds. If the archive process fails, iHub 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 iHub and an external archiving tool.

You can use an archive application that calls the online archive SOAP-based API. iHub ships with a configurable, Java-based Encyclopedia volume autoarchive application that uses the SOAP-based autoarchive API.

When iHub performs autoarchiving, it loads the archive application. If a file autoarchive policy specifies deletion and includes the Archive files before deletion option, iHub exports the file to the external archiving tool.

iHub 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, iHub deletes the file. If the archiving fails, iHub does not delete the file.

Setting the volume's autoarchiving and purging rules

On Volume—Properties—Archiving and Purging, shown in Figure 7-3, 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, 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. iHub retains the values you set for multiple file types and applies the values when you choose OK.

Figure 7-3 shows settings for an autoarchive policy on Volume—Properties—Archiving and Purging.

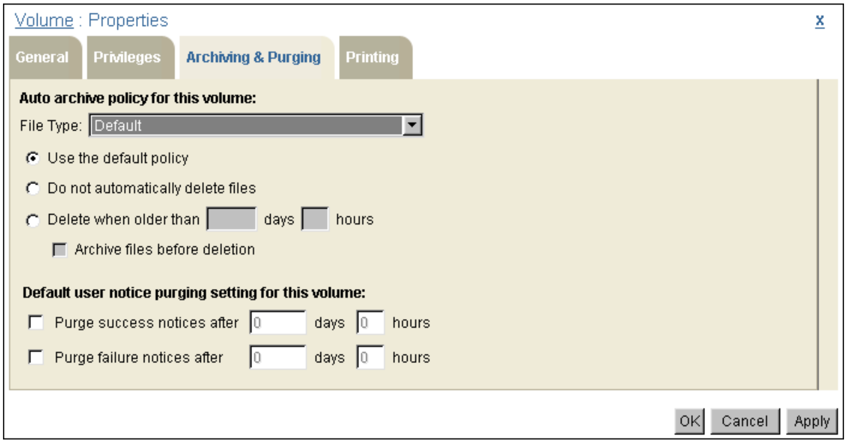


Figure 7-3 Viewing Volume—Properties—Archiving and Purging

Volume—Properties—Archiving and Purging also displays the settings for the volume's default purging policy. Using the options described in Table 7-2, the administrator sets the volume default policy specifying how long a job completion notice remains on a user's personal channel before iHub can delete the notice.

Table 7-2 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 iHub 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 iHub 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 7-1.

How to stop an autoarchiving cycle

When iHub is running an archive sweep on an Encyclopedia volume, you can stop the process from Volume, using Stop Archive Thread, as shown in Figure 7-4.

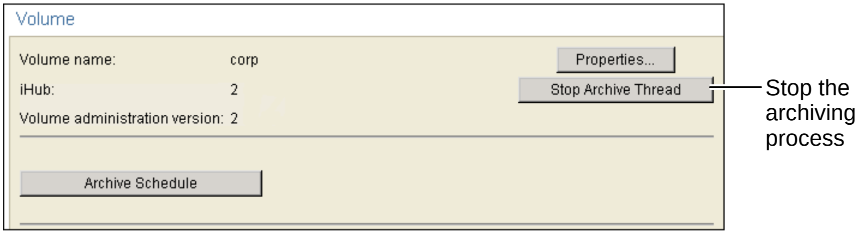


Figure 7-4 Stopping an autoarchive sweep

How to schedule an autoarchiving cycle

Choose Archive Schedule, as shown in Figure 7-4, 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 7-5. 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, iHub does not store DHTML files. You can specify the length of time before the cached pages expire on Volume—Properties—General.

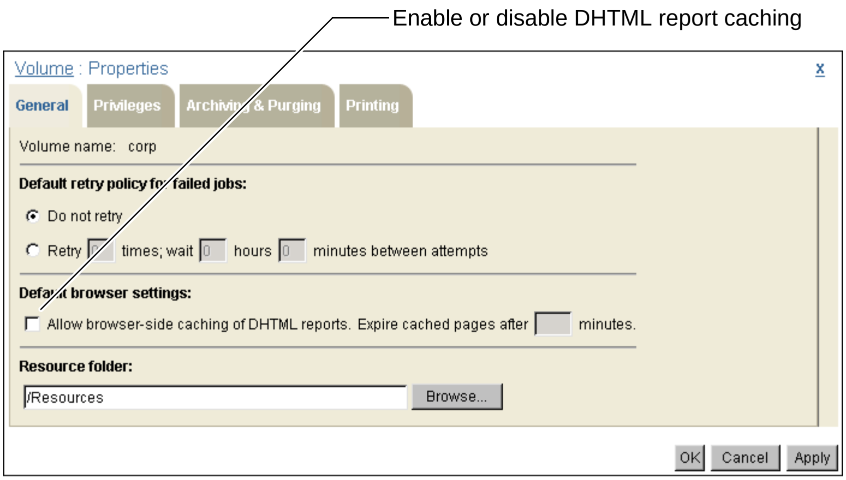


Figure 7-5 Enabling or disabling DHTML report caching

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 7-6 shows the default setting.

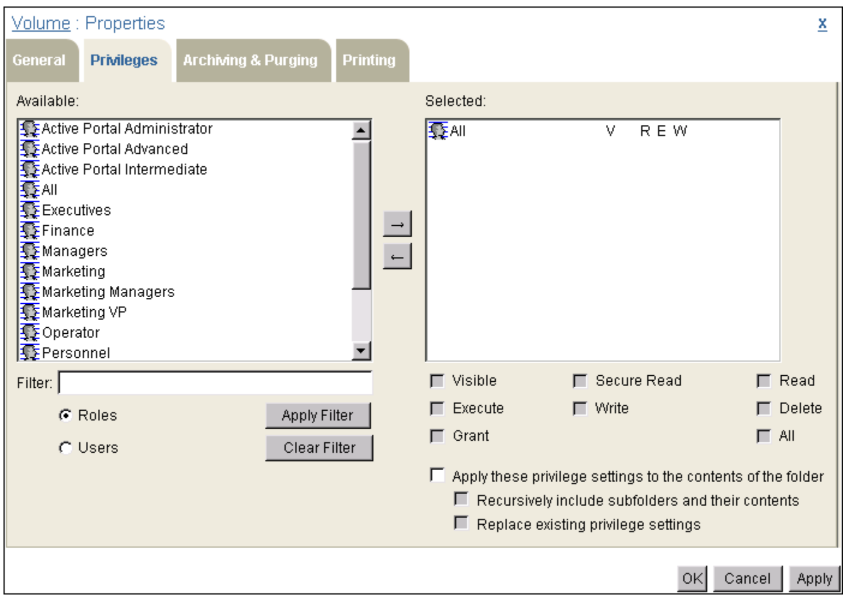


Figure 7-6 Viewing Volume—Properties—Privileges

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 iHub. 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 7-3 describes these properties.

Table 7-3 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.
2-Sided printing	Select: ■ 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, iHub 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, iHub 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, iHub uses the page size that the scheduled design or document specifies. iHub does not use the Encyclopedia volume default setting.

Figure 7-7 shows how iHub determines which printer properties to use for a print job.

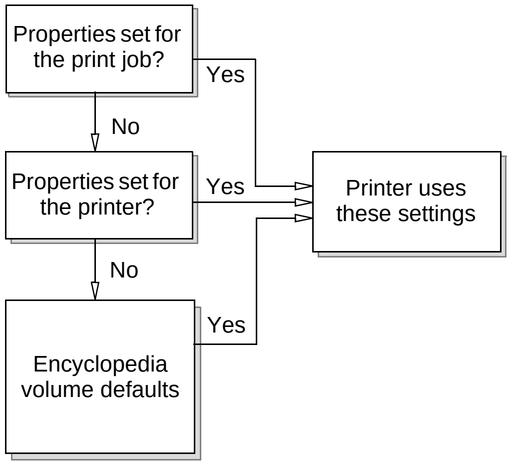


Figure 7-7 Precedence for printer properties

Using Volume—Properties—Printing, an administrator can set property values for any iHub 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 7-8.

   If available, 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.

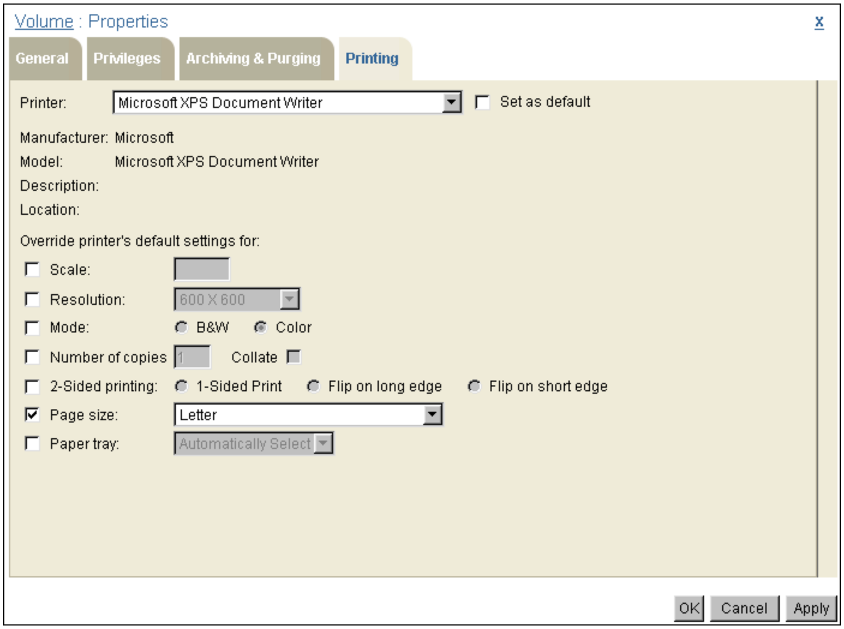


Figure 7-8 Setting print properties on Volume—Properties—Printing

Chapter

8

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 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 8-1.

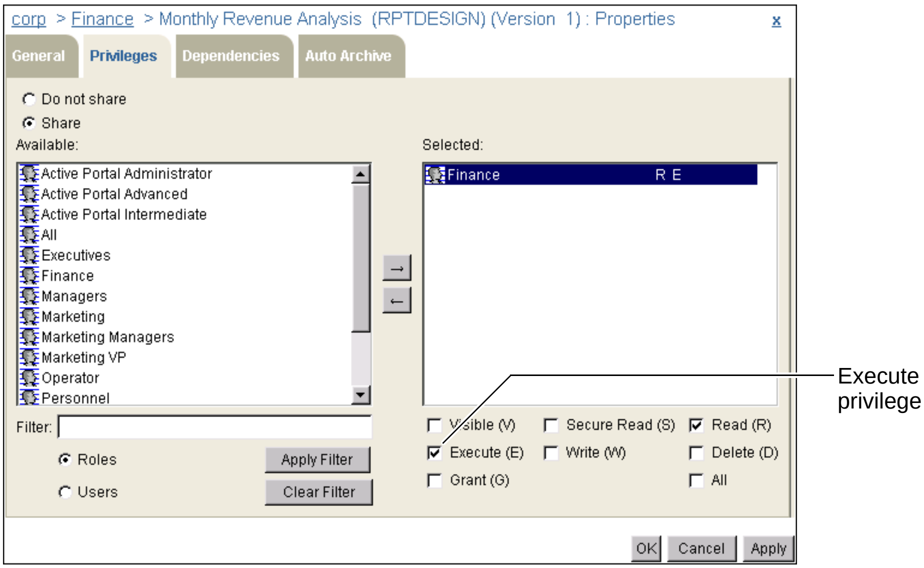


Figure 8-1 Assigning a privilege to a security role

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, iHub must have BIRT Page Level 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 option

You purchase a license to use Page Level Security to restrict user access to specific pages of a BIRT document. Users or security roles that have the secure read privilege can read specific pages of a document protected by page-level security.

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 the 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 8-1 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.

Table 8-1 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
Deleting a folder	Visible—folder Delete—folder Delete—files in the folder
Deleting a file	Visible Delete
Downloading contents of a document	Read
Downloading a document with restricted content	Read and Execute
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 iHub printer	Visible Read
Reading contents of a document	Read
Reading restricted contents of a document	Secure read

Table 8-1 Privileges to access files and folders

Tasks	Required privileges
Running or scheduling a design to run	Read, secure read, or visible—design Execute—design Delete—pre-existing document file if the run replaces it
Running a document with restricted content	Secure read—document
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 the properties of an item	Visible, Read, or Secure read

Table 8-2 lists the privileges that a user needs to perform typical tasks in channels.

Table 8-2 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, iHub does not check the privileges of any data sources that the information object uses. If the user has only execute privilege, iHub checks the privileges of the underlying data sources before it runs the information object. Figure 8-2 shows an example of iHub 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, iHub checks privileges on MyObject and Source1. iHub does not check privileges on Source2.

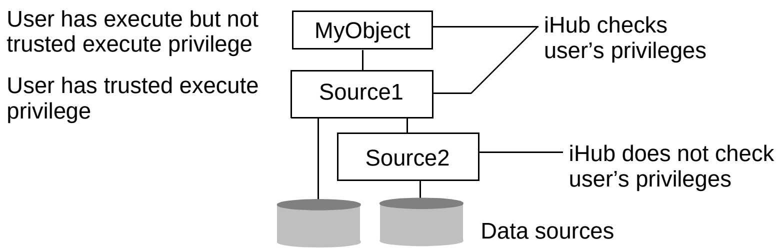


Figure 8-2 Using trusted execute privilege

In Files and Folders, the administrator can set the trusted execute privilege on Properties—Privileges for an information object, as shown in Figure 8-3. iHub removes the trusted execute privilege when you update or copy an object.

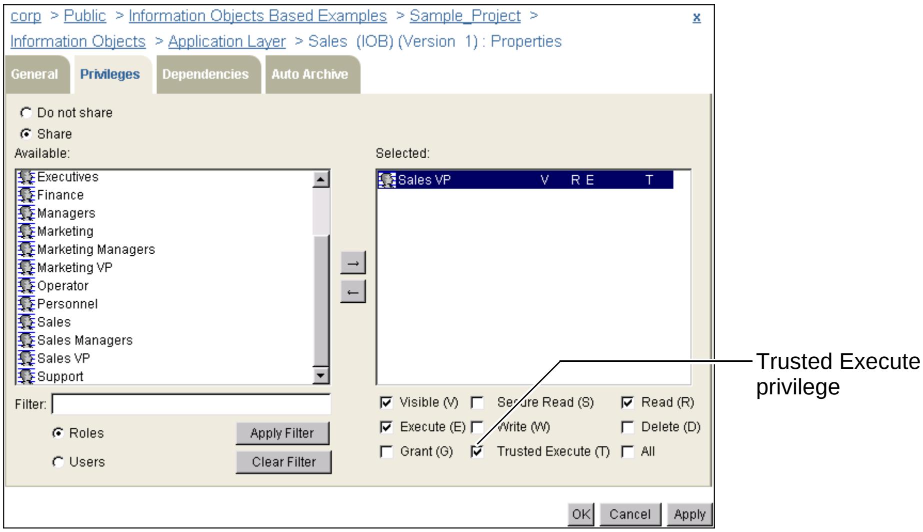


Figure 8-3 Assigning trusted execute privilege to a role

Using page-level security

BIRT Page Level Security option supports page-level security for BIRT designs (.rptdesign). 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. iHub uses this list to generate the access control list (ACL) for each document page.

Viewing documents 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 iHub 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 a shared document, the administrator must assign BIRT Page Level Security option and secure read privilege to a user or role. This option and privilege gives the user or role access to the parts of the document the user or role has the authorization to view, and the ability to run the document. A user typically runs a document to convert its format, for example, from .rptdocument to PDF.

If a user or security role has read privilege on a document that uses page-level security, the user or role has authorization to 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 pass-through security with an Encyclopedia volume security role, the role must have only individual users as members. iHub 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 8-4.

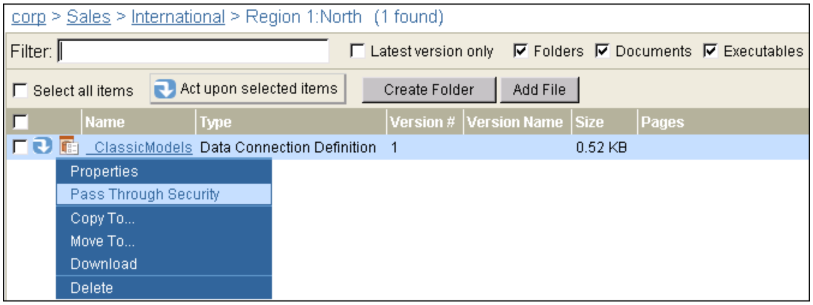
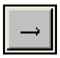


Figure 8-4 Configuring a DCD for pass-through security



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 8-5.

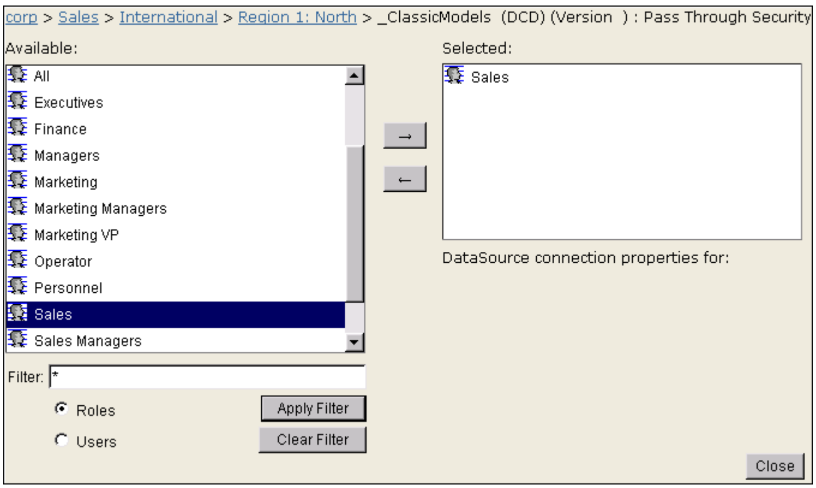


Figure 8-5 Specifying security roles or users

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 8-6. 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 8-6.

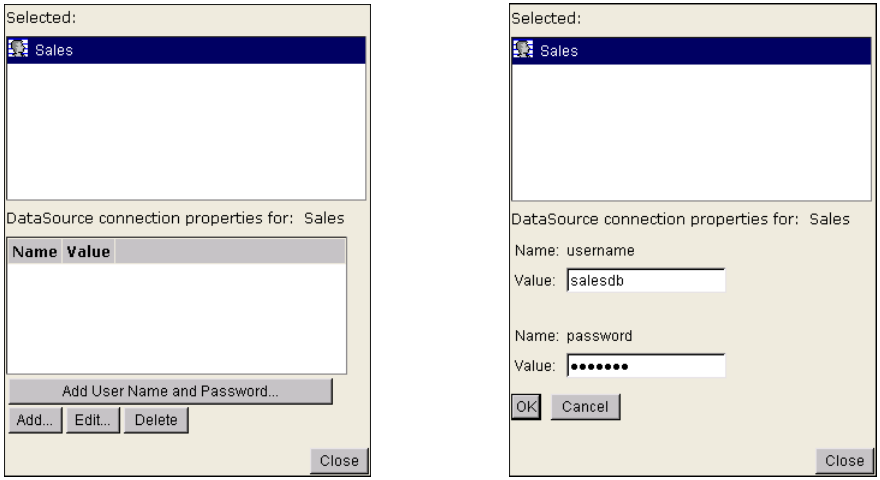


Figure 8-6 Setting data source connection properties

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. Then, select the name and value to edit and choose Edit, as shown in Figure 8-7.

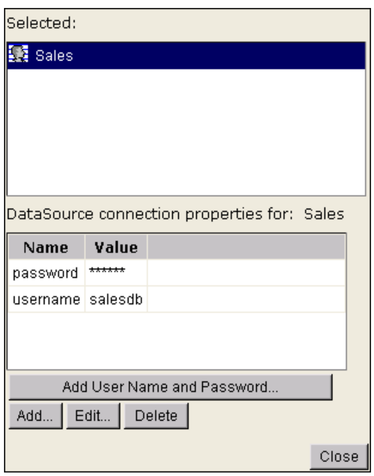


Figure 8-7 Editing data source connection properties

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, iHub 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, iHub 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. iHub can use internal security functionality or an RSSE application to use external security information. In either situation, iHub uses privileges to control access to Encyclopedia volume information.

Actuate provides a set of applications that use a Java RSSE service in \Actuate\ServerIntTech2\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 \Actuate\ServerIntTech2\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 \Actuate\ServerIntTech2 \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 documents 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 document 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 iHub list to an application-specific access control list. You can see this type of application using a Java RSSE service in \Actuate\ServerIntTech2\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 iHub Integration Technology*.
- In the directory into which Server Integration Technology installs, see \Java Report Server Security Extension\LDAP\readme.txt. iHub Integration Technology typically installs into Program Files (x86)\Actuate\ ServerIntTech2 on Windows platforms and /ServerIntTech on Linux platforms.

Open Security levels

Open Security can be configured for one of several levels of use. Table 8-3 lists and describes all Open Security levels.

Table 8-3 Open Security levels

Level	Description
Open Security not used	The Encyclopedia volume stores information such as users, security roles, notification groups, and privileges.

(continues)

Table 8-3 Open Security levels (continued)

Level	Description
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 iHub 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 iHub:

- 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, iHub 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 designs, 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 designs, 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 designs 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, iHub 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 iHub, 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 create and delete an auto archive schedule and execute an auto archive sweep. 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 iHub, iHub 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, iHub 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 8-8 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.

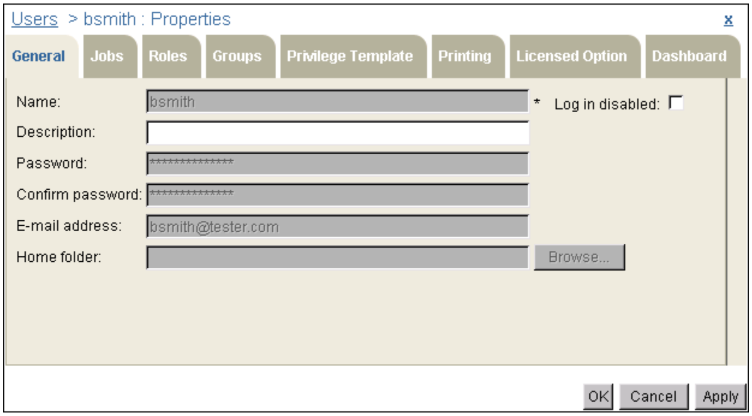


Figure 8-8 Viewing externally defined properties

About searching when using an RSSE application

iHub 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, iHub 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 security

Using the Report Server Security Extension (RSSE) and page-level 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 a BIRT 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

A

B

C

D

E

F

M

N

O

P

R

S

T

U

V

W