IBM OpenPages GRC Platform
Version 6.1.0

Administrator's Guide

Note
Before using this information and the product it supports, read the information in "Notices" on page 639.

Product Information

This document applies to IBM OpenPages GRC Platform 6.1.0 and may also apply to subsequent releases.

Contents

Document Release and Update Information

This topic lists information about this document and where updates to this document can be found.

Document Release Information

Software Version: 6.1.0

Document Published: May 2012

Last Modified: May 4, 2012

Document Updates

You can download the latest revision of this document from the IBM information server at http://www.ibm.com/support/docview.wss?uid=swg27023798.

Chapter 1. Introduction

This Administrator's Guide provides information and instructions for maintaining and administrating the IBM® OpenPages® GRC Platform application. Topics covered include user and group administration, database backup and restoration, customizing the application's look and feel, using the data loader capabilities, and more.

What's New

This section highlights the major new features and enhancements made to this guide for the IBM OpenPages 6.1.0 release.

Table 1. Highlights of 6.1.0 New Features and Enhancements

New Feature or Enhancement	Summary
Long String Fields • "Working with Long String Fields" on page 142 • "Configuring Display Types for Long String Fields" on page 227 • "String Concatentation Utility" on page 378	Long string fields (data type is long string) are considered to be any text of length more than 4000 bytes. Long string fields have two sub-types: medium and large. There four display types for medium long string data: On Demand, On Demand Rich Text, Text Area, and Rich Text. There two display types for large long string data: On Demand, and On Demand Rich Text. String concatenation lets you merge up to 8 simple strings into a new long text field (long string data type).
Filters • "Adding Filters to Object Types" on page 158 • "Using Complex Logic in a Search Filter" on page 162 • "Utilities for Filtering on Long String Field Content" on page 373	The user interface for filter creation has been improved. You can add complex logic to filters to help refine searches using logical operators such as OR, NOT, and parentheses. By default, the system uses only the `AND` operator to return results from a filtered search. You can filter based on the content of long string fields if the Oracle Text feature has been enabled.
Environment Migration • Chapter 17, "Migrating IBM OpenPages Environments," on page 479	If your organization has multiple IBM OpenPages environments, you can use IBM OpenPages environment migration to move both configuration and metadata from one environment to another through the IBM OpenPages application, without needing physical access to either environment. Migration means exporting from a source environment and importing into a target environment.

Table 1. Highlights of 6.1.0 New Features and Enhancements (continued)

New Feature or Enhancement	Summary
Backup and Restore • "Backing Up Custom OpenPages Files" on page 337 • "Running a Live OpenPages Backup" on page 338 • "Enabling and Disabling Storage Backup" on page 341	Custom OpenPages files, such as SiteSync or scheduled job files that are custom to your environment, can be included in the backup using an OpenPages manifest file. A live OpenPages backup means that the OpenPages application can continue running while the backup is in progress. You can disable storage backup by setting the `BACKUP_OP_STORAGE` parameter in the `op-backup-restore.env` file.
Enumerated Strings • "Configuring Display Types for Enumerated Strings" on page 232	For object fields that have an Enumerated String data type, you can configure how enumerated string data displays to users on an object's details page. The display types for Enumerated String data include lists, radio buttons, and check boxes.
Workflow Purge Utility • "About the Workflow Purge Utility" on page 370	The IBM OpenPages Workflow Purge Utility is intended to be run when database administrators want to reduce the size of the workflow database, by selectively removing data related to completed jobs, terminated jobs, and tasks, thereby increasing overall application performance.
Locale Codes • "About Locale Codes" on page 235 • "Setting Localization Options" on page 276	Three new locale codes have been added: Brazilian Portuguese (pt_BR), Simplified Chinese (zh_CN), and Traditional Chinese (zh_TW).
Save as Draft • "Configuring Save As Draft Fields" on page 140	Configure the Save As Draft feature to display a **Save As Draft** button when editing or creating objects so users can save object data without filling in all of an object's required fields.

Change History

This section lists content changes or corrections made to this book since its last publication. Content changes are cumulative and are reflected in the latest publication.

Note: The numbers in brackets after some entries, such as [QC12345], are for internal tracking use only.

Table 2. Documentation Change History

Section and Page	Change or Correction
" IBM OpenPages Application Permissions" on page 20	ExportConfiguration and ImportConfiguration are application permissions that allows members of the user group to access the environment migration tool to export configuration items for import into another system. [RTC208616]
"About Platform Object Types" on page 144	The SOXProject object type is for **system use only**; it is the "master" parent object type for all top level Business Entities and top level Milestones. [RTC218275]
"Enabling Associations Between Object Types" on page 148	You must be in System Administration Mode (SAM) before enabling associations. [QC13496]
"Associating a File Type with an Object Type" on page 154	File extensions specified for File Types associated with SOXDocument object types are case sensitive. [QC13731]
"Adding Filters to Object Types" on page 158	The user interface for filter creation has been improved. [RTC160963]
"About Configuring Fields in Detail and Activity Views" on page 215	The **Export to Excel** function has been renamed as the **Export** function. [RTC193078]
"About Oracle Data Pump" on page 330	Only IMPDP and EXPDP commands are valid. IMP and EXP are not supported. [QC13089]
"Changing the Oracle WebLogic Password for the IBM OpenPages and Workflow Accounts" on page 394	The procedure to change the Oracle WebLogic passwords for OpenPages and Workflow accounts has been updated. [PM59547 QC13942]
"Encrypting Database Passwords in the Backup-Restore Utility Environment Files" on page 334	Added the procedure to encrypt passwords in `op-backup-restore.env` and `op-cc-backup-restore.env` environment files if the passwords are changed. [PM60262 QC13962]

Table 2. Documentation Change History (continued)

Section and Page	Change or Correction
"Backing Up Custom OpenPages Files" on page 337	Added the procedure to backup custom files. [RTC220921]
"Changing the IP Address of an Application Server" on page 398	Added the procedure to change a server IP address for an application server. [SFDC53097 QC12458]
"Import the Production Data into the Test Environment" on page 359	The Oracle Data Pump command IMPDP is used as the IMP command is not supported. [QC13089]
"Internet Explorer 8 Security Issues and Running Reports" on page 443	To run reports on IE8, modify the options of the **Trusted Sites** zone and set the **Enable XSS Filter** property to **Disable** [QC12890]
"Internet Explorer 8 Security Issues and Running Reports" on page 443	Added IE8 custom level properties settings to support Excel reports. [QC13120]
"About Using Parameters in Tasks" on page 494	The name of the server should **not** contain underscores (for example: OP_Host). Issues with connectivity between the Oracle Enterprise Manager and the Oracle WebLogic Server can occur. [QC12758]
"Configuring the Job Launch Manager" on page 546	Added the resource_hierarchy_depth property to the Job Launch Manager property set. [QC11755]
"Remediating Jobs" on page 549	Structural edits to jobs using Interstage BPM Console are not supported. Interstage BPM Console should only be used to view details of a job and to reactivate it as part of job remediation process. [QC14054]
"An Overview of the FastMap Import Process" on page 574	The **Export to Excel** button has been renamed as **Export**. [RTC193078]

Table 2. Documentation Change History (continued)

Section and Page	Change or Correction
"FastMap Parameters for Importing and/or Exporting Data" on page 584	Added the `useSystemNames` parameter documentation to the import and export parameter list for FastMap. [SFDC53849 QC12797]

About the IBM OpenPages GRC Platform

The IBM OpenPages GRC Platform serves as the foundation for a company's enterprise risk management (ERM) efforts by unifying enterprise-wide risk and compliance initiatives into a single management system. With solutions for IBM OpenPages Financial Controls Management, IBM OpenPages Operational Risk Management, IBM OpenPages IT Governance, IBM OpenPages Policy and Compliance Management, and IBM OpenPages Internal Audit, the IBM OpenPages GRC Platform provides a modular and integrated approach to governance, risk and compliance.

Each component provides a highly configurable capability that supports your specific methodology, without having to write custom code, whether in loss events, KRI or any other solution component. The result is that companies can embed risk management into the business and improve outcomes over time.

IBM OpenPages GRC Platform Modules

The IBM OpenPages GRC Platform consists of the following modules:

- **IBM OpenPages Financial Controls Management (FCM)** — provides automated assessment, testing, and certification processes to standardize and manage Sarbanes-Oxley (SOX) compliance enterprise-wide.
- **IBM OpenPages Operational Risk Management (ORM)** — provides a fully integrated operational risk solution, including risk control self-assessments (RCSAs), key risk Indicators, (KRIs), loss event data management, and advanced reporting and business intelligence with IBM Cognos® finance integrated risk management. Dashboard components are available to provide an enterprise-wide view of risk across the business and manage Basel II AMA compliance in the banking industry.
- **IBM OpenPages IT Governance (ITG)** — provides a risk-based, policy-driven approach to managing risk and compliance initiative for the IT organization.
- **IBM OpenPages Policy and Compliance Management (PCM)** — provides an integrated solution for reducing the complexity of complying with numerous industrial, ethics, privacy, and government regulatory mandates.
- **IBM OpenPages Internal Audit Management (IAM)** — provides an integrated audit management solution to manage the full life cycle of internal audits.

How Can the IBM OpenPages GRC Platform Help Me?

The IBM OpenPages GRC Platform application provides many new capabilities to simplify and centralize compliance and risk management activities, including:

Shared Content Management and Common Repository

- Logically presents processes, risks and controls in many-to-many and shared relationships at multiple levels that can be configured to your business processes

- Supports importing existing corporate data and maintains a complete audit trail and version history
- Ensures consistent regulatory enforcement and monitoring across multiple regulations.

Dynamic Decision Support with CommandCenter

- Delivers rich, interactive, real-time executive dashboards and reports
- CrossTrack enables drill-down from reports into supporting reports as well as the underlying detail data
- Provide organizational assurance for regulatory compliance

Simple Configuration and Localization

- Detail user-specific tasks and actions on a personal home page
- Reduce training costs with intuitive navigation, easy-to-use web-based layout and localized text in English, French, Italian, Spanish, German, Japanese, Simplified Chinese, Traditional Chinese, and Brazilian Portuguese.
- Lower administration costs with simple browser based configuration capabilities managed by administrators for end-users

Flexible Automation

- Robust workflow establishes and automates best practice processes for:
  - Management assessments
  - Process design reviews
  - Control testing
  - Issue remediation
  - Sign-offs and Certifications
- Streamlined compliance procedures and automated sub-certifications without sacrificing risk.

Web Services based integration

- OpenAccess API Interoperate with leading third-party applications to enhance policies and procedures with actual business data
- Reduced total cost of ownership and easy integration with existing corporate compliance management systems

Chapter 2. Administering Users, Groups, and Domains

This chapter explains how to manage IBM OpenPages user accounts and groups using the IBM OpenPages interface.

This chapter contains the following sections:

About Users and Groups

Within the IBM OpenPages application, users and groups are organized under the following top-level groups:

-  **Security Domains** - this top-level group acts as a container for the security domain groups that are automatically created by the system when a business entity or sub-entity is added. You can use security domains to distribute your users and organizational groups so they can be administered by delegated administrators. For an overview of security domains, see "About Security Domains" on page 39.

-  **Workflow, Reporting and Others** - this top-level group acts as a container for organizational groups that are used system wide. Administrators often create organizational groups to organize users and other groups. You can define all your users and group under the **Workflow, Reporting and Others** group and then later associate them to different security domains. For upgrade customers, this top-level group also hosts the groups that existed in prior IBM OpenPages releases.

Note: The term 'groups' in this book includes both organizational and security domain groups unless otherwise specified.

To create and administer users and groups for the IBM OpenPages application, you must have access to an IBM OpenPages user account with administrative privileges. For information about delegating and assigning administrator permissions, see "About Administrators" on page 9.

When a user or group is disassociated from an organizational or security domain group and that user or group is not a direct or indirect member of any other group, then the system will make that user or group a member of a special group called 'Standalone Users and Groups'. Only the Super Administrator will have administrative access to this special group.

Accessing Users, Groups and Domains

Only an OpenPages Super Administrator or a delegated administrator with any administrator permission can access the **Users, Groups and Domains** menu item.

To navigate to a group detail page, the logged in user must be a delegated administrator of that group with at least **Browse** administrative permission. For information about delegating administrator permissions, see "Delegating Administrator Permissions" on page 10.

When you expand a security domain group, only child security domains are displayed. Any organizational groups and users associated with that security domain can be viewed only from the detail page of that security domain group.

Procedure

1. Log on to the IBM OpenPages application as a user with any administrator permission set.
2. From the menu bar, select **Administration** and click **Users, Groups and Domains**.

   Note: To view any organizational groups and users associated with a security domain, navigate to the detail page of that security domain group.

Results

From the **Users, Groups and Domains** page, you can view a list of all users and groups, and access the detail page of an organizational group, security domain group, or user.

Rules for User Names and Passwords

When you create user names, these rules apply:

- The maximum length of a user name is 256 characters

  Important: If you are using Microsoft Active Directory Users and Computers as your LDAP authentication server, the user name is limited to a length of 20 characters. User names that exceed the 20 character limit are truncated to 20 characters. This length limitation does not occur in the LDAP server provided by Sun. For more information about LDAP, see "Configuring the LDAP Authentication Module" on page 51.
- The user name can contain alphanumeric characters and any of the special characters listed in the table below.

Note: If you want to exclude any characters - including special characters - from user names, you can specify these characters in the **Illegal Characters** setting. For details, see "Excluding Characters From User Names" on page 274.

Table 3. Special Characters Allowed in User Names

Allowed Special Character	Description
@	At sign
-	Dash
!	Exclamation point or bang
.	Period or dot
_	Underscore
/	Forward slash
:	Colon
*	Asterisk

Table 3. Special Characters Allowed in User Names (continued)

Allowed Special Character	Description
\	Backslash
"	Double quotation marks
#	Pound sign
%	Percentile mark
?	Question mark
<	Less than
>	Greater than

When you create passwords, these rules apply:

- The maximum length of a password is 32 characters
- Passwords cannot contain spaces

About Administrators

The IBM OpenPages application provides a means to flexibly manage your security. By assigning specific security management permissions to an administrator's user account, you can delegate various security management activities to that administrator. For example, you could set up an administrator for a security domain group (such as a regional or local office) who would only have the ability to reset passwords for that group.

The Super Administrator

The Super Administrator (specified during the install or upgrade process) is a user who has complete access to all objects, folders, Role Templates, and groups in the system. In a new (first-time) installation, the Super Administrator is the only user in the system. In an upgrade installation, customers can enter a new user or select one of the existing users (such as 'SOXAdministrator' or 'OpenPagesAdministrator') as a Super Administrator during the upgrade process.

A Super Administrator can create users, groups, other system administrators, and assign roles. The IBM OpenPages application provides a Super Administrator with the ability to decentralize and delegate administration activities by assigning various roles to users through the use of Role Templates (for details see "Using Role Templates" on page 43) and group administrator permissions (for details, see "Delegating Administrator Permissions" on page 10).

A Super Administrator can also assign an administrator to a security domain or organizational group, without making the administrator a member of that group.

Some examples of the types of administrators a Super Administrator could create are:

- A Regional or Group Administrator - this would be a user with at least one security management permission assigned to perform administrative activities for a security domain or organizational group.
- A Delegated Administrator - this would be a group administrator with certain security management permissions who could, in turn, assign new administrators to the same group or to any of the child groups, granting them the same security management permissions.

- Decentralized Administrators - each group (security domain or organizational) could have an administrator who would have one or more administrators responsible for creating and associating users to that group as well as for enable/disable, lock/unlock, assign roles and reset password operations. A decentralized administrator would be able to perform these operations on all child groups associated to their group but not on other groups in the system.

Important:

- If you change the logon user name and/or password of the OpenPages Super Administrator account after installation (using the application interface), you must manually make corresponding changes to the CommandCenter Framework Generator property file so the reporting framework will update properly. For details, see "Changing the Administrator Logon Account and Framework Generation" on page 65.
- If you are using Microsoft Active Directory Users and Computers as your LDAP authentication server, the user name is limited to a length of 20 characters. User names that exceed the 20 character limit are truncated to 20 characters. This length limitation does not occur in the LDAP server provided by Sun.

Delegating Administrator Permissions

As an administrator, you can delegate various security management activities, such as only managing users or only resetting passwords, to other administrators for organizational and business entity security domain groups (for information about entity groups, see "Understanding Security Context Points" on page 35). If there are child groups under a parent group, the administrator can delegate an administrator for each child group as well.

Administrators do not have to be members of groups for which they perform administrative tasks. By default, only the Super Administrator has Read and Write access to objects in the system. Delegating administration responsibilities to a user on a security domain, does not automatically grant Read and Write access to objects under the corresponding entity.

Important:

- You can only assign those permissions that you have to other administrators.
- If you disassociate an administrator from a security domain or organizational group, all user management privileges (such as manage users, lock/unlock users, reset passwords, enable/disable users, assign roles) are retained by that administrator and are not revoked.

Example

Let's say you want to designate Mary Smith as an administrator who can reset passwords for any users in the Boston Sales Office. You would navigate to the Boston Sales Office entity group detail page and assign the 'Reset Password' permission to Mary Smith's user account.

If there are multiple child groups under the Boston Sales Office entity group, Mary Smith could delegate an administrator for each child group. She would only be able to assign the 'Reset Password' permission to another administrator.

Note:

- Once administrator permissions are assigned to a user, the name of that user is no longer displayed in the user selector list. To modify permissions for an administrator, see “Modifying Administrator Permissions” on page 12.
- Security domain groups are not displayed in the User/Group selector list.

Types of Administrator Permissions

The table below lists the various security management permissions that you can delegate to a security domain or user group administrator.

Table 4. Administrator Permissions

This permission...	Allows the selected user to...
Manage	Create, modify, and associate users and groups.
Lock	Lock a user account, which prevents logon to the IBM OpenPages application from that account. With this permission, a **Lock** button can be selected at the top of the User Information details page.
Unlock	Unlock a previously locked user account. With this permission, an **Unlock** button can be selected at the top of the User Information details page.
Reset Password	Reset passwords for users. With this permission, a **Reset Password** button can be selected at the top of the User Information details page.
Assign Roles	• Assign one or more roles to users and groups. • Revoke a role from a user or group.
Browse	View users and groups within that group. This permission is selected by default.

Example

Figure 1 on page 12 shows a diagram with a sample decentralized security administration structure in which certain administrative permissions have been delegated to users as follows:

1. Jim has all administrative permissions on Company ABC group as well as on all child groups.
2. Ken can create users and associate them to North America and its child groups.
3. Mary can only reset passwords of users who belong to the USA group and its child groups - Boston and New York.
4. Steve has all administrative permissions on all the users and child groups of the Asia Pacific group. However, Steve does not have administrative privileges on the North America and Europe group hierarchies.
5. Tim has all administrative permissions on all the users and child groups of the Europe group. However Tim does not have administrative privileges on the North America and Asia Pacific group hierarchies.

In terms of delegation, Mary could assign an administrator to the Boston or New York group but can only grant the 'Reset Password' administrative permission. However, Jim can assign and grant all administrative permissions to administrators on Boston and New York.

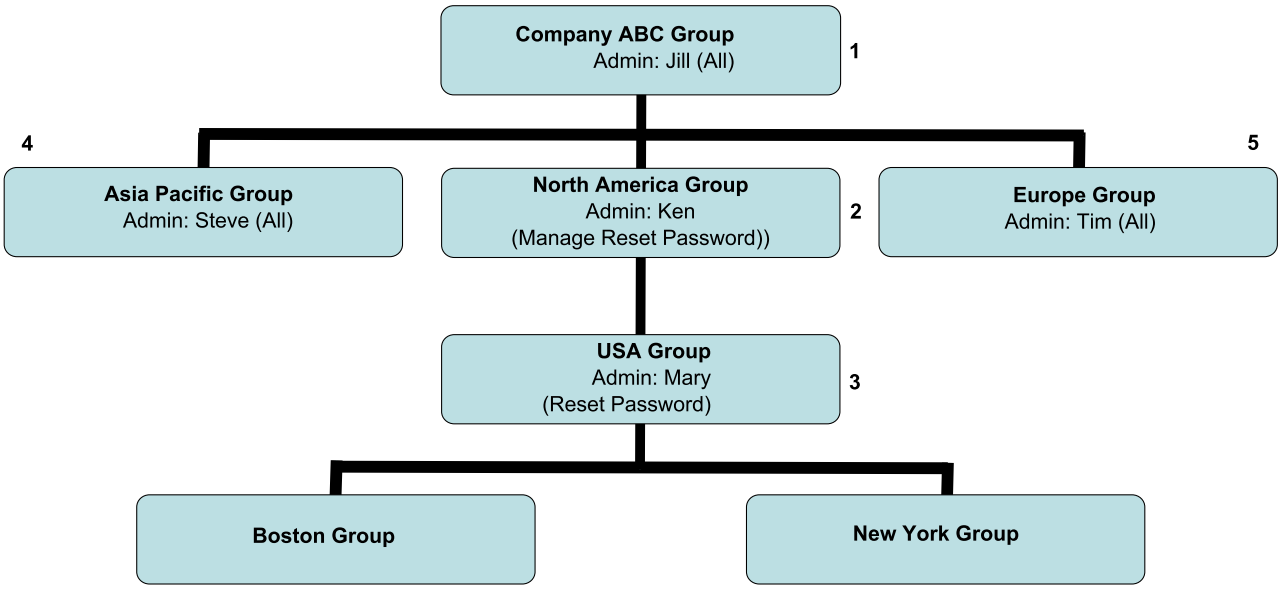


Figure 1. Sample Decentralized Security Administration

Assigning Administrator Permissions

You can assign one or more group administrator permissions to selected users.

Procedure

1. Log on to the OpenPages application as a user with any administrator permission set.
2. From the menu bar, select **Administration** and click **Users, Groups and Domains**.
3. On the **Users, Groups and Domains** page, click the name of the group for which you want to assign administrative permissions to selected users.
4. On the detail page of the selected group, navigate to the **Administrators & Permissions** tab.
5. Click **Assign**.
6. Do one of the following:
   - To select a user, click in the **User** box or click the user icon (if configured).
   - To search for a user, click the magnifying glass icon .
7. In the **Specify Permissions** box, select the administrative permissions you want to assign to this user (see "Types of Administrator Permissions" on page 11 for a list of permissions). To select all permissions, select the **Permissions** box in the column heading.
8. When finished, click one of the following buttons:
   - **Assign** to return to the selected group's detail page
   - **Assign & Next** to assign administrative permissions to another user.

Modifying Administrator Permissions

You can modify administrator permissions assigned to a user at any time.

Procedure

1. Access the **Users, Groups and Domains** page (see “Accessing Users, Groups and Domains” on page 7).
2. On the **Users, Groups and Domains** page, click the name of the group for which you want to modify administrative permissions.
3. On the detail page of the selected group, navigate to the **Administrators & Permissions** tab.
4. From the list of administrative users, click the  (pencil icon) next to the user whose permissions you want to edit.
5. In the **Specify Permissions** box, select or clear administrative permissions for this user as wanted (see “Types of Administrator Permissions” on page 11 for a list of permissions).
6. When finished, click **Save**.

Revoking Administrator Permissions

You can revoke administrator permissions assigned to one or more users.

Procedure

1. Access the **Users, Groups and Domains** page (see “Accessing Users, Groups and Domains” on page 7).
2. On the **Users, Groups and Domains** page, select the check box next to the name of each user for whom you want to revoke administrative permissions.
3. When finished, click **Revoke**.

Results

The name of the user is removed from the list of group administrators.

Managing User Accounts

This section describes how to configure non-administrative user accounts.

For information about accessing the **Users, Groups and Domains** menu item, see “Accessing Users, Groups and Domains” on page 7.

Note: To configure security for user accounts, see “Configuring Security for User Log On” on page 279. If you are using single sign-on, you can also redirect the log-out link (see “Redirecting the IBM OpenPages Log Off Link” on page 279).

Creating New Users

When creating a new IBM OpenPages user, you must first select the group to which the user will belong, and then enter information about the user and user account.

If you have not created an appropriate group for the new user, you can add them to the top-level **Security Domains** group or **Workflow, Reporting and Others** group. In addition, you can create an "Everyone" or "All_Users" group under the top-level **Workflow, Reporting and Others** group and add all the users to this group. At a later time, you can then associate these users to the required security domains. In this way, there is one group that lists all users. See “Creating a New Organizational Group” on page 17 for details.

If a user will be responsible for adding, editing, or removing folder-based access control (ACLs) using the **Custom Security** menu option on the **Administration** menu, the user should be associated with a group that has the **Access Control Lists** application permission.

Procedure

1. Access the **Users, Groups and Domains** page (see "Accessing Users, Groups and Domains" on page 7).
2. Expand the list of groups until the group to which you want to add the new user is displayed. Click the name of the group to display the group's detail page.
3. Navigate to the **Users** tab that lists all of the users who currently belong to the group, and click **Add New**.
4. Enter the necessary information for the new user account.

   Note: Once the record is saved, you cannot change the user name.

   Important: If you are using Microsoft Active Directory Users and Computers as your LDAP authentication server, the user name is limited to a length of 20 characters. User names that exceed the 20 character limit are truncated to 20 characters. This length limitation does not occur in the LDAP server provided by Sun.
5. Assign the user a profile:
   a. Click the **Profile** arrow.
   b. Select a value from the list.
6. Decide which password behavior below you want to apply to the new user account.

   Note: Skip this step if you are using single sign-on (SSO) or LDAP authentication.

If you select this option...	Then...
User must change password at next log in	The next time the user logs on to the application, the user is prompted to change the password. The new password must be a valid password that satisfies any active strong password policies.
User cannot change password	The **Change Password** button is disabled and the user will be unable to change the password. This option is mutually exclusive with 'User must change password at next login.'
Password never expires	The user will not be prompted to change their password after a period of time.
Password expires in _____ days	After the specified period of time has elapsed, the user will be forced to change their password. This setting is mutually exclusive with the 'Password never expires' and 'User cannot change password' settings.

7. Click **Create**.
8. If the new user account was created:

a. Under an "Everyone" or "All_Users" group, go to “Associating Existing Users with a Group” to give the user access to a business entity.
b. Under a security domain group that corresponds to a particular business entity, go to “Assigning a Role to a User or Group” on page 47 to assign the user access control permissions.

Associating Existing Users with a Group

If a new user only belongs to an "Everyone" or "All_Users" group, you need to give the user access to the appropriate business entity or entities. You do this by associating the user to the security domain group that corresponds to the business entity for which they need access. For information about security domains, see “About Security Domains” on page 39.

Note: Administrators can only associate users with groups to which they have the Browse administrative permission. If you select a group to which you do not have access, an error message is displayed.

Procedure

1. Access the **Users, Groups and Domains** page (see “Accessing Users, Groups and Domains” on page 7).
2. Navigate to the group to which you want to associate an existing user.

   Note: To expand a group hierarchy, click the + (plus) sign next to the group you want. The **Security Domains** top-level group contains the security domain groups for all business entities.
3. From the list of groups, click the name of the group you want.
4. On the detail page of the selected group:
   a. Navigate to the **Users** tab.
   b. Click the **Associate** button.
5. On the Associate Users with Group page:
   a. Expand the list to display the users.
   b. Select the check box next to each user account you want to associate.
   c. When finished, click **Associate**.
6. To assign access control permissions to a user, go to “Assigning a Role to a User or Group” on page 47

Disassociating Users from a Group

Note:

- Disassociating users from a security domain group does not result in removal of their role assignments on that entity. Use 'Revoke' to remove the role assignments of a user on a given entity (see “Revoking a Role From a User or Group” on page 48).
- If you disassociate an administrator from a security domain or organizational group, all user management privileges (such as manage users, lock/unlock users, reset passwords, enable/disable users, assign roles) are retained by that administrator and are not revoked.

Procedure

1. Access the **Users, Groups and Domains** page (see “Accessing Users, Groups and Domains” on page 7).

2. Expand the list of groups and click the name of the group that contains the user you want to disassociate. If you have, for example, an "Everyone" or "All_Users" group under the **Workflow, Reporting and Others** group, you can navigate there to locate the user
3. On the **Users** tab of the selected group:
   a. Select the check box next to each user you want to disassociate from the group.
   b. Click the **Disassociate** button.
   c. At the prompt, click **OK**.

      The name of the user is removed from the list.

Modifying Existing User Accounts

As necessary, you can edit a user account.

Procedure

1. Access the **Users, Groups and Domains** page (see "Accessing Users, Groups and Domains" on page 7).
2. Expand the list until the organizational group or Security Domain that contains the user account is displayed.
3. Click the name of the organizational group or security domain to open its detail page and then click the user name to display that detail page. If you have an "Everyone" or "All_Users" group under the **Workflow, Reporting and Others** group, you can navigate there to locate the user.
4. Click the **Edit...** button at the top of the User Information section. The Edit User Information page is displayed.

   Note: You cannot change a user name.
5. Edit the necessary information, and click **Save** to return to the User detail page.

Disabling User Accounts

User accounts cannot be deleted through the IBM OpenPages application user interface. When a user account is disabled, the user of that account is prevented from logging in, and the user is removed from selection on the user selector list.

Note: If you want to prevent a user from logging in, but still want the user to appear in user selectors, you should Lock the user instead. See "About Locking and Unlocking Objects" on page 293 for more information.

Procedure

1. Access the **Users, Groups and Domains** page (see "Accessing Users, Groups and Domains" on page 7).
2. Expand the list until the organizational group or Security Domain that contains the user account you want to disable is displayed.
3. Click the name of the organizational group or security domain to open its detail page and then click the user name to display that detail page. If you have, for example, an "Everyone" or "All_Users" group under the **Workflow, Reporting and Others** group, you can navigate there to locate the user.
4. Click the **Disable** button at the top of the User Information section. The button text changes to Enable and the value of the Status field changes to Inactive.

Enabling User Accounts

You can re-enable a disabled user account.

Procedure

1. Access the **Users, Groups and Domains** page (see “Accessing Users, Groups and Domains” on page 7).
2. Expand the list until the organizational group or Security Domain that contains the user account you want to enable is displayed.
3. Click the name of the organizational group or security domain to open its detail page and then click the user name to display that detail page. If you have, for example, an "Everyone" or "All_Users" group under the **Workflow, Reporting and Others** group, you can navigate there to locate the user.
4. Click the **Enable** button at the top of the User Information section. The button text changes to Disable and the value of the Status field changes to Active.

Managing Organizational Groups

This section describes how to configure organizational groups.

For information about accessing the **Users, Groups and Domains** menu item, see “Accessing Users, Groups and Domains” on page 7.

Creating a New Organizational Group

To more easily find a specific user without browsing through multiple groups and subgroups, it is recommended that you create an "Everyone" group (or other suitable name) as a sub-group of the **Workflow, Reporting and Others** group.

This is useful since normally you create IBM OpenPages users in the context of a group, and then add them to multiple groups directly. This means that in order to find an existing user, you need to know a group to which the user belongs. To help this process, follow the suggestions below.

As you create your list of IBM OpenPages users, add them directly to the "Everyone" group as well as the functional groups they will belong to. In this manner, to find a specific user quickly, you can open the "Everyone" group and select the user directly.

If you want to deny a user access to the IBM OpenPages application by removing him from all groups, you will need to remove him from the "Everyone" group as well.

Note: If you have set up your security access controls for your groups and users, it is important that the "Everyone" group is not granted access control to your IBM OpenPages data. Otherwise, the access permissions of the "Everyone" group may override your security settings. The "Everyone" group is merely a convenience to help administrators quickly find a specific user and modify their information.

Users with the correct permissions can create groups using the User/Group interface. Groups can contain other groups and users, and inherit application permissions from the groups that they belong to.

Procedure

1. Access the **Users, Groups and Domains** page (see “Accessing Users, Groups and Domains” on page 7).

2. Expand the list and click the name of the group to which the new group will belong. If there is no higher-level group for the new group, select the root **Security Domains** or **Workflow, Reporting and Others** group.
3. On the detail page of the selected group, navigate to the **Groups** tab and click **Add New**.
4. Fill in the required information for the new group and click **Create**. The parent group's detail page is displayed with the new group listed in the Sub-Groups section.
5. Click the name of the new group to view the detail page if you want to add users to the group or modify the group permissions.

Disassociating a Group

When you disassociate a group and that group does not belong to any other IBM OpenPages group, the group will be listed under the special group named **Standalone Users and Groups**, which is under the top-level **Workflow, Reporting and Others** group.

When adding an existing group to another group, the disassociated group will still be available in the group selector list.

Procedure

1. Access the **Users, Groups and Domains** page (see "Accessing Users, Groups and Domains" on page 7).
2. Expand the list and click the name of the group to which the soon-to-be-disassociated group belongs. The detail page of the group is displayed.
3. Navigate to the **Groups** tab and select the check box next to each group to be disassociated.
4. When finished, click **Disassociate**. A confirmation box is displayed.
5. Click **OK** in the box to disassociate the selected groups.

Associating a Group

You can associate groups to each other.

Procedure

1. Access the **Users, Groups and Domains** page (see "Accessing Users, Groups and Domains" on page 7).
2. Expand the list of groups and click the name of the group to which you want to associate another group. The detail page of the selected group is displayed.
3. Navigate to the **Groups** tab and select the check box next to each group to be associated
4. When finished, click **Associate**.

Configuring Application Permissions

IBM OpenPages provides a set of application permissions that administrators can use to limit the activities of the various user groups that can access the IBM OpenPages application.

Defining Application Permissions

You can define application permissions within the IBM OpenPages application interface as follows:

- In **Role Templates** - this is the preferred method for granting users or groups application permissions.

  Note:

  – Both application permissions and ACLs are included in the role definition process. When a role is assigned to a user or a group on any business entity or security context point, that user or group automatically acquires the application permissions defined in that Role Template.

  – When a user or group is assigned multiple roles, the user or group accumulates the application permissions that are defined in the various roles. Application permissions are granted by the role (not the security context point) and apply in all situations where the user has the correct ACL access. For example, users with Read permission to Business Entities and the **Audit Trail** application permission will be able to view the Change History (audit trail) for those Business Entities.

  For more details, see "Using Role Templates" on page 43.

- As part of an organizational group definition - this method is provided for backward compatibility for upgrade customers and for administering system-wide organizational groups. Organizational groups can be created under the **Workflow, Reporting and Others** root folder on the **Users, Groups and Domains** page. For more details, see "Managing Organizational Groups" on page 17.

Understanding Group Application Permissions

By setting application permissions on a group (either through a Role Template or on organizational groups), you can control, for example, whether or not users in that group can lock objects, view audit trail information, create reporting periods, and so forth.

Notes

- To delegate group security management permissions to administrators, see "Delegating Administrator Permissions" on page 10.
- To assign application permissions for a role, see "Accessing the Role Templates Page" on page 43.

Procedure

1. Access the **Users, Groups and Domains** page (see "Accessing Users, Groups and Domains" on page 7).
2. On the **Users, Groups and Domains** page, click the name of the group whose application permissions you want to view or modify.
3. On the detail page of the selected group, navigate to the **Permissions** tab.

   Note: Most IBM OpenPages application permissions are grouped under the 'SOX' heading. Selecting the 'SOX' permission selects all the permissions under that heading. This is only advisable for administrative level users.

   For a description of the various permissions, see " IBM OpenPages Application Permissions" on page 20 and "Other Permissions" on page 23.
4. To modify application permissions for a group, click **Edit**, make the required changes, and then click **Save**.

5. To assign user and group management permissions to selected users, see “Delegating Administrator Permissions” on page 10.

IBM OpenPages Application Permissions

The following permissions reside under the SOX permissions heading and can be applied to IBM OpenPages user groups:

Administration

This application permission grants all permissions in the Administration grouping. If you wish to create an administrative-level group, they will need this permission set. If a user group possesses any of these permissions, they will see the **Administration** menu on the menu bar with the appropriate sub-menus.

Access Control Lists:

Allows members of the user group to view, edit, and remove the access control listings for objects through the **Custom Security** menu item on the **Administration** menu. See the "Setting Up Security" section for more information on Access Control Lists (ACLs).

Application Text:

Allows members of the user group to view and edit locale-specific application label values through the **Application Text** menu item on the **Administration** menu.

Currencies:

Allows members of the user group to administer currencies.

ExportConfiguration:

Allows members of the user group to access the environment migration tool to export configuration items for import into another system. See Chapter 17, “Migrating IBM OpenPages Environments,” on page 479.

Field Groups:

Allows members of the user group to view and manage the configuration of field groups with their related field definitions through the **Field Groups** menu item on the **Administration** menu.

ImportConfiguration:

Allows members of the user group to access the environment migration tool to import configuration items exported from another system. See Chapter 17, “Migrating IBM OpenPages Environments,” on page 479.

Object Profiles:

Allows members of the user group to view and manage the configuration of the profile, which includes the object types, through the **Profiles** menu item on the **Administration** menu.

Object Reset:

Allows members of the user group to reset objects for a new reporting period. For information on governing reset behavior, see the chapter, Chapter 12, "Resetting Objects," on page 247.

Object Text:

Allows members of the user group to view and edit locale-specific object label values through the **Object Text** menu item on the **Administration** menu.

Object Types:

Allows members of the user group to view and manage the configuration of object types with their related field groups and associated objects through the **Object Types** menu item on the **Administration** menu.

Reporting Framework:

Allows members of the user group to generate and manage the reporting framework through the **Reporting Framework** menu item on the Administration menu.

Reporting Framework Configuration:

Allows members of the user group to administer and configure the reporting framework through the **Reporting Framework** menu item on the Administration menu.

Reporting Periods:

Allows members of the user group to create and delete Reporting Periods through the **Reporting Periods** menu item on the Administration menu.

Finalize:

Allows members of the user group to finalize the active Reporting Period.

Reapply:

Allows members of the user group to reapply the active Reporting Period.

Reporting Schema:

Allows members of the user group to manage the Reporting Schema through the **Reporting Schema** menu item on the Administration menu.

Role Templates:

Allows members of the user group to view, add, and manage roles through the **Role Templates** menu item on the Administration menu

Settings:

Allows members of the user group to view and manage settings through the **Settings** menu item on the Administration menu.

Audit Trail

This application permission allows members of the user group to view the Audit Trail information for objects. With this permission enabled, an **Audit Trail** button can be selected at the top of the object's detail page.

Browse Files

This application permission allows members of the user group to view and navigate the **Browse** menu item on the **My OpenPages, Attachments** menu.

CommandCenter Studios

This application permission allows members of the user group to launch all supported Studio applications from links on the **Reporting** menu.

Analysis Studio:

This application permission launches Analysis Studio through the **Analysis Studio** menu item on the **Reporting** menu.

Cognos Connection:

This application permission launches Cognos Connection through the **Cognos Connection** menu item on the **Reporting** menu.

Go Dashboard:

This application permission launches Go! Dashboard through the **Go! Dashboard** menu item on the **Reporting** menu.

Query Studio:

This application permission launches Query Studio through the **Query Studio** menu item on the **Reporting** menu.

Report Studio:

This application permission launches Report Studio through the **Report Studio** menu item on the **Reporting** menu.

Folders

This application permission allows members of the user group to create new folders in the object repository that do not correspond to business entities. This allows users to create their own folder structure.

Issues

The application permission allows members of a user group to view the list of Issues through the **Issues** menu item on the **Remediation** menu.

Note: This application permission is in effect only for upgrade customers who have not yet migrated their access control data to the role-based security model. For new first-time installations, this permission is not honored.

Project Management

The application permission allows members of the user group to use the Project Management capabilities available through the **Project** menu item on the **My OpenPages** menu.

View Locks

Users with the View Locks permission can view the existing locks on objects. The View Locks permission does not grant the right to lock or unlock an object - for that you need either the Lock permission or the Unlock permission.

Other Permissions

The following application permissions are not contained under the SOX permission heading, but still have an impact on IBM OpenPages application behavior. Application permissions determine what functional areas and administrative operations a given user or group is able to perform. Typically, end users do not require these application permissions.

All Permissions

Grants members of the user group all permissions and access to every functional and administrative area within IBM OpenPages (Web and server).

Administration

Grants members of the user group the ability to archive and restore document versions.

Archive Management:

Allows group members to enable and disable System Administration Mode and perform certain administrative functions.

System Administration Mode:

Allows group members to enable and disable System Administration Mode and perform certain administrative functions. For details see, Chapter 4, “Using System Admin Mode,” on page 57.

Collaboration

This application permission grants all administrative permissions under the Collaboration grouping that are related to managing tasks and jobs.

Manage Job Types:

Allows group members to add and modify job types. Job types are templates that can be used to create individual jobs.

Start Jobs:

Allows group members to start a job.

View All Jobs:

Allows group members to view a list of jobs and the detail page related to a selected job.

Files

This application permission grants all administrative permissions under the Files grouping that are related to managing files and folders.

Add Folders:

Allows group members to create and add new folders.

Cancel Checkout:

Allows group members to cancel the file check out process for associated files that were checked out by others. When a file check out is canceled, the file is checked back into the system without applying any changes and no new version of the file is created.

Lock:

Allows group members to lock any IBM OpenPages object, regardless of sign-off or ACL restrictions.

Reassign Primary Association:

Allows members of the user group to reassign primary parent associations and view the **Make this <*object*> Primary** button on the Parent tab of an object. Where <*object*> is the object type.

Remove All Tree Locks:

Allows members of the user group to unlock resources and/or resource sub-trees.

Unlock:

Allows group members to unlock any IBM OpenPages object.

Publishing

Add Folder Assignments:

Allows group members to create a new folder assignment. Folder assignments link to an existing folder in the repository and automatically create a reference in the current channel folder to any files of a particular file type.

Add Folders:

Allows group members to create and add a new channel folder.

Add Pages:

Allows group members to create and add publishing-specific files that are used to generate published web pages. Pages are based on page templates.

Add Templates:

Allows group members to create and add page templates that are used to create Web pages.

Assign Files:

Allows group members to assign files to specific channel folders.

Browse Channels:

Allows group members to browse channels. A channel represents the structure of a published website.

Create Channels:

Allows group members to create a new channel for publishing a website.

Manage Rules:

Allows group members to add and modify file rules that specify how file assignments are published within a given channel folder.

Configuring Password Behavior

Overview

The IBM OpenPages product supports the use of strong passwords (passwords that include letters, numbers, and symbols). It also allows administrators to enforce mandatory password changes and other password behavior.

Note: This section on configuring password behavior does not apply if you use single sign-on (SSO), such as LDAP or Microsoft Active Directory, as your internal IT policies will dictate password behavior within the IBM OpenPages application.

Configuring Password Policies

The IBM OpenPages platform allows administrators who can access the Settings administrative section to modify the password policies in effect for the application.

Using the password policies, administrators can enable strong passwords and control whether user passwords must be changed after a certain length of time.

Administrators can modify the following settings (located under **OpenPages | Platform | Security | Password**) as described in Table 5:

Table 5. Password Settings

Setting Group	Setting	Description
Encryption	Encryption Administrator	The user name who is allowed to change the password encryption algorithm and the encryption key.

Table 5. Password Settings (continued)

Setting Group	Setting	Description
Policy	Strong Policies - Character Groups 1-4	These settings allow the administrator to configure the strong password policies for the application. Each Character Group takes a comma-separated list of characters. By default, these groups are empty. If strong passwords are enabled, each password will be required to contain at least one character from each group. If a group is empty, that group is ignored.
	Strong Policies - Enabled	If the value is set to: • `true` - then users will be required to enter strong passwords when specifying their user password. • `false` - then users will not be required to enter strong passwords when specifying their user password. This value is set by default.
	Default Expiry Days	When a user is created or edited, the administrator can set a period of time before the password expires. The default value for that setting is determined by this value. The default value for this setting is 90 days.
	Enabled	Sets whether the password policies are active or not. The default value for this setting is '`false`'.
	Maximum Length	Sets the maximum length of the password. The default value for this setting is '`32`'.
	Minimum Length	Sets the minimum length of the password. The default value for this setting is '`6`'.
	Notify Before Days	Sets the number of days before a user's password expires that the user is shown a warning message at logon about their password expiring.

About Configuring Password Encryption

The IBM OpenPages platform contains the ability to modify the encryption algorithm used to encrypt IBM OpenPages user passwords. The tool used to modify the encryption is called the Update Password Encryption Algorithm tool, hereafter referred to as UPEA.

The UPEA tool can be used to:

- Change the triple DES (3DES) encryption key - this is the default encryption algorithm.
- Change the encryption algorithm in legacy (4.x or 5.1x versions of IBM OpenPages) systems from OP-CUSTOM to 3DES.

  Note: For legacy systems running 4.x or 5.1x versions of IBM OpenPages , when you change the encryption algorithm from OP-CUSTOM to 3DES, all user passwords reset to '`0p3nP4g3s`' (first character is a zero). Users will need to change their passwords the next time they log into the system.

About The UPEA Tool

The UPEA tool is named as follows:

Windows `UpdatePasswordEncryptionAlgorithm.cmd`

and, is located in the <OP_Home>|bin directory of your IBM OpenPages GRC Platform installation.

Where: <OP_Home> represents the installation location of the IBM OpenPages GRC Platform application. By default, this is:	
Windows	C:\OpenPages
AIX	/opt/OpenPages

Before You Begin

Before using the UPEA tool, make sure you read and perform the prerequisite tasks outlined in the following sections.

Verifying the Current Encryption Algorithm

If you have a legacy system, we recommend that you verify the name of the current encryption algorithm before running the UPEA tool to change the algorithm to 3DES as follows.

Procedure

1. Log on to a machine with SQL*Plus and access to the database server.
2. Execute the following SQL statement:

   ```
   select algorithmname from encryptionmodules where inactive=0;
   ```

3. When finished, log out of SQL*Plus.

Results

If the SQL statement returns the name:

- OP-CUSTOM, then run the UPEA tool to change the encryption algorithm to 3DES.
- 3DES, then you already have the triple DES encryption algorithm and can use, if wanted, the UPEA tool to change the 3DES encryption key.

Pre-Requisite Tasks

Verify the Environment:

The following tasks must be completed before running the UPEA tool.

- There must be a properly installed and functioning IBM OpenPages system on the machine.
- All users must log off the system.
- A full backup of the IBM OpenPages database must be completed (see Chapter 14, “Using Utilities,” on page 329).
- Stop all IBM OpenPages servers, including any secondary servers, except for the OpenPagesAdminServer service (Windows) or IBM OpenPages Dmgr server (AIX). This ensures that no users are logged onto the system during the password encryption update.

  Note: For details on starting and stopping servers for both Windows and AIX environments, see “Starting and Stopping OpenPages Application Servers” on page 465.

Configure the Security Provider in the java.security File:

Procedure

Verify that the BouncyCastleProvider security provider has been added to the java.security file as follows:

1. Open a command or shell window on the application server.
2. Navigate to:
   <Java_Home>|jre|lib|security
   Where:
   <Java_Home> is the installation location of the Java Runtime Environment.

   Windows C:\OpenPages\jre\lib\security
   AIX IBM/WebSphere/AppServer/java/jre/lib/security

3. Make a backup copy of the java.security file before modifying it.
4. Open the java.security file in a text editor of your choice.
5. Locate the following property in the file:
   security.provider.<#>=
   Where: <#> is a number (for example, 9).
6. If the BouncyCastleProvider security provider is not present, modify the value after the equal sign so it matches this:
   security.provider.<#>=org.bouncycastle.jce.provider.BouncyCastleProvider
7. When finished, save and close the file.

Change Passwords in the aurora.properties Property File:

Procedure

1. Open a command or shell window on the application server.
2. Navigate to the <OP_Home>|aurora|conf directory.

Where: <OP_Home> represents the installation location of the IBM OpenPages GRC Platform application. By default, this is:	
Windows	C:\OpenPages
AIX	/opt/OpenPages

3. Locate the aurora.properties file in the conf directory and do the following:
   a. Make a backup copy of the file before modifying it.
   b. Open the file in a text editor of your choice.
   c. Search the file for properties that include the string 'password='.
   d. Change all password values following the equal sign to plain text.
   e. When finished, save and close the file.

   Note: Passwords become encrypted when servers are restarted.

For Upgraded Databases Only: Update the Users Table to Change Passwords:

Procedure

1. From a machine with SQL*Plus and access to the database server, log on as the 'openpages' database user.

2. Run the following SQL statements to update the Users table so passwords can be changed:

   ```
   Sqlplus openpages/openpages@<host_name>
   update users set flag_can_change_password=1 where actorid !=8
   ```

   Where:

   `<host_name>` is the name of the database server.

   `actorid=8` is 'OPSystem'.

Using the UPEA Tool

About UPEA Syntax

```
UpdatePasswordEncryptionAlgorithm -Mode [CA|CK] -AlgorithmName
[3DES|OP-CUSTOM] [-ProviderName BC -ProviderClass
org.bouncycastle.jce.provider.BouncyCastleProvider]
-Username OPAdministrator -Password <OPAdministrator password> [-KeySize
<length>] [-Port <portnumber>] [-?]
```

Table 6 describes the various UPEA parameters.

Table 6. UPEA Parameters

Parameter	Description
-Mode	**Required**. Use to specify the mode in which the tool should run. Possible modes are: • `CA` (for Change Algorithm) — used to switch the encryption algorithm from OP-CUSTOM to 3DES. • `CK` (for Change Key) — used to change the 3DES encryption key.
-AlgorithmName	**Required**. Use to specify the type of encryption algorithm that will be used. Valid values are: • `3DES` • `OP-CUSTOM` (only used with legacy systems running 4.x or 5.1x versions of IBM OpenPages)
-Host	**Required**. Use to specify the host name of the application machine.
-ProviderName	**Required**. Use when changing algorithms to the 3DES encryption algorithm only. Has only one valid value: `BC`.
-ProviderClass	**Required**. Use only in conjugation with `-ProviderName` to specify the class for the new encryption algorithm. Has only one valid value: `org.bouncycastle.jce.provider.BouncyCastleProvider`
-Username	**Required**. Use to specify the user name to use when modifying the user passwords. Must be the same as the user specified in the **OpenPages** | **Platform** | **Security** | **Password** | **Encryption** | **Encryption Administrator** setting.
-Password	**Required**. Use to specify the password to the Encryption Administrator account.
-Port	**Optional**. Use to specify the bootstrap port number.

Table 6. UPEA Parameters (continued)

Parameter	Description
-KeySize	**Optional**. Use to specify the length of the 3DES encryption key. The smallest recommended length is 192. If an invalid value is given, or no value is provided, the default value of 112 is used, which is the smallest valid size.
-?	**Optional**. Displays the on-screen help for the UPEA tool.

Changing Password Encryption Algorithms From OP-CUSTOM to 3DES

If you have a legacy system running a version of IBM OpenPages prior to 5.5 and are using the OP-CUSTOM encryption algorithm, you can use the following procedure to run the UPEA tool and change the password encryption algorithm from OP-CUSTOM to 3DES.

Note: Only the `OpenPagesAdminServer` service should be running when using the UPEA tool.

Procedure

1. Open a command or shell window on the IBM OpenPages server.

   Navigate to the `<OP_Home>|bin` directory.

Where: `<OP_Home>` represents the installation location of the IBM OpenPages GRC Platform application. By default, this is:	
Windows	`C:\OpenPages`
AIX	`/opt/OpenPages`

   From the command or shell window, run the following command on a single line:

   Windows

```
UpdatePasswordEncryptionAlgorithm.cmd -Mode CK -Host <host name>
-Port <http port> -AlgorithmName 3DES
-KeySize 112 -Username <OpenPagesAdministrator>
 -Password <password>
```

   AIX

```
sh UpdatePasswordEncryptionAlgorithm.sh -Mode CK -Host <host name>
 -Port <http port> -AlgorithmName 3DES
 -KeySize 112 -Username <OpenPagesAdministrator>
-Password <password>
```

   Where: `<password>` is the password for the OpenPagesAdministrator account.

   Note: If you have changed the default port for IBM OpenPages to a port other than 7001, add the `-Port` parameter to the end of the command with the new port number.

2. The tool will display a message describing the changes it will make and ask for confirmation. Type `Y` at the prompt and press the **Enter** key to proceed.
3. Once the UPEA tool has finished, a success message will be displayed.
4. Restart all IBM OpenPages services.
5. You (or the site administrator) must notify all users that their passwords have been reset to '`0p3nP4g3s`', and that they must change their passwords the next time they log into the system.

Changing the 3DES Encryption Key

At certain times, you may want to change the encryption key used by the 3DES encryption algorithm. To change the encryption key using the UPEA tool, perform the following steps.

Note: Only the `OpenPagesAdminServer` service should be running when using the UPEA tool.

Procedure

1. Log on to the IBM OpenPages server as a user with administrative privileges.
2. Open a command or shell window and change directories to the `<OP_Home>|bin` directory

Where: `<OP_Home>` represents the installation location of the IBM OpenPages GRC Platform application. By default, this is:	
Windows	`C:\OpenPages`
AIX	`/opt/OpenPages`

3. From the command or shell window, run the following command on a single line:

   Windows

   ```
   UpdatePasswordEncryptionAlgorithm -Mode CK -AlgorithmName 3DES
   -Username OpenPagesAdministrator -Password <password>
   ```

   AIX

   ```
   sh UpdatePasswordEncryptionAlgorithm.sh -Mode CK -AlgorithmName 3DES
   -Username OpenPagesAdministrator -Password <password>
   ```

   Where: `<password>` is the password for the OpenPagesAdministrator account.

   Note: If you have changed the default port for IBM OpenPages to a port other than 7001, add the `-Port` parameter to the end of the command with the new port number.
4. The tool will display a message describing the changes it will make. To confirm the changes, type `Y` at the prompt and press the **Enter** key to proceed.

   Once the UPEA tool has finished, a success message will be displayed.
5. Restart IBM OpenPages services to effect the change.

Chapter 3. Granting Access Control Using Role Templates

This chapter explains the various OpenPages access security models, how to configure security based upon Role Templates.

This chapter contains the following topics:

About Role-based Security Models

A role-based security model provides a way for administrators to control user and group access to objects that are under a defined security point within the object hierarchy according to the role the user or group is expected to perform within the organization. Typical security points are business entities, processes, or sub-processes (can also be set at lower security point levels if wanted).

Figure 2 on page 34 shows how various users and groups can have different permissions set for accessing business entities (a defined security point in the object hierarchy) and objects that are under a specific hierarchy.

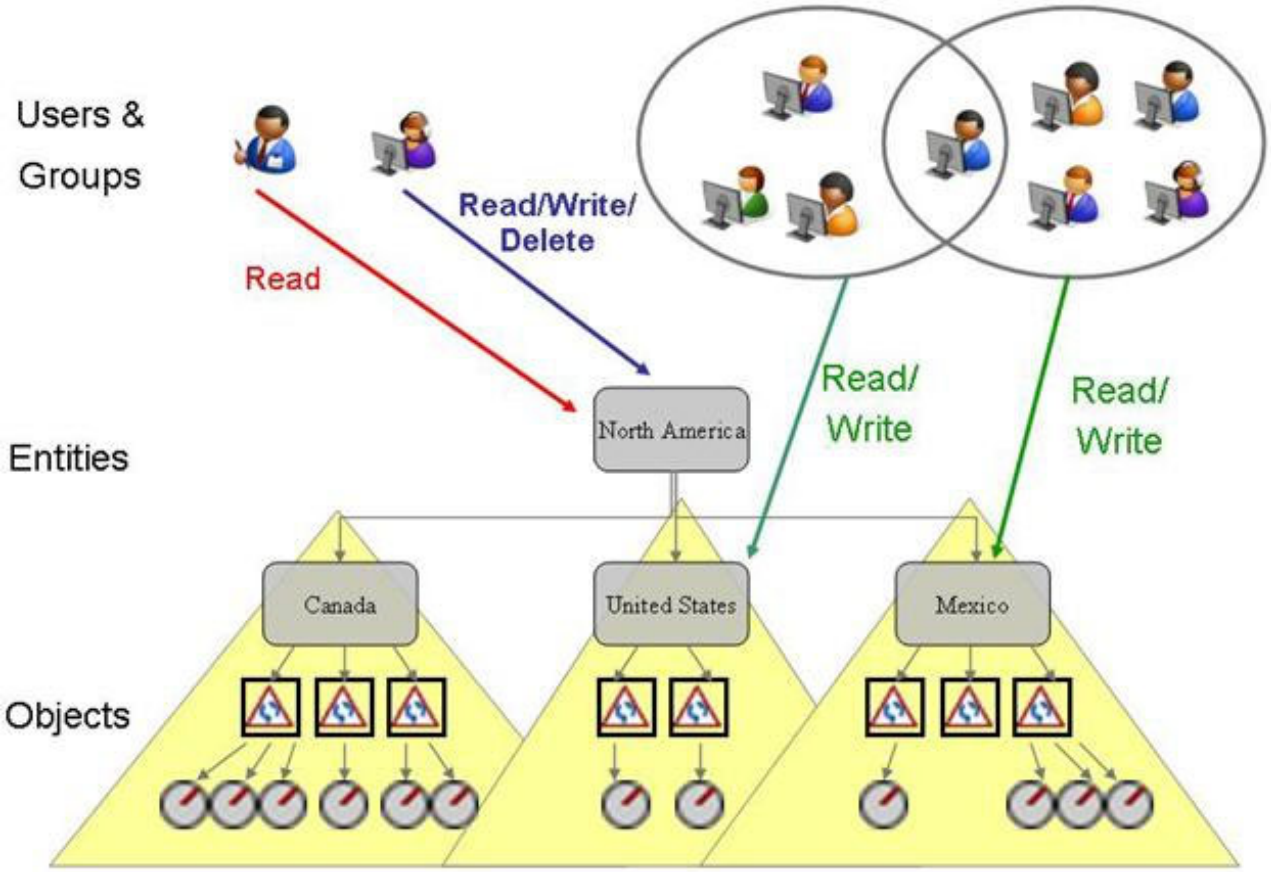


Figure 2. Security Concepts in a Hierarchy

Based on the type of security context points defined in your security model, such as Business Entity, Process, Control Objective or Risk Assessment, you can use a Role Template to define a set of permissions for a set of object types.

For each Role Template that you define, you can set the following:

- Access control (Read, Write, Delete, Associate) for each object type included in that role. For details, see "Using Role-based Access Control Permissions" on page 41.
- Application permissions for the role. For information about the various application permissions, see "Configuring Application Permissions" on page 18.

  Important: These application permissions do not include administrative group and user security management permissions, such as resetting passwords, assigning roles, adding users, and so forth. To learn more about assigning group and user security management permissions to administrators, see "Delegating Administrator Permissions" on page 10.

By assigning a role (an instance of a Role Template) to a user or group at specific security context point in the object hierarchy, you can control access to objects and with which permissions. *Roles* represent the usual or expected function that a user or group plays within an organization. Some examples of roles are: Finance Reviewer, Tester, External Auditor, System Administrator, Control Owner, Risk Assessor.

When you assign a role to a group or user, the security settings of that Role Template are acquired by that group or user and permissions are automatically granted, per the role template definition, to all objects below or under the specified security point.

For example, if a role were assigned to a user for a business unit (security context point), access control for specific object types under that security point would be set in the object hierarchy. Object types that were excluded from the role would be hidden from view, object types that were included would be visible and could be accessed by users and groups assigned to that role.

So that you can have a clear and accurate understanding of which users and groups have access to what and with which permissions, and what access control modifications were made in the system, you can run a variety of reports to view this data. For details on the types of configuration audit and security reports available to you, see the section "Audit Reports Folder" on page 82.

Understanding Security Context Points

The structure of the object hierarchy that is defined in your system also acts as the security context point to which access control can be assigned.

Roles (defined by Role Templates) are granted to specific security points in the object hierarchy, and permissions for a particular role are automatically granted to all objects that are created in the same location beneath that security point. If a role is assigned to a group on a top-level Business Entity, then all users of that group would have access to that business entity and would be able to access all objects under that entity as per the permissions in the role.

By default, the installation process automatically sets Business Entity (`SOXBusEntity`) as the security context point within the object hierarchy at which roles can be assigned.

Example

Let's say you have a regional office called 'North America' and a sub-regional office called 'United States'. When you create the business entity, the folder structure `/BusinessEntity/North America/United States` would automatically be created.

Let's say you also created a Role Template called 'Entity Owners' that has access defined for the following object types:

- Business Entity
- Process
- Sub-process
- Control Objective
- Risk
- Control

When you assign the 'Entity Owners' Role Template to the 'United States' business entity, the following structure is automatically generated under the root folder of each object type:

```
/Processes/North America/United States
/Sub-processes/North America/United States
/ControlObjectives/North America/United States
/Risks/North America/United States
/Controls/North America/United States
```

Note: that the folder structure `/BusinessEntity/North America/United States` does not have to be generated since it already exists (was automatically created when the business entity was initially created).

Figure 3 shows how access permissions (R=Read, W=Write, D=Delete, A=Associate) can be granted to specific objects in the hierarchy under the 'United States' business entity security context point.

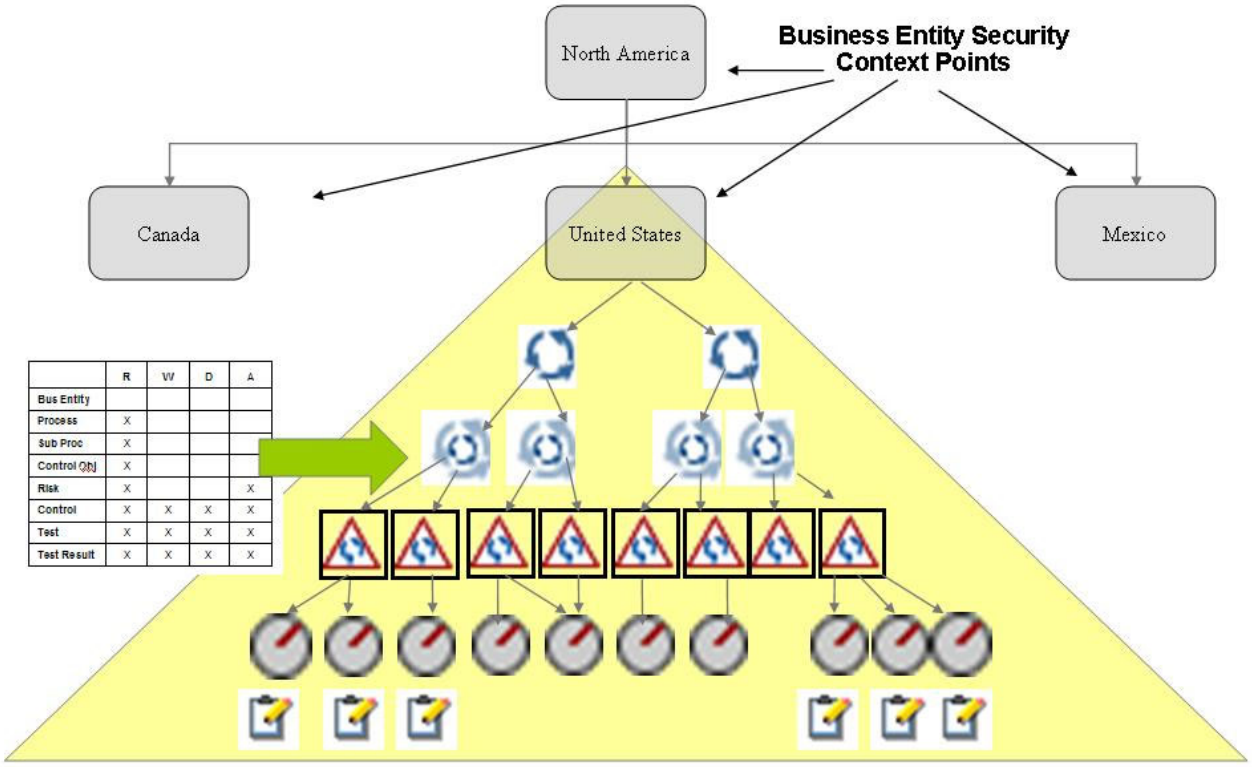


Figure 3. Business Entity Security Context Points

For details on assigning security management permissions to security domain group administrators, see "Delegating Administrator Permissions" on page 10.

Extending Security Context Points

To achieve a finer level of control, it is possible to extend the security context point to other objects in the hierarchy (such as Business Entity-Process or Business Entity-Risk Assessment) by changing the 'Model' setting (for details, see "Setting the System Security Model" on page 274).

Note: The 'Model' setting is a system-wide setting. Switching the security model after data is loaded (or migrated) into the system is not recommended and requires assistance from OpenPages Professional Services.

To determine the optimal security context points for your organization, you need to evaluate your requirements for securing resources at lower security context points in your hierarchy. Extending the security context points to achieve a finer level of control does not prevent you from defining security at higher security context points.

Example

Let's say you extended the security context points to include Business Entity-Process. In this scenario, administrators could assign, for example, a "Process Role Template" to one or more users or groups on one or more Processes.

Permissions (Read, Write, Delete, Associate) in the "Process Role Template" could then be assigned to that Process security context point. The permissions in that template are applied to every object created beneath that point in the object hierarchy and to any object that is created in the future below that point.

Although users and groups who are assigned the "Process Role Template" would be able to navigate to and access Processes and child objects beneath a Process hierarchy, the details of the parent Business Entity would be hidden from them.

Note: Users who have roles that are assigned to a context security point below the Business Entity level, only have navigation access to the parent Business Entity. If users require the ability to view or modify the details of a parent Business Entity, then you must use an Entity-based Role Template to grant explicit Read and/or Write permission to users at an Entity security point.

The IBM OpenPages application interface does not allow breaking folder ACL inheritance on any folder on which role-based access control is assigned. Administrators are **strongly advised not to break** folder inheritance using ObjectManager or any other application interfaces on any object type folders as this will cause role-based security to fail.

Figure 4 on page 38 shows how access permissions can be granted when the security context points are extended to include Process objects as security points to achieve a higher level of control.

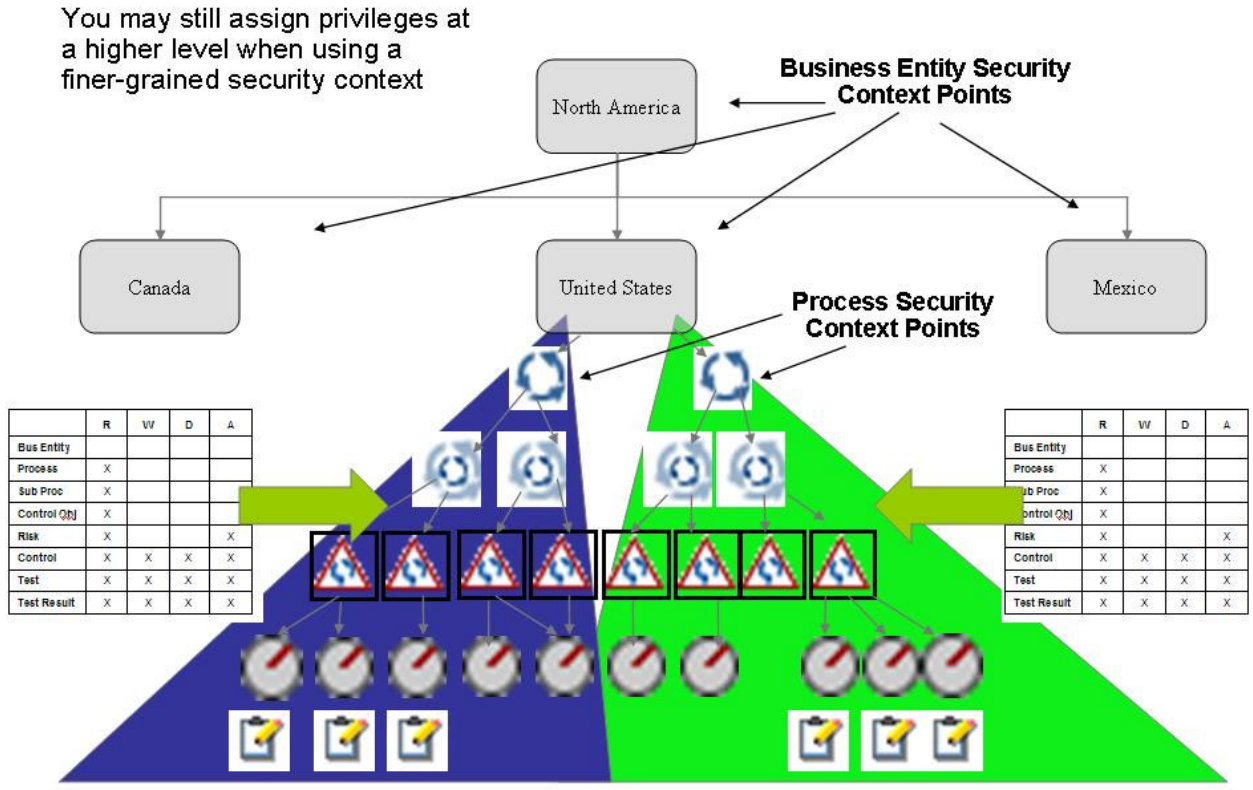


Figure 4. Business Entity and Process Extended Context Points

About The Reporting Framework and Multiple Security Context Points

In a security model that contains multiple security context points, objects that form a "triangle" relationship have implications for the reporting framework.

Triangle relationships are formed among objects when an object type is configured to have a parent of more than one type (typically, the second parent is a recursive object type).

For example, if Risk object types are configured to be a child of Process and a child of SubProcess object types, then a triangle relationship will exist among these different object types. Figure 5 on page 39 shows an example of a triangle relationship between a child Risk and parent Process and Sub-Process object types.

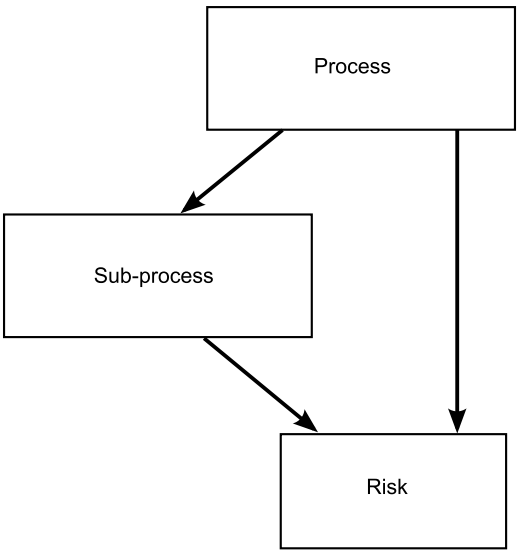


Figure 5. Triangle Relationship Between Different Object Types

In the reporting framework, fields from parent objects within a triangle relationship (for example, Process and Sub-Process) are stored in the same Query Subject along with the ID of the shared child object (such as, Risk ID). When both Process and Sub-Process fields are part of the same Query Subject, a user would require Read permission on both Process and Sub-Process object types to view these fields in a report.

When a triangle relationship exists among objects, we recommend as best practice that you avoid the use of the Sub-Process (or similar) object type as a security point in your system unless you are willing to always grant Read access to the parent object type (such as Process).

Note: For information about configuring triangle object relationships in the reporting framework, see "Configuring Triangle Object Relationships" on page 315.

Sample Scenario

Let's say a user has Read access for Sub-Process object types, so they can view details for Sub-Process objects in the application user interface.

If the same user does not have Read or Write access to the parent Process and Business Entity, that user will still have an implicit Navigate permission to the Process and Business Entity object types. The implicit Navigate permission allows users to navigate through the object hierarchy from, for example, an Overview page to object types that are lower in the hierarchy (such as Sub-Process) for which they have explicit permission (in this case, Read access).

If a triangle relationship exists among these object types, the same user would not have permission to view the Sub-Process detail in a report unless the user was also granted explicit Read access on the Process object type (as `SUBPROCESSES` and `PROCESSES` reside in the same Query Subject).

About Security Domains

In the IBM OpenPages security model, special user groups - called 'security domain groups' - are automatically created when a Business Entity or Sub-entity

object is created. Security domain groups act as containers for users and organizational groups associated with that business entity.

Each security domain group is identified by a people hierarchy  icon under a top-level (root) **Security Domains** folder on the **Users, Groups and Domains** page, and the name of the group corresponds to the name of the business entity to which it belongs.

Users in a security domain group are generally assigned roles to work on the objects under that entity. You can also delegate specific security management activities to administrators in a security domain group for managing users and groups within that business entity.

Note: When you expand a security domain group, only child security domains are displayed. Any organizational groups and users associated with that security domain can be viewed only from the detail page of that security domain group.

Example

Let's say you want to delegate the security activity of resetting passwords to an administrator for members of a particular Sales Office security domain group.

You would navigate to the detail page of the Sales Office security domain group and assign the 'Reset Password' permission to an administrator. That administrator would then be able to only reset passwords for users in that Sales Office security domain group. You could repeat this process of delegating 'Reset Password' permission to an administrator for each security domain group within your organizational hierarchy.

About Moving Business Entities

On occasion, you may need to re-organize your business entity structure by moving a Business Entity with its corresponding object hierarchy from one location to another.

When you move a business entity structure, all role assignments that were made on that business entity remain intact.

This means that users and groups who were granted various roles at a specific Business Entity security context point before the move operation, will continue to have the same roles and access after the move operation.

About Copying Business Entities

If you use the copy operation to expedite the setup of child business entities by duplicating an instance of an existing business entity, a security domain group for that new child business entity is automatically created by the system and is associated to the security domain group of the parent business entity.

Initially, the new security domain group that corresponds to the new child business entity is empty (no users or groups). However, users and groups who have assigned roles with access control defined for the parent business entity will have the same access on the new child business entity.

An administrator of the security domain group for the parent business entity can add and/or associate users and groups to the security domain group of the new

child business entity. An administrator of the parent business entity can delegate administration activities by selecting an administrator. For details, see “Delegating Administrator Permissions” on page 10.

To refine user access to the new child business entity, you can use the application interface to define Role Templates and grant roles to users and groups. For details, see “Using Role Templates” on page 43.

Using Role-based Access Control Permissions

When you create a Role Template, you can specify the type of security access control you want to have on an object type’s folder structure for groups and users who are assigned to that role.

Note:

- The file (SOXDocument) and link (SOXExternalDocument) object types have the same root storage folder path. As a result, you can configure only one set of ACLs for both these object types in a role.
- Role-based security does not apply to Project Milestones and Project Action Items. For details on setting security access for these object types, see “Setting Custom Security for Projects” on page 49.
- Any new object types that are added to the system are excluded from all existing Role Templates.

Understanding Security Access Control Permissions

For each object type that you want to include in a Role Template, you can set the following access control (ACL) permissions on the object’s folder structure:

- **Read** - when you select an object type for inclusion in a role, the value of the Read permission is automatically set to ‘Granted’ on the object’s folder structure. This means that any groups or users assigned to this role can navigate to, and view the details of objects (parent and child) contained in the folder and the folder itself, but cannot modify any object data unless other permissions are explicitly set.
- **Write** - the groups or users assigned to this role can modify the details of objects within the selected folder, but cannot delete objects. Write access to a folder is required for creating new objects within the folder.
- **Delete** - the group or user assigned to this role can delete objects within the folder structure.
- **Associate** - the group or user assigned to this role can create associations between objects.

For each ACL permission, you can set an explicit value. These values or settings are propagated downward and inherited by any child object storage folders under that parent object’s folder structure.

For each ACL permission, you can set one of the following values:

Note: For usage examples, see “Using Access Control Setting” on page 42.

- **Unspecified** - by default, no access is explicitly granted to the user or group for the corresponding object through this role. The ‘Unspecified’ setting does not override any access that is granted on this object through other roles or access inherited through a role on higher level security context points. This value should be used instead of ‘Denied’ since it is less restrictive.

- **Granted** - this explicit setting gives a user or group full access to the specified action (Write/Delete/Associate). The user can modify, or delete the file or folder, depending on the permission.
- **Denied** - this explicit setting does not allow a user or group to perform the specified action (Write/Delete/Associate). The 'Denied' setting overrides any access that is granted on this object through other roles or access inherited through a role on higher level security context points.

Using Access Control Setting

The following use case scenarios provide examples of how the system may respond with various settings.

Scenario 1: Using Explicit Settings

If a user or group is assigned multiple roles and the explicit ACL settings within these roles conflict, the most restrictive explicit setting will be used.

Example

Let's say we create a 'Test Performer' and a 'Test Reviewer' role for the Test object type. Each role has the **Write** ACL permission explicitly set to the following:

- 'Test Performer' has **Write** = **Granted**
- 'Test Reviewer' has **Write** = **Denied**

If we assign both roles ('Test Performer' and 'Test Reviewer') to a user called 'Tester1', 'Tester1' will not be able to create new Test objects even though the 'Test Performer' role has Write = Granted. This is because the Write = Denied permission of the 'Test Reviewer' role is more restrictive than the Write = Granted permission, and the most restrictive setting is automatically applied.

Scenario 2: Using Explicit and Unspecified Settings

If a user or group is assigned multiple roles and one role has an explicit ACL settings but the other role has 'Unspecified' for the same permission, the explicit setting will be used.

Example

Let's say we create an 'Initial Test' and a 'Final Test' role for the Test object type. The roles have the **Write** ACL permission set to the following:

- 'Initial Test' has **Write** = **Granted**
- 'Final Test' has **Write** = **Unspecified**

If we assign both roles ('Initial Test' and 'Final Test') to a user called 'Tester1', 'Tester1' will be able to create new Test objects even though the 'Final Test' role has Write = Unspecified. This is because the Write = Granted permission is explicit and the explicit setting is automatically applied.

Scenario 3: Using Unspecified Settings

If a user or group is assigned a single role and the ACL settings within this role:

- Use the default value 'Unspecified', and
- No other access control has been explicitly set for the user or group

then access is DENIED.

Example

Let's say we create an 'Initial Test' role for the Test object type. The role has the **Write** ACL permission set to the following:

'Initial Test' has **Write** = **Unspecified**

If we assign the role ('Initial Test') to a user called 'Tester1' and 'Tester1' has not been granted access through any group-inheritance, 'Tester1' will not be able to create new Test objects.

Using Role Templates

Role Templates have the following characteristics:

- When you perform an action on a Role Template (such as creating, editing, assigning, enabling or disabling), the Role Template is automatically locked by the system to prevent other users from simultaneously accessing the template. Once you save your changes (or cancel the operation), the Role Template becomes unlocked.
- Role Templates are the preferred method for granting users or groups application permissions.

  Note:
  - Both application permissions and ACLs are included in the role definition process. When a role is assigned to a user or a group on any business entity or security context point, that user or group automatically acquires the application permissions defined in that Role Template.
  - When a user or group is assigned multiple roles, the user or group accumulates the application permissions that are defined in the various roles. Application permissions are granted by the role (not the security context point) and apply in all situations where the user has the correct ACL access. For example, users with Read permission to Business Entities and the **Audit Trail** application permission will be able to view the Change History (audit trail) for those Business Entities.
- Role Templates are global to the application and are available for role assignment by any administrator of a security domain who has the **Assign Roles** administrator permission.

Accessing the Role Templates Page

Only an OpenPages Super Administrator or a delegated administrator with the **Role Templates** permission can access the **Role Templates** menu item. For information about delegating administrator permissions, see "Delegating Administrator Permissions" on page 10.

Procedure

1. Log on to the IBM OpenPages application user interface as a user with the **Role Templates** application permission set.
2. From the menu bar, select **Administration** and click **Role Templates**.

Results

From the Role Templates page, you can add, view, and modify Role Templates.

Adding a Role Template

The Role Template wizard will guide you thorough creating a new role, selecting object types for inclusion or exclusion, and setting security on the selected object types.

Role Template names are not localizable.

Note: Users who have roles that are assigned to a context security point below the Business Entity level, only have navigation access to the parent Business Entity. If users require the ability to view or modify the details of a parent Business Entity, then you must use an Entity-based Role Template to grant explicit Read and/or Write permission to users at an Entity security point.

Procedure

1. Ensure that System Administration Mode is disabled (for details, see "Enabling and Disabling System Admin Mode" on page 58).
2. Access the Role Templates page (see "Accessing the Role Templates Page" on page 43).
3. On the **Role Templates** tab, click **Add** to open the Add Role Template wizard.
4. On the Specify Role Details page:
   a. In the **Name** box, type a name for the role. For example, *Tester01*.
   b. In the **Description** box, optionally type a brief description of this role.
   c. Click the **Role Type** arrow, and select the type of security context point you want from the list.

      Note: If only one security context point type (such as Business Entity) is defined for your system, this will be the only value in the list. Security context point types are derived from the security model in effect for your installation.
   d. Click **Next**.
5. On the Specify Access Controls page:
   a. Select the check box next to each object type for which you want to configure folder permissions. For example, if you wanted to configure permissions for Risk and Test objects, you would select *SOXRisk* and *SOXTest*.

      Note: To select all object types, select the check box in the **Name** column.
   b. In the row for each selected object type, select a setting value for each permission (Write, Delete, and Associate). By default, Read is always set to 'Granted', and all other permissions are set to 'Unspecified'.

      For setting details, see "Using Role-based Access Control Permissions" on page 41.
   c. When finished, click **Next**.
6. On the Specify Permissions page:
   a. Select the application permissions you want to assign to this Role Template. For a description of the various application permissions, see "Configuring Application Permissions" on page 18.
   b. When finished, click **Finish**. The new role is listed on the Role Templates page.
7. To assign the role to a user or group, see "Assigning a Role to a User or Group" on page 47.

Modifying a Role Template

When you modify a Role Template after assigning it to users and/or groups, any changes you make to access control (ACLs) and application permissions are automatically propagated to those users and groups. You can use this propagation feature to grant additional access control or revoke access control on certain object types to existing users and/or groups, by modifying the role template.

Typically, a Super Administrator or a top-level security domain administrator (with **Assign Roles** administration permission and **Role Templates** application permission) are able to modify, disable or delete a Role Template. This is because a lower-level security domain administrator, though having **Role Templates** application permission, will not have **Assign Roles** administration permission on higher-level entities and hence will not be able to successfully edit, disable, or delete a template.

Note: If you become distracted while editing a Role Template and the session times out before you are able to complete the task, an **Unlock** button is displayed on the detail page of the Role Template. To unlock the Role Template and resume your editing activity, click the **Unlock** button.

Procedure

1. Access the Role Templates page (see "Accessing the Role Templates Page" on page 43).
2. From the list on the **Role Templates** tab, click the name of the role you want to modify.
3. On the detail page of the selected role, click **Edit**.
4. Make the required changes.
5. When finished, click **Save**.

Disabling a Role Template

If wanted, you can make a role inactive and keep it for future use by disabling the role.

When you disable a role, the following occurs:

- Depending on the **Disable Role Group** application setting, any users and groups, who were previously assigned that role, will either retain or lose their access control and application permissions. By default, the setting allows users and groups to retain access after a role is disabled. For more details on this setting, see "Disabling Access Control on Role Groups" on page 275.
- The disabled role template is removed from the role assignment selection list and cannot be used for further role assignments.
- The status of the role on the **Role Templates** list page changes from 'Active' to 'Inactive'.
- The role can be enabled for use at a later time (for details, see "Enabling a Role Template" on page 46).

Procedure

1. Access the Role Templates page (see "Accessing the Role Templates Page" on page 43).
2. From the list on the **Role Templates** tab, click the name of the role you want to disable. The detail page of the selected role is displayed.
3. On the **Role Information** tab, click **Disable**.

Note: The button changes from **Disable** to **Enable**.

Enabling a Role Template

You can enable a role that was previously disabled. When you enable a role, the following occurs:

- Any users or groups who are assigned that role will be able to perform activities on objects associated with that role.
- The enabled role template is included in the role assignment selection list and can be used for further role assignments.
- The status of the role on the **Role Templates** list page changes from 'Inactive' to 'Active'.
- The role can be disabled again at a later time (for details, see "Disabling a Role Template" on page 45).

Procedure

1. Access the Role Templates page (see "Accessing the Role Templates Page" on page 43).
2. From the list on the **Role Templates** tab, click the name of the role you want to enable. The detail page of the selected role is displayed.
3. On the **Role Information** tab, click **Enable**.

   Note: The button changes from **Enable** to **Disable**.

Deleting a Role Template

An administrator (or Super Administrator) with **Role Templates** application permission and the **Assign Roles** administrator permission has the ability to assign and/or revoke roles on any entity in the system. In effect, only a Super Administrator or a top-level entity administrator will be able to delete role templates, since this action automatically revokes all role assignments made using the selected Role Template on any business unit in the application.

When you delete a role, the following occurs:

- Any users or groups who were assigned that role will no longer be able to perform the activities on objects associated with that role.
- The role is permanently removed from the list of roles on the **Role Templates** tab and cannot be restored.

If you want to remove a role without deleting it, you can disassociate the role instead. For details, see "Revoking a Role From a User or Group" on page 48.

Procedure

1. Access the Role Templates page (see "Accessing the Role Templates Page" on page 43).
2. You can delete a role from either the **Role Templates** list page or from the detail page of the role.
   - From the Role Templates page:
     a. From the list on the **Role Templates** tab, select the check box next to each role you want to delete.
     b. Click **Delete**.
   - From the detail page of the selected role:

a. Click the name of the role you want to delete from the list on the **Role Templates** tab to open its detail page.
b. On the **Role Information** tab, click **Delete**.

3. At the confirmation prompt, click **OK**.

Assigning and Revoking Roles

An administrator of a parent domain group can assign or revoke roles only from its child groups and users. For example, an administrator who has the **Assign Roles** administrator permission on a top-level a domain group, could assign any Role Template to users and groups on that business entity or its child sub-entities.

If an administrator assigns a Role Template to a user or group on a security domain, the same access control that is granted on the corresponding business entity will be propagated to its child entities.

When an administrator assigns a role to a user or group on a lower-level domain that gives the user Read access to a lower-level business entity, the application provides the necessary access to navigate to that lower-level entity even though the user may not have Read access to all of its parent entities.

Example

Let's say we have a business entity with the following hierarchical structure:

Entities:

Company ABC > North America > Boston

Processes:

Company ABC > North America > Boston > P1

Company ABC > North America > Boston > P2

If the administrator of the Boston office assigns a "Process Owner" role to user "Mary" granting Read access only to Processes associated with the Boston entity, then user "Mary" can navigate to processes associated with the Boston entity only, even though "Mary" cannot view the details of the entities Company ABC, North America and Boston.

Assigning a Role to a User or Group

Once Role Templates are created (see Adding a Role Template), you can assign one or more roles to groups and users on a security context point within a business entity security domain. If your organization has many security context points, you can filter on the name of a security context point to reduce the scope of the items listed.

Procedure

1. Access the **Users, Groups and Domains** page (see "Accessing Users, Groups and Domains" on page 7).
2. Under the **Security Domains** group, click the name of the security domain group to which you want to add a role assignment for a user.
3. On the detail page of the selected security domain group:
   a. Navigate to the **Role Assignments** tab.
   b. Click **Assign** to display the Assign Roles wizard.

4. On the Select Users/Groups page:
   a. Click **Add**.
   b. In the selection box, select the check box next to each group or user you want.

      Note: To expand the group/user hierarchy, click the + (plus) sign.
   c. When finished, click **Next**.
5. On the Select Role Type and Roles page:
   a. Click the **Role Type** arrow and select a security point from the list, and then click **Go**. If only one security point (such as Business Entity) is defined for your system, this will be the only value in the list.
   b. In the **Roles** box, select one or more roles from the list.
   c. When finished, click **Next**.
6. On the Select Business Units page:
   a. In the **Name** box, optionally type a security context point name or portion of a name and then click **Filter**. If the list of security context points is large, the filter will reduce the scope of the list by returning only those items that match the text you typed.
   b. In the **Business Units** box, select one or more security context points from the list.
   c. When finished, click **Finish**.

Revoking a Role From a User or Group

Disassociating users from a security domain group does not result in removal of their role assignments on that entity. However, when you revoke a role from a user or group, the role assignment is explicitly removed from the user or group on a given entity.

Procedure

1. Access the **Users, Groups and Domains** page (see "Accessing Users, Groups and Domains" on page 7).
2. Under the `Security Domain` root group, click the name of the business entity security domain group from which you want to revoke a role.
3. On the detail page of the selected security domain group:
   a. Navigate to the **Role Assignments** tab.
   b. Select the check box next to the name of each group or user you want to revoke.
   c. When finished, click **Revoke**. The name of the selected group or user is removed from the list.

Viewing Roles Assigned to Users or Groups

You can view which roles are assigned to users and groups by:

- Running reports (for details about available reports, see the section "Security Folder" on page 85)
- Navigating to a user or group detail page and see the list of all roles granted to that user or group.
- Navigating to the detail page of a business entity security domain group as described in the following steps.

Note: Role Templates that were assigned directly to a parent or child business entity security domain group can only be viewed from the detail page of that parent or child. Role assignments made on a security domain are only displayed for that domain.

In the case of an extended security context model, for example, SOXBusEntity/SOXProcess or SOXBusEntity/SOXProcess/SOXSubprocess security models, role assignments on processes and sub-processes associated with the current security domain are also displayed.

Procedure

1. Access the **Users, Groups and Domains** page (see "Accessing Users, Groups and Domains" on page 7).
2. Under the `Security Domain` root group, click the name of the business entity security domain group whose role assignments you want to view.
3. On the detail page of the selected security domain group, navigate to the **Role Assignments** tab.
4. To view role assignments made directly to another business entity security domain group, repeat Steps 2 and 3.

Setting Custom Security for Projects

If required, you can set custom security access control (Read, Write, Delete, Associate) on folders for Project Milestones and Project Action Items from the **Custom Security Access Control** page. By default, inheritance for access control (ACL) is set to 'true'.

By default, the custom ACL shows only Project Milestone and Project Action Items. To show other object types in the custom ACL, add values to the **OpenPages | Common | Custom ACL Object Types** setting. Add object names separated by commas. For details on working with settings, see "Accessing the Settings Page" on page 268.

About the Folder Hierarchy and Inheritance

On the Access Control page, the 'Milestone' folder is the container for Project Milestone objects and the 'Task' folder is the container for Project Action Item objects. Both these folders are under a 'Plan' folder.

By default, inheritance on the 'Plan' folder is set to 'false' and cannot be changed. Inheritance on the 'Milestone' and 'Task' object folders, by default, is set to 'true'. If wanted, you can disable inheritance on these folders. If a folder does not have an ACL set for a particular group, the application looks back up the folder tree until it finds an ACL for that group and uses it for the current folder. When folder inheritance is enabled and a folder does not have an ACL set for a particular group, the application looks backwards up the folder tree until it finds an ACL for that group and uses it for the current folder.

Accessing the Access Control Page

Only an IBM OpenPages Super Administrator can access the **Custom Security** menu item.

Procedure

1. Log on to the IBM OpenPages application user interface as a Super Administrator user with the **Access Control Lists** application permission set.

2. From the menu bar, select **Administration** and click **Custom Security**.

Creating an Access Control List

If wanted, you can control which users and/or groups can access Project Milestones and/or Project Action Items.

Procedure

1. Access the Access Control page (see "Accessing the Access Control Page" on page 49).
2. Under the 'Plan' folder, do the following:
   - For Project Milestones - click the **Milestone** link.
   - For Project Action Items - click the **Task** link.
3. On the **Access Control List** tab, click **Add**.
4. On the access control entry page:
   a. Click the User/Group arrow and select the user or group you want to add.
   b. For each permission (Read, Write, Delete, Associate), select a setting value (Granted, Inherited, Denied).

      Note: 'Read' permission is required for 'Write' and 'Associate' access, and 'Write' access is required in order for 'Delete' access to be granted. You can select any combination of permissions, but when you save the ACL, it will be modified to be a valid combination of permissions.
   c. When finished, click **OK**.

Edit an Access Control List

To edit an Access Control List for a user or group, perform the following steps.

Procedure

1. Access the Access Control page (see "Accessing the Access Control Page" on page 49).
2. Expand the folder hierarchy and click the folder that has the Access Control List you want to modify.
3. On the **Access Control List** tab:
   a. Select the check box next to the user or group for which you want to modify access control.
   b. Click **Edit**.
   c. Make the necessary changes.
   d. When finished, click **Save**.

Delete an Access Control List

To delete an Access Control List for a user or group, perform the following steps.

Procedure

1. Access the Access Control page (see "Accessing the Access Control Page" on page 49).
2. Expand the folder hierarchy and click the folder that has the Access Control List you want to modify.
3. On the **Access Control List** tab:

a. Select the check box next to the user or group for which you want to delete access control.
b. Click **Delete**.

Setting Up LDAP User Authentication

Overview of LDAP Authentication

The IBM OpenPages platform supports the use of an LDAP (Lightweight Directory Access Protocol) authentication server to control user access. This section details the configuration steps required to integrate the IBM OpenPages application with an LDAP data source.

Only one login module can be active at the same time. The underlying IBM OpenPages platform supports a single namespace, so all users must be authenticated through the same data source. Multiple authentication modules can be used in a multi-forested environment.

Any users that are created or imported into the IBM OpenPages application must also be present in the LDAP authentication server. It is the responsibility of the person managing the IBM OpenPages users to maintain the correlation between the IBM OpenPages user list and the external LDAP data source. If a user is disabled on the IBM OpenPages server, they must be manually disabled on the LDAP Directory server.

Note: If an LDAP Directory Server is being used for user authentication, the **Change Password** button will be disabled in the IBM OpenPages user interface. When an LDAP server is used, passwords are not maintained in the IBM OpenPages application. The password must be changed directly in the LDAP server.

Supported LDAP Servers

The IBM OpenPages platform has been certified for use with the following LDAP servers:

- Microsoft Active Directory
- Sun ONE Directory Server (formerly known as iPlanet Directory Server)

Configuring the LDAP Authentication Module

To successfully use an LDAP Directory Server with the IBM OpenPages application, you must configure the LDAP Authentication Module to recognize the presence of the LDAP server. This is accomplished by completing the following steps:

- "Add Existing Users to the LDAP Server"
- "Update the Logon Account Used by the Framework Generator" on page 52
- "Change the OPSystem Password (optional)" on page 52
- "Modify the LDAP Configuration File" on page 53

The following sections will detail the steps required to configure the IBM OpenPages application to work with an external LDAP authentication source.

Add Existing Users to the LDAP Server

Make sure to refer to your LDAP Directory Server documentation for the steps required to add IBM OpenPages users to the LDAP server.

Important: If you are using Microsoft Active Directory Users and Computers as your LDAP authentication server, the user name is limited to a length of 20 characters. User names that exceed the 20 character limit are truncated to 20 characters. This length limitation does not occur in the LDAP server provided by Sun.

All users that require access to the IBM OpenPages GRC Platform application or server platform must be added to the LDAP authentication server. In addition, the following users will need to be added to the LDAP server:

- OPSystem

  Note: If you specify a password for the OPSystem account that is different from the one installed by the product, you will need to complete "Change the OPSystem Password (optional)" to change the OPSystem account password system-wide.
- The IBM OpenPages Super Administrator (for more information, see "The Super Administrator" on page 9)
- OPAdministrator (only if you are using this account)

Update the Logon Account Used by the Framework Generator

The `OpenPagesAdministrator` account is used, by default, as the logon account to CommandCenter during reporting framework generation.

Note: Some upgrade customers can also use `SOXAdministrator`.

Whether you choose to use the `OpenPagesAdministrator` account or use a different valid LDAP account for CommandCenter logon, the LDAP and CommandCenter logon user names and passwords must match. If there is a mismatch between these logon user names and passwords, the framework generation process will fail.

To change the user name and password for the administrator account used for reporting framework generation, you must edit values in the `framework.properties` file to a valid LDAP user name and password.

For details on editing the `framework.properties` file, see "Changing the Administrator Logon Account and Framework Generation" on page 65.

Change the OPSystem Password (optional)

If the OPSystem password on the LDAP server does not match the one installed by the IBM OpenPages application, you will need to change the OPSystem password using the provided tool.

Procedure

1. Start all services.
2. Open a command or shell window on the application server.
3. Navigate to the `<OP_Home>|bin` directory.

Where: `<OP_Home>` represents the installation location of the IBM OpenPages GRC Platform application. By default, this is:	
Windows	`C:\OpenPages`
AIX	`/opt/OpenPages`

4. Execute one of the following commands to open the `chng-sys-pswd` tool:

Windows `chng-sys-pswd.bat`
AIX `chng-sys-pswd.sh`

You will be prompted for the old OPSystem password and then the new password.

5. Follow the on-screen prompts.
6. When directed, stop all services.
7. In a command or shell window, navigate to the following workflow `bin` directory:

   `<Workflow_Home>|server|deployment|bin`

Where:	
`<Workflow_Home>` represents the installation location of the Fujitsu Interstage BPM server. By default, this is:	
Windows	`c:\Fujitsu\InterstageBPM`
AIX	`/opt/Fujitsu/InterstageBPM`

8. From the workflow `bin` directory, run the `importProperties` command (on a single line) as follows:

   Windows
   ```
   importProperties.bat <Workflow_Home>\server\instance\default\
   ibpm.properties <opworkflow_db_user> <opworkflow_db_password>
   ```
   AIX
   ```
   importProperties.sh <Workflow_Home>/server/instance/default/
   ibpm.properties <opworkflow_db_user> <opworkflow_db_password>
   ```

   Example (Windows)

   ```
   importProperties.bat c:\Fujitsu\InterstageBPM\server\instance\default\
   ibpm.properties opworkflow opworkflow
   ```
9. Restart all services to enable the new password.

Modify the LDAP Configuration File

Finally, you must modify the authentication configuration file to enable the LDAP Directory Server you are using.

The `aurora_auth.config` file contains three authentication modules:

- Openpages - the default internal user directory
- OpenpagesIP - the LDAP configuration for the Sun One Directory Server
- OpenpagesAD - the LDAP configuration for the Microsoft Active Directory Server

The only module that the IBM OpenPages system pays attention to is the module named 'Openpages'. Therefore, in this step we will modify the configuration file to change the name of the correct LDAP authentication server module to 'Openpages', and then change the settings to reflect the settings of your LDAP server.

Procedure

1. Stop all IBM OpenPages services.
2. Open and edit the `<OP_Home>\aurora\conf\aurora_auth.config` file in a text editor.

   Where:

<OP_Home> is the installation location of the OpenPages application. By default, this is c:\OpenPages.

3. Find the module named 'Openpages' and change the name to 'OpenpagesDefault' (without the quotes).
4. Depending on the LDAP server you intend to use, modify either the OpenpagesIP or OpenpagesAD module name to 'Openpages' (again without the quotes).

   If you are using a Microsoft Active Directory server, change the OpenpagesAD module. If you are using a Sun One Directory Server, change the OpenpagesIP module.
5. Specify the correct values for the following properties in the appropriate module:
   - provider.url - Change the value to the hostname and port number for the LDAP authentication server.
   - base.dn - The top level of the LDAP directory tree structure (Domain Name) on the LDAP server. If the users to be authenticated are located in multiple locations within your Active Directory structure, you will need to list all of the locations explicitly by using the distinguished names of the locations, each separated by a semi-colon.

     For example:

     ```
     base.dn="DC=LDAPTesting,DC=local;CN=Users,DC=LDAPTesting,DC=local;
     OU=Auditors,OU=External Auditors,OU=Staff,DC=LDAPTesting,DC=local"
     ```
   - user.attr.id - the attribute name of the user identifier (for example, "uid", "cn", etc.)
   - Additional custom parameters can be added by preceding them with the prefix "ctx.env." (without the quotes).

     For example, when using the Sun One Directory Server:

     ```
     OpenpagesIP
     {
        com.openpages.aurora.service.security.namespace.LDAPLoginModule
        required debug=false
           provider.url="ldap://192.168.0.169:30429"
           security.authentication="simple"
           base.dn="DC=LDAPTesting,DC=local;OU=People,DC=LDAPTesting,
           DC=local"
           user.attr.id="uid"
           ctx.env.your.param="paramvalue"
           ;
     };
     ```

     An example when using the Microsoft Active Directory server:

     ```
     OpenpagesAD
     {
        com.openpages.aurora.service.security.namespace.LDAPLoginModule
             required debug=false
           provider.url="ldap://192.168.0.165:389"
           security.authentication="simple"
           security.search.user.dn="CN=Paul Smith,CN=Users,DC=LDAPTesting,
              DC=local"
           security.search.user.credentials="openpages"
           base.dn="CN=Users,DC=LDAPTesting,DC=local"
           user.attr.id="CN"
           ;
     };
     ```
6. When you are finished editing the file, save your changes and exit.
7. Restart all services.

Results

You have configured the IBM OpenPages system to use an external LDAP user authentication server.

Configuring a Multi-Forested LDAP Authentication

IBM OpenPages supports the use of multiple LDAP authentication servers in a multi-forested configuration. If IBM OpenPages cannot find the user in the first authentication server, it will check the next server in the list and repeat until it finds the user or checks all listed authentication servers.

When listing multiple LDAP servers, the `aurora_auth.config` file must be modified to contain multiple sets of server information.

This file is located in the `<OP_Home>\aurora\conf` directory, where `<OP_Home>` is the installation location of the OpenPages application. By default, this is `c:\OpenPages`.

This is accomplished by grouping the server information by index key, as in the following example:

```
com.openpages.aurora.service.security.namespace.LDAPLoginModule required
debug=true
provider.url.1="ldap://10.128.22.106:389"
security.authentication.1="simple"
security.search.user.dn.1="CN=Administrator,CN=Users,DC=parent,DC=parentchil
d,DC=localdomain"
security.search.user.credentials.1="Op3nPag3s"
base.dn.1="DC=parent,DC=parentchild,DC=localdomain"
user.attr.id.1="CN"
provider.url.2="ldap://10.128.22.107:389"
security.authentication.2="simple"
security.search.user.dn.2="CN=Administrator,CN=Users,DC=child,DC=parent,DC=p
arentchild,DC=localdomain"
security.search.user.credentials.2="Op3nPag3s"
base.dn.2="DC=child,DC=parent,DC=parentchild,DC=localdomain"
user.attr.id.2="CN"
```

By adding a ".1" key to the end of each parameter, IBM OpenPages can parse the settings correctly and differentiate between separate LDAP server information sets. You would append a ".2" to the keys for the second LDAP server, and so on.

For single LDAP server implementations, you do not need to append an identifier to the end of the parameter names.

Chapter 4. Using System Admin Mode

This chapter contains the following topics:

About System Administration Mode (SAM)

You use System Administration Mode (SAM) to restrict user access to the IBM OpenPages application when you apply configuration changes or other updates to the system.

When System Administration Mode (SAM) is enabled:

- Only administrative users with **System Administration Mode** application permission can log on to the system. All other users are restricted from logging on.
- All Write operations are restricted, with these exceptions:
  - Reporting period operations if the Reporting Schema is not enabled
  - Metadata (schema) changes
  - Enumerated string conversions from single to multivalued selection
  - Setting changes that are made through the user interface

Before you enable SAM, you may want to notify application users to log off the system. If a user is already logged on to the system when SAM is enabled, the user will only be able to view objects and will not be able to create new instances of objects or save any modifications made to existing objects.

Depending on your configuration, SAM mode may not start until all asynchronous background jobs run to completion (see "Running Asynchronous Background Jobs and Administrative Functions" on page 332).

You must be in System Administration Mode (SAM) if you:

- Want to perform any of the actions on the Reporting Schema list view page (such as create, re-create, enable, or drop a reporting schema). For Reporting Schema details see, "Administering the Reporting Schema" on page 59.
- Have an existing Reporting Schema and want to add, remove, or refresh a reporting period.
- Have configuration changes to make to the system, such as changes to the object model hierarchy or modifications to object types, field groups, and object fields.
- Are converting an enumerated string value from a single selection to a multi-value selection (see "About Data Types" on page 111 for multi-value conversion details).

In all other instances you can make configuration changes without enabling SAM. However, there may be situations where you want to enable SAM to restrict general user access. For example, if you need to modify one or more object text labels, you may not want users to create new instances of the object type while you are making these changes.

Enabling and Disabling System Admin Mode

Note: You must have the **System Administration Mode** application permission set on your account to view the **System Admin Mode** link at the top of a page and the **System Admin Mode** menu item from the **Administration** menu.

The setting for System Administration Mode are:

If Link...	If button...	Use to...
Enabled	Enable	enter System Administration Mode
Disabled	Disable	exit and terminate System Administration Mode

The link switches between **Enabled** and **Disabled**, and the button switches between **Enable** and **Disable** depending on which mode it is in.

If the system is processing operations that require System Admin Mode, you will have to wait until processing is complete before you can disable System Admin Mode.

Procedure

1. Log on to the OpenPages application user interface as a user with the **System Administration Mode** application permission set.
2. Do one of the following:
   - Click the **System Admin Mode Enabled** or **Disabled** link at the top of a page
   - From the menu bar, select **Administration** and click **System Admin Mode** and click **Enable** or **Disable**.
3. At the prompt, click **OK** to change modes.

Chapter 5. Managing the Reporting Schema and Framework

This chapter contains the following topics:

Administering the Reporting Schema

The IBM OpenPages application supports the use of a "real-time" reporting schema model that allows CommandCenter reports to access information as it is entered into the IBM OpenPages system. Users no longer need to export their data to an external reporting database repository.

System administrators will only need to re-create their reporting schema after changing their object schema. There is no need to restart the IBM OpenPages application after regenerating the reporting schema.

The Reporting Schema page is used to control the creation and deletion of the reporting schema. It is usable by administrative-level users who have the Reporting Schema application permission.

About Permissions

Before performing any actions on a reporting schema, you should have the following application permissions set on your account (for details, see "Configuring Application Permissions" on page 18):

This Application Permission...	Is used to...
Reporting Schema	access the **Reporting Schema** menu item.
System Administration Mode	enable and disable System Administration Mode.
Reporting Framework	update the reporting framework.

Accessing the Reporting Schema

Important: The system must be in System Administration Mode (see Chapter 4, "Using System Admin Mode," on page 57) to make any modifications to the reporting schema.

Procedure

1. Log on to the IBM OpenPages application user interface as a user with the **Reporting Schema** application permission set.
2. From the menu bar, select **Administration** and click **Reporting Schema**.

Results

From the Reporting Schema detail page, you can create, re-create, disable, drop, and view the status of a reporting schema.

About Updating the Reporting Schema

The IBM OpenPages application allows users to create a new or updated reporting schema when necessary.

Any of the following changes to the application would require an update to the reporting schema:

- Configuring the triangles setting (see "Configuring Triangle Object Relationships" on page 315)
- Changing the value of the 'Populate Past Periods' setting (see "Populating Past Reporting Periods" on page 61)
- Changing any setting that is used to compose the URL links in the Reporting Schema (such as the 'Host', 'Port', and 'Protocol' settings, see "Updating URL Host Pointers for CommandCenter Reports" on page 387)
- Adding an index to an RT_ column (done through the setting 'Create Index on Fields').

  Note: The 'Create Index on Fields' setting is located on the Settings page under the **OpenPages | Platform | Reporting Schema** folder.

There are two ways to update the reporting schema:

- Incrementally through scripts - contact your IBM representative for assistance in executing special PL/SQL scripts that will incrementally update the reporting schema. These scripts are maintained by IBM OpenPages Support and do not ship as part of the product.
- Application user interface - this method updates the entire reporting schema (see "Creating or Re-creating the Reporting Schema"). It is a good idea to schedule this activity ahead of time, since creating a reporting schema requires that the application be in System Administration Mode. In this mode, users are not able to log onto the system and users who are currently logged in are not able to commit changes to the repository.

Note: Depending on your changes, recreating the reporting schema and updating the reporting framework (for CommandCenter reports) may not cause your modifications to appear in the standard (out-of-the-box) reports. You may also need to modify the existing reports or create new reports to display the additional information (such as adding new fields).

Creating or Re-creating the Reporting Schema

The following procedure describes how to use the IBM OpenPages application user interface to create or re-create the reporting schema.

Procedure

1. Access the Reporting Schema page (see "Accessing the Reporting Schema" on page 59).
2. Enable System Administration Mode (for details, see "Enabling and Disabling System Admin Mode" on page 58).
3. As needed, either create a new reporting schema or re-create the existing reporting schema. Do one of the following:

- If a reporting schema already exists - drop the existing schema before creating the new schema. Click the **Re-Create** button to drop the existing schema and create a new schema.
- If no reporting schema exists - click the **Create** button to create a new reporting schema.

4. When the creation task (or re-creation task) is completed, update the Reporting Framework so that the CommandCenter reports can access the new schema. For details, see "Updating the Reporting Framework" on page 64.

Populating Past Reporting Periods

By default, the reporting schema is only populated with the data from the current reporting period. The **Populate Past Periods** setting controls whether data from previous reporting periods is included in the reporting schema.

Procedure

1. From the menu bar, select **Administration** and click **Settings**.
2. Expand the **OpenPages | Platform | Reporting Schema** folder hierarchy.
3. Click the **Populate Past Periods** setting to open its details page.
4. In the **Value** field, type one of the following values:

If the value is set to...	Then...
true	The reporting schema is populated with the data from previous reporting periods. **Note:** Turning this setting on will add to the amount of data that is published by the Reporting Schema operation and will increase the time it takes to drop and recreate the Reporting Schema.
false	The reporting schema is populated with the data from the current reporting period. This value is set by default.

5. When finished, click **Save**.
6. Recreate the reporting schema (see, "About Updating the Reporting Schema" on page 60).

Enabling and Disabling the Reporting Schema

Creating a new reporting schema automatically enables the reporting schema, while dropping the reporting schema automatically disables it.

When the reporting schema is 'Enabled', the database tracks changes to the application data and allows the reporting engine to access the updated data. When the schema is 'Disabled', the database no longer tracks changes to the application data, but is still aware of changes to the schema (such as new fields).

Note: You must be in System Administration Mode (SAM) to enable the buttons that allow you to perform these tasks.

Enabling the Real-time Reporting Schema

Procedure

1. Enable System Administration Mode (for details, see "Enabling and Disabling System Admin Mode" on page 58).

2. From the menu bar, select **Administration** and click **Reporting Schema**.
3. Click the **Enable** button to enable the reporting schema. A reporting schema must be created in order to enable the reporting schema using the **Enable** button.
4. If one does not exist, click the **Create** button to create the reporting schema. Creating the reporting schema will automatically enable the new schema.
5. Once the task is completed, disable System Administrator Mode.

Disabling the Real-time Reporting Schema

Procedure

1. Enable System Administration Mode (for details, see "Enabling and Disabling System Admin Mode" on page 58).
2. From the menu bar, select **Administration** and click **Reporting Schema**.
3. If you want to reclaim the database space taken by the reporting schema tables, you must click the **Drop** button**.** This will automatically disable the reporting schema. Otherwise, continue to the next step.
4. Click the **Disable** button to disable the reporting schema. A reporting schema must be created in order to disable the reporting schema using the **Disable** button.
5. Once the task is completed, disable System Administrator Mode.

Viewing Reporting Schema Operation Details

The IBM OpenPages application keeps a log of each reporting schema operation that has been performed.

Procedure

1. Access the Reporting Schema page (see "Accessing the Reporting Schema" on page 59).
2. On the **Reporting Schema Operations** tab, click the name of the operation in the list.
3. On the **Operation Detail** tab, click the **View Log** button.

   The log message detail page appears.

About Using the Reporting Framework

Users with the correct permissions can use the reporting framework to do the following:

- Update the reporting framework when the real-time reporting schema is updated (see "Generating the Reporting Framework" on page 63)
- Configure facts and dimensions for object types in the dimensional namespace

Accessing the Reporting Framework

Important: To update or configure the reporting framework, you must NOT be in System Administration Mode (for more information, see Chapter 4, "Using System Admin Mode," on page 57).

Before you begin, make sure the correct application permissions are set on the user account as follows:

To do this...	Requires this application permission...
Update all or selected components of the reporting framework	Reporting Framework
Configure facts and dimensions	Reporting Framework Configuration

Procedure

1. Log on to the IBM OpenPages application user interface as a user with the correct application permission set.
2. From the menu bar, select **Administration**, point to **Reporting Framework**, and click one of the following:
   - **Generation** — to update all or selected components of the reporting framework, such as metadata, labels, dimensions and facts, and custom query subjects.
   - **Configuration** — to configure facts and dimensions, object type dimensions, and date dimension types.

Generating the Reporting Framework

About the IBM OpenPages Reporting Framework V6

IBM OpenPages Reporting Framework V6 supports two data models:

- A relational model based upon the object types defined in your system and their relationship to each other
- A dimensional model based upon facts and dimensions selected for each object type.

When the Reporting Framework V6 is generated, the `OPENPAGES_REPORTING_V6` package is published to the CommandCenter server with the following default namespaces:

- `DEFAULT_REL` — this relational namespace is similar to the framework model included with previous versions of IBM OpenPages but has been reorganized for easier access and higher performance.
- `DEFAULT_DIM` — this dimensional namespace is organized into facts and dimensions, and gives report authors access to Analysis Studio and the online analytical processing (OLAP) features that are available in CommandCenter.

Using the query subjects and query items in these namespaces, report authors can create a variety of reports with faster execution from within IBM OpenPages .

About Backward Compatibility with the Legacy Reporting Framework

For systems that have been upgraded from versions of IBM OpenPages 5.x or earlier and want to continue to use the Legacy Reporting Framework for certain reports, **Legacy Framework Generation** options are available.

About Choosing Update Options in the Reporting Framework

When you generate the Reporting Framework V6 and/or the Legacy Reporting Framework, you can choose to update all or particular components of the reporting framework. Table 7 on page 64 lists the various options for updating the reporting framework.

Table 7. Reporting Framework Generation Options

This option...	Is available in this Reporting Framework...	And does this...
Framework Model	• Reporting Framework V6 • Legacy Reporting Framework	Generates the relational model for all your object types.
Labels	• Reporting Framework V6 • Legacy Reporting Framework	Imports your object text into the reporting framework.
Facts and Dimensions	Reporting Framework V6	Generates the dimensions and facts in the dimensional model.
Custom Query Subjects	Reporting Framework V6	Generates any custom query subjects that are defined.

When you update the reporting framework, any changes to the reporting schema are reflected in CommandCenter. Once the reporting framework model in CommandCenter is updated, report authors can create new (or modify existing) reports based on these changes. If the reporting framework is not updated, external reports such as those built with CommandCenter will not be able to access the updated reporting schema.

Example

Let's say you add two new fields to a Risk object type and add a new child or parent relationship to a Control object type. You also want users to be able to run reports that contain these new fields or relationships.

To make these changes available to a report author in the CommandCenter tool, you would update the reporting framework through the administrative application interface.

Once the CommandCenter reporting framework is updated, a report author could then create new (or modify existing) reports that contained the new fields or relationships.

About Regenerating the Reporting Framework

If you make any of the following changes in the IBM OpenPages application, you must regenerate the reporting framework:

- Adding a new field to a field group
- Adding a new object type
- Adding a new association between object types

Important: Whenever you Update the reporting framework, you need to revalidate reports. Failing to do so may result in reporting errors.

Updating the Reporting Framework

Once the reporting schema has been updated, the reporting framework must be updated as well to propagate the changes to the CommandCenter reports.

Note: For purposes of this procedure, we are assuming that you have just created a new reporting schema.

Procedure

1. Access the **Reporting Framework Operations** page (see "Accessing the Reporting Framework" on page 62).
2. Disable System Administration Mode if it is enabled (for details, see "Enabling and Disabling System Admin Mode" on page 58).
3. On the Reporting Framework Operations page, click **Update**.
4. In the Reporting Framework Generation window, do the following:
   a. Under **Framework Generation**, select the **Framework Model** and **Labels** options (and any additional options you want) for generation in the Reporting Framework V6 relational data model.

      Note: For upgraded systems that have the Legacy Reporting Framework setting enabled, if you also want to generate the Legacy Reporting Framework relational data model, under **Legacy Framework Generation**, select the **Framework Model** and **Labels** options.
   b. Click **Submit** to begin the update procedure.

      You are returned to the Reporting Framework Operations page with the new task listed in the Reporting Framework Operations table.
5. To view the progress of the update, click **Refresh**. The Percent Complete column on the Reporting Framework Operations table will update the percentage of completion.

Viewing Reporting Framework Details

You can view the details of a refresh operation, including any errors that were encountered.

Procedure

1. Access the Reporting Framework page (see "Accessing the Reporting Framework" on page 62).
2. On the **Reporting Framework Operations** tab, click the name of the operation in the list.
3. On the **Operation Detail** tab, click the **View Log** button.

   The log message detail page appears.
4. If a sub-operation exists, it is listed in the **Sub Operations** table of the detail page.
   a. To view sub-operation details, click the name of the sub-operation.
   b. To view log details, click the **View Log** button.

Changing the Administrator Logon Account and Framework Generation

The Reporting Framework Generator, by default, uses the Super Administrator account (set during initial installation) as the CommandCenter logon account to update the reporting framework model (for details about Administrator accounts, see "About Administrators" on page 9).

If you change the logon user name and/or password of the Super Administrator account after installation (using the application interface), you must make the corresponding changes in the `framework.properties` file on the CommandCenter server.

If a mismatch exists between the logon user name and/or password and the specified user name and/or password in the property file, the Reporting Framework Generator will not be able to log on to CommandCenter to update the reporting framework.

The procedure to manually change the CommandCenter framework generator property file follows.

Procedure

1. Log on to the CommandCenter server as a user with administrative permissions.
2. Stop the `OpenPages Framework Model Generator` service.
3. Navigate to the `CommandCenter|framework|conf` folder.
   By default, the path is:

   Windows `C:\OpenPages\CommandCenter\framework\conf`
   AIX `/opt/OpenPages/CommandCenter/framework/conf`

4. Locate the `framework.properties` file in the `conf` folder and do the following:
   a. Make a backup copy of the file before modifying it.
   b. Open the `framework.properties` file in a text editor of your choice.
   c. Locate the following code lines in the file:

      ```
      op.password=<password value>
      op.user=OpenPagesAdministrator (this is the default user)
      ```

      Where: `<password value>` is the password that corresponds to the user account value in the `op.user` property.
   d. Edit the password property with the new value (the new password will be in clear text). If you also changed the user account, edit that value as well.
   e. When finished, save the change to the file.
5. Restart the `OpenPages Framework Model Generator` service.

   Note: The passwords will be automatically re-encrypted the next time the service accesses the files.
6. Update the reporting framework (see "Updating the Reporting Framework" on page 64).

Configuring Facts and Dimensions

About Facts and Dimensions

Facts and dimensions are components of a dimensional data model. Dimensionally-modeled data works well with crosstab and graphical reports (such as charts and maps).

Facts are fields with a numeric data type (such as Currency, Integer, Decimal) that can be aggregated and analyzed. For each fact that is selected for inclusion in the dimensional model, you can also use the **Fact Types** setting to globally control the types of aggregations that can be created for each configured fact field (see "Reporting Framework Configuration Settings" on page 318).

Dimensions include enumerated fields, date fields, and dependent picklists that can be used by report authors as business filters and grouping fields.

You can control which facts and dimensions are represented in the dimensional namespace for each object type that can be used by report authors in reports.

Process Overview

Table 8 provides an overview of the configuration tasks for setting up facts and dimensions and a reference to the related information.

Table 8. Tasks for Configuring Reporting Fragment Fields

✓	Task Description	Related Topic
☐	For the selected object type, configure the facts you want available for reports in the dimensional namespace.	"Enabling and Disabling Facts"
☐	If the object type has enumerated fields and dependent picklists, configure the dimensions you want in reports for these fields and picklists in the dimensional namespace.	"Enabling and Disabling Enumeration and Dependent Picklist Dimensions" on page 68
☐	If wanted, configure the types of date dimensions you want available for reports in the dimensional namespace.	"Using Date Dimension Types" on page 70
☐	Update the Reporting Framework V6 to effect changes to facts and dimensions.	"Updating the Reporting Framework" on page 64

Enabling and Disabling Facts

If an object type includes fields with a numeric data type (such as Currency, Integer, Decimal) then these fields are automatically listed in the **Facts** table for selection. For example, fact fields for a Risk object type might include such fields as 'Inherent Frequency' (a decimal data type field) and 'Inherent Severity' (a currency data type field).

When regenerating the reporting framework to effect the changes made to fact fields, you can choose the 'Dimensions and Facts' option to regenerate and update only that portion of the reporting framework that has changed.

Note: When you disable facts that were previously enabled, any reports that used these facts will no longer run.

Procedure

1. Do one of the following to access facts and dimensions for an object type:

From the Administration menu, select this...	And then do this...
Reporting Framework then Configuration	From the list on the **Facts and Dimensions** table, click the name of the object type you want. **Note:** To access this menu item, you must have the **Reporting Framework Configuration** application permission set.

From the Administration menu, select this...	And then do this...
Object Types	1. From the list on the **Object Types** table, click the name of the object type you want. 2. Navigate to the **Facts and Dimensions** table, and click **Edit**.

2. Under the **Facts** table, do one of the following:
   - To enable a fact, select the box next to each fact you want included in the reporting framework.
   - To disable a fact, clear the box next to each fact you want excluded from the reporting framework.
3. When finished, click **Save**.
4. At the prompt, click **OK**.
5. Update the reporting framework to effect the changes (see "Updating the Reporting Framework" on page 64).

Enabling and Disabling Enumeration and Dependent Picklist Dimensions

If an object type includes fields with an Enumerated String data type, then these fields are automatically listed under the Enumerated Fields column in the **Enumeration and Dependent Picklist Dimensions** table for selection as dimensions. For example, enumerated fields for a Risk object type might include such fields as 'Category' (a single value selection field) and 'Domain' (a multivalued selection field).

All dependent picklists that have been defined in the application user interface (including any disabled picklists) for a selected object type are automatically displayed under the Dependent Picklists column in the **Enumeration and Dependent Picklist Dimensions** table.

Note:

- Disabling an enumerated field or dependent picklist that was previously enabled as a dimension, will cause any reports that used these dimensions to no longer run.
- Enabling a dependent picklist as a dimension automatically enables the parent enumerated field, which is located in the same row as the dependent picklist. A dependent picklist cannot be enabled as a dimension without the parent enumerated field also being enabled.
- Disabling an enumerated field as a dimension will also disable all child dependent fields.
- If you disable a dependent picklist as a dimension, the parent enumerated field remains enabled.
- A dependent picklist that is disabled for an object type cannot be selected as a dimension.

Procedure

1. Do one of the following to access facts and dimensions for an object type:

From the Administration menu, select this...	And then do this...
Reporting Framework then Configuration	From the list on the **Facts and Dimensions** table, click the name of the object type you want. **Note:** To access this menu item, you must have the **Reporting Framework Configuration** application permission set.
Object Types	1. From the list on the **Object Types** table, click the name of the object type you want. 2. Navigate to the **Facts and Dimensions** table, and click **Edit**.

2. Under the **Enumeration and Dependent Picklist Dimensions** table, do one of the following:

To do this...	Then...
Enable an enumerated field as a dimension	Under the **Enumerated Fields** column, select the box next to each enumerated field you want included as a dimension in the reporting framework.
Disable an enumerated field as a dimension	Under the **Enumerated Fields** column, clear the box next to each enumerated field you want excluded as a dimension from the reporting framework.
Enable a dependent picklist as a dimension	1. Under the **Dependent Picklists** column, select the box next to the picklist you want included as a dimension in the reporting framework. 2. In the same row as the dependent picklist, under the **Enumerated Fields** column, select the box next to the parent enumerated field if is not already selected.
Disable a dependent picklist as a dimension	1. Under the **Dependent Picklists** column, clear the box next to the picklist you want excluded as a dimension from the reporting framework. 2. In the same row as the dependent picklist, under the **Enumerated Fields** column, clear the box next to the parent enumerated field if not wanted as a dimension.

3. When finished, click **Save**.
4. At the prompt, click **OK**.
5. Update the reporting framework to effect the changes (see "Updating the Reporting Framework" on page 64).

Using Date Dimension Types

When date fields are used as dimensions in reports, users could, for example, drill down through a date hierarchy from the year to a specific quarter, month, and/or day.

For date fields to be used as dimensions, you must first define a date dimension type then map that dimension to the date fields of an object type. The date dimension types that you define are globally available for all object type date fields.

If wanted, you can localize the name of a date dimension type for display in the reporting framework. If no translated text is provided, the value that is typed into the **Name** field for a date dimension type is automatically used.

By default, the following system date fields are available under the Date Dimensions table for all object types but are not automatically configured with a date dimension type:

- Creation Date
- Last modification Date

Note: If a system date field is configured with a date dimension type, it applies to all object types.

Adding a Date Dimension Type

When you define a date dimension type, that dimension is available for selection on all date fields for any object type. See Table 9 on page 71 for a list and brief description of each date dimension type.

Procedure

1. From the **Administration** menu select **Reporting Framework**, and then **Configuration**.
2. On the **Date Dimensions Type** table, click **Add**.
3. In the **Name** box, type a name for this date dimension.
4. If wanted, localize the text of the **Name** field for display in the reporting framework as follows.

   Note: If no localized display text is specified, the value in the **Name** field is used by default.

   a. Click the **Translate** link.
   b. In the Translate window, next to each language you want, type the localized text into the box.
   c. When finished, click **Apply**.
5. In the **Description** box, optionally type some descriptive text.
6. Click the arrow next to each dimension you want for this date type and select a value.

   Note: Only one value can be selected from the list for each type of date dimension.

Table 9. Date Dimension Types

Date Type	Description
Year	Returns the calendar year of the field. **Example** : 2010
Quarter	Returns the quarter within the calendar year. **Example** : 'Quarter' would return '3' for the month of August.
Month	Depending on the selection, will return either a numeric or text string for the month. **Example** : 'Month of Year' would return '8' for the month of August.
Week	Depending on the selection, will return the number of the week for either the month, quarter, or year based on a starting criteria. **Example** : 'Week of Year (Starts on Sunday)' would return '33' for August 18, 2010.
Day	Depending on the selection, will return either a numeric or text string for the day of the week, month, quarter, or year based on an optional starting criteria. **Example** : 'Day of Year' would return '230' for August 18, 2010.

7. When finished, click **Save**.
8. If wanted, map the date dimension to an object type's date fields. See "Mapping Date Dimension Types to Date Fields."

Mapping Date Dimension Types to Date Fields

After you create a date dimension type, you can then map that dimension to one or more date fields for an object type.

Each column in the **Date Dimensions** table represents a defined date dimension type, and each row represents a date field for the selected object type.

Procedure

1. Do one of the following to access facts and dimensions for an object type:

From the Administration menu, select this...	And then do this...
Reporting Framework then Configuration	From the list on the **Facts and Dimensions** table, click the name of the object type you want. **Note:** To access this menu item, you must have the **Reporting Framework Configuration** application permission set.
Object Types	1. From the list on the **Object Types** table, click the name of the object type you want. 2. Navigate to the **Facts and Dimensions** table, and click **Edit**.

2. On the **Date Dimensions** table, for each date field in a row, select one or more date dimension types represented in a column.

   Note: To select or clear a value from a row, click the name of the value.
3. When finished, click **Save**.
4. At the prompt, click **OK**.
5. Update the reporting framework to effect the changes (see "Updating the Reporting Framework" on page 64).

Enabling and Disabling a Date Dimension Type

When you disable or re-enable a date dimension type, that date dimension type is disabled or re-enabled for all date fields in any object type.

Note: When you disable a date dimension type, any reports that used that date dimension type will no longer run.

Procedure

1. From the **Administration** menu select **Reporting Framework**, and then **Configuration**.
2. In the **Date Dimension Types** table, navigate to the row containing the date dimension type you want to disable or re-enable.
3. Under the **Actions** column in the same row for that date dimension type, do one of the following:

To do this...	Click this link...
Disable a date dimension type	Disable
Enable a previously disabled date dimension type	Enable

   Note: The link toggles between 'Disable' and 'Enable' depending on the selected action.
4. At the prompt, click **OK**.
5. Update the reporting framework to effect the changes (see "Updating the Reporting Framework" on page 64).

Modifying a Date Dimension Type

If wanted, you can modify a date dimension type after you create it. Perhaps, for example, translated text needs to be modified or added, or a previously selected value needs to be changed.

Note: When you modify a date dimension type, any reports that used that date dimension type will no longer run.

Procedure

1. From the **Administration** menu select **Reporting Framework**, and then **Configuration**.
2. In the **Date Dimension Types** table, click the name of the date dimension type you want to modify to open its detail page.
3. Make the changes you want.
4. When finished, click **Save**.
5. At the prompt, click **OK**.

6. Update the reporting framework to effect the changes (see "Updating the Reporting Framework" on page 64).

Deleting a Date Dimension Type

When you delete a date dimension type, that date dimension type is permanently removed from the system on all date fields for any object type and cannot be retrieved.

Note: When you delete a date dimension type, any reports that used that date dimension type will no longer run.

Procedure

1. From the **Administration** menu select **Reporting Framework**, and then **Configuration**.
2. In the **Date Dimension Types** table, navigate to the row containing the date dimension type you want to delete.
3. Under the **Actions** column in the same row for that date dimension type, click the **Delete** link.
4. At the prompt, click **OK**.
5. Update the reporting framework to effect the changes (see "Updating the Reporting Framework" on page 64).

Configuring Recursive Object Levels

If you want reporting capability in the dimensional data model of the reporting framework, you can use recursive object types to create sets of levels that will be reflected in the reporting framework for use by report authors.

A recursive object type can repeat itself indefinitely or until some set limit is reached. The following object types are recursive within the IBM OpenPages application:

- Business Entity (SOXBusEntity)
- Sub-Process (SOXSubprocess)
- Sub-Account (SOXSubaccount)
- Sub-Mandate (Submandate)

About Recursive Object Levels

For each recursive object type, you can define multiple object levels. For the Business Entity object type, you can also create multiple sets of recursive object levels with each set having a different number of levels.

Recursive object levels allow you to create a representation of corporate data using common names for each level of the set thereby providing the report author with additional context for creating reports (see Table 10 on page 74).

When the Reporting Framework V6 is generated, all levels that have been defined for recursive object types are reflected in the dimensional data model of the reporting framework. These structures allow report authors to create, for example, drill-down dimensional reports where users can progressively navigate through the levels to more detailed data.

For a finer level of control, if wanted, you can also specify which recursive object level sets you want available in a given namespace (see "Configuring Namespaces in the Reporting Framework" on page 311).

Note:

- You cannot delete Level1 for non-entity recursive object types.
- If you remove or edit levels in a set, reports that used these levels will no longer run.

Example

A report author works for Global Financial Services (GFS), a large multinational bank, with an organizational structure that is comprised of many business functions and groups. The report author has a requirement to create reports so business users at GFS can assess the risks associated with various processes that go across the company's business units. GFS has its business organized around functions, divisions, departments, and units.

To return data about the various business processes and their associated risks for each organizational level of the business, you might create a new set of recursive object levels for the Business Entity object type called 'Risk Assessment' with the following levels as shown in Table 10.

Table 10. Sample Recursive Object Levels

Level number	Level name	Example Business Entity instance user data
1	Group	Global Financial Services
2	Global Function	Client Markets
3	Division	Asia
4	Department	Underwriting
5	Unit	Japan

In addition to defining the business levels of the organizational structure for the Business Entity object type, you need to determine which business entity should be the starting point for scoping the data. In this example, we want the reporting data to start at the Global Function level. In the 'Starting Entity' field, you would type: `/Global Financial Services`

When the reporting framework is updated, a new 'Risk Assessment' folder with the corresponding level folders and query items would be created within the `OpenPages_Reports_V6` package under the `GRC Objects|Business Entity Folder` for report authors to use in creating CommandCenter reports.

Rules for Defining Sets of Recursive Object Levels

The following rules apply to the definition of sets of recursive object levels:

- Business Entity — this is the only recursive object type where you can define multiple sets of recursive object levels with a different starting entity for each set. Sets of Business Entity recursive object levels can also be edited and deleted.

  By default, no recursive object levels are predefined for Business Entity object types.

- All other recursive object types (Sub-Process, Sub-Account, Sub-Mandate) have only one set of recursive object levels that, by default, is predefined and cannot be deleted.

  By default, each of these recursive object types (excluding Business Entity) have a predefined first level that cannot be deleted but can be renamed.
- Each set of recursive object levels for the Business Entity object type requires a name and a root path.
- The name of each user-defined level must be unique across all recursive object types.
- The names of sets and levels can be localized.

Working With Business Entity Recursive Object Levels

For the Business Entity object type, you can define and delete sets of recursive object levels, and modify the levels within each set.

By default, the Business Entity object type does not have any predefined sets of recursive object levels.

When the Reporting Framework V6 is generated, all user-defined sets of recursive object levels are available to report authors under the `GRC_OBJECTS|SOXBUSENTITY_FOLDER` folder in the default dimensional namespace. In addition, this structure is also available in the IBM OpenPages administrator interface when configuring object type dimensions (see "Configuring Object Type Dimensions" on page 77).

Defining Business Entity Recursive Object Levels

Use the following instructions to create multiple sets of recursive object levels for generation in the Reporting Framework V6.

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list of object types, click the **SOXBusEntity** (Business Entity) link to open its detail page.
3. Navigate to the **Recursive Object Levels** table and click **Edit**.
4. In the definition pane, do the following:

Table 11. Recursive Object Levels Definition Boxes

In this box...	Do this...
Name	Type a name for this set of levels.
Description	Optionally type a description of this set.
Starting Entity	Type the full path, beginning with a slash, to the starting Business Entity. **Note:** If wanted, you can use a single slash (/) to specify all top level (Level 1) business entities.
Level 1	Type a unique name for this level.

5. To add another level to this set, click the  (plus symbol) button and type a unique name for this level. Repeat this step for each level you want to add to this set.

Note: To remove a level that was added, click the  (minus symbol) button.

6. If wanted, localize the text for the names of the set and levels for display in the reporting framework as follows.

   Note: If no localized display text is specified, the values in the **Name** and **Level** fields are used by default.

   a. Click the **Translate** link.
   b. In the Translate window, for the language you want, type the localized text into the box.
   c. When finished, click **Apply**.
7. To add another set, click **Add** and repeat Steps 4 - 6.
8. When finished, click **Save**.
9. At the prompt, click **OK**.
10. To specify which recursive object level set you want available in a given namespace, configure the `Entity Recursive Object Levels` setting (see "Configuring Namespaces in the Reporting Framework" on page 311).
11. When finished, update the reporting framework to effect the changes (see "Updating the Reporting Framework" on page 64).

Deleting Business Entity Sets of Recursive Object Levels

Note: When you delete a set of recursive object levels for a Business Entity, all the levels that have been defined for that set are deleted and any reports that used these levels will no longer run.

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list of object types, click the **SOXBusEntity** (Business Entity) link to open its detail page.
3. Navigate to the **Recursive Object Levels** table and click **Edit**.
4. Navigate to the pane with the set you want to delete, and do the following:
   a. Click the **Delete** link.
   b. At the prompt, click **OK**.
5. When finished, click **Save**.
6. At the prompt, click **OK**.
7. Update the reporting framework to effect the changes (see "Updating the Reporting Framework" on page 64).

Modifying Recursive Object Levels

You can add and remove levels in a set for all recursive object types.

Note:

- You cannot delete Level1 for non-entity recursive object types.
- If you modify existing recursive object levels in a set, reports that used these levels will no longer run.

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list, click the name of the recursive object type you want to modify.
3. On the **Recursive Object Levels** table, click **Edit**.
4. In the definition pane, make the required changes.

   To add or remove levels, do the following:

If you want to do this...	Then...
Add another level to the set	Click the  (plus symbol) button and type a unique name for this level.
Remove a level that was added	Click the  (minus symbol) button.

5. When finished, click **Save**.
6. At the prompt, click **OK**.
7. Update the reporting framework to effect the changes (see "Updating the Reporting Framework" on page 64).

Configuring Object Type Dimensions

To enhance report authoring capability in the dimensional data model, you can define object type dimensions.

About Object Type Dimensions

Object type dimensions allow report authors to represent associations between object types as a dimension in the reporting framework. The object types do not have to be directly associated.

Example

A report author works for Global Financial Services (GFS), a large multinational bank, with an organizational structure that is comprised of many business functions and groups. The report author has a requirement to create a report that shows aggregate test results and their associated controls for each division of the company.

The typical parent-child path in an object hierarchy between Business Entity and Test Result objects types is: Business Entity - Process - Risk - Control - Test - Test Result.

To skip object types in the hierarchy and create an association between Business Entity and Control objects, you could define an object type dimension called 'Entity-Control.'

Since you already created a set of recursive object levels for the Business Entity object type (as shown in Table 10 on page 74), you could use the 'Division' recursive object type level as a filter for the starting object type followed by the Control object type.

If wanted, you can localize the name of the object type dimension for display in the reporting framework. If no translated text is provided, the value that is typed into the **Name** field for the object type dimension is automatically used.

When the Reporting Framework V6 is generated, the 'Entity-Control' object type dimension would be available to report authors under the `OBJECT_TYPE_DIMENSIONS` folder in the `DEFAULT` dimensional namespace.

About Selecting a Starting Object Type for a Dimension

The following rules apply to the selection of an object type as a starting point for object type dimensions:

- Any object type can be selected as the starting object type.
- For the Business Entity object type, you can select a recursive object level as a starting point (for details on recursive object levels, see "Defining Business Entity Recursive Object Levels" on page 75).

Adding Object Type Dimensions

Use the following instructions to define object type dimensions for generation in the Reporting Framework V6.

Procedure

1. From the **Administration** menu select **Reporting Framework**, and then **Configuration**.
2. On the **Object Type Dimensions** table, click **Add**.
3. In the **Name** box, type a name for this object type dimension.
4. If wanted, localize the text of the **Name** field for display in the reporting framework as follows.

   Note: If no localized display text is specified, the value in the **Name** field is used by default.

   a. Click the **Translate** link.
   b. In the Translate window, next to each language you want, type the localized text into the box.
   c. When finished, click **Apply**.
5. In the **Description** box, optionally type some descriptive text.
6. Click the **Starting Object Type** arrow and select an object type or a recursive object level (if defined for Business Entity object types) from the list, then click **Go**.
7. To add another object type to this dimension, do the following:
   a. In the **Selected Object Types** table, under the **Actions** column, click the **Choose Object Type** link.
   b. In the Choose Object Type window, select an object type then click **Apply**.
   c. Repeat Steps a and b to add another object type to this dimension.
8. When finished, click **Create**.
9. Update the reporting framework to effect the changes (see "Updating the Reporting Framework" on page 64).

Modifying Object Type Dimensions

If wanted, you can modify an object type dimension after you create it. Perhaps, for example, translated text needs to be modified or added, or a previously selected object type in a level needs to be changed.

Note: If you modify object types in an existing object type dimension, reports that used this object type dimension will no longer run.

Procedure

1. From the **Administration** menu select **Reporting Framework**, and then **Configuration**.
2. From the list in the **Object Type Dimensions** table, click the name of the object type dimension you want to modify.
3. Make the changes you want (see Table 12).

Table 12. Modifying an Object Type Dimension

If you want to...	Then do this...
Change an object type	Click the **Choose Object Type** link above the object type you want to change and make another selection. **Note:** When you change an object type, all previously selected levels below that level are also deleted.
Delete a level	Click the **Choose Object Type** link above the object type level you want to delete and clear the selection box. **Note:** When you delete a level, all levels below that level are also deleted.
Change or add translation text for the **Name** field	Click the **Translate** link to open the Translate window.

4. When finished, click **Save**.
5. At the prompt, click **OK**.
6. Update the reporting framework to effect the changes (see In the **Description** box, optionally type some descriptive text.

Enabling and Disabling Object Type Dimensions

If wanted, you can disable and then re-enable an object type dimension at a later time.

Note: When you disable an object type dimension, reports that used this object type dimension will no longer run.

Procedure

1. From the **Administration** menu select **Reporting Framework**, and then **Configuration**.
2. In the **Object Type Dimensions** table, navigate to the row containing the object type dimension you want to disable or re-enable.
3. Under the **Actions** column in the same row for that object type dimension, do one of the following:

To do this...	Click this link...
Disable an object type dimension	Disable

To do this...	Click this link...
Enable a previously disabled an object type dimension	Enable

Note: The link toggles between 'Disable' and 'Enable' depending on the selected action.

4. At the prompt, click **OK**.
5. Update the reporting framework to effect the changes (see "Updating the Reporting Framework" on page 64).

Deleting Object Type Dimensions

When you delete an object type dimension, that object type dimension is permanently removed from the system and cannot be retrieved.

Note: When you delete an object type dimension, reports that used this object type dimension will no longer run.

Procedure

1. From the **Administration** menu select **Reporting Framework**, and then **Configuration**.
2. In the **Object Type Dimensions** table, navigate to the row containing the object type dimension you want to delete.
3. Under the **Actions** column in the same row for that object type dimension, click the **Delete** link.
4. At the prompt, click **OK**.
5. Update the reporting framework to effect the changes (see "Updating the Reporting Framework" on page 64).

Chapter 6. Managing Reports

This chapter contains the following topics:

The IBM OpenPages application contains a set of reports that allows users with the correct permissions to quickly view and organize information about the current state of your, for example, financial, compliance, or operational project. For example, users can quickly view information grouped by either user, by location, or view.

Accessing Reports

Accessing Reports From the Application User Interface

You can access reports from the IBM OpenPages application user interface (typically `/openpages`).

Procedure

1. From a browser window, log on to the IBM OpenPages application user interface.
2. Select **Reporting** on the menu bar and choose a report from the list. A separate browser window opens with the selected report.

   If you selected the 'All Reports' option, the Reports page is displayed. From the list on the Reports page, click the name of the report you want to launch.

   Note: Depending on your configuration, application, and permissions, you may see different reports and folders.
3. If this is a "scoped" report, at the prompt, choose the object where you want the report to run from. For example, if you select a business entity, then the report will use the selected business entity as the starting point and limit the scope of the report to all objects contained below that entity.

   If the report is not scoped, it will run as soon as you click the name of the report.

About Supplied Reports

The IBM OpenPages application comes with a selection of predefined reports that allow you to quickly view important information about your project. The IBM OpenPages application contains the following supplied reports (grouped by folder).

Note: The following list of reports are for a fresh installation of the IBM OpenPages application. If you have additional reports tailored to your particular

business needs or have upgraded from an earlier version of the IBM OpenPages application, the classification of the supplied reports may differ from that documented in this guide.

IBM OpenPages V6 Folder Reports

The IBM OpenPages V6 folder contains a number of sub-folders (listed in the following sections) and the following report, which resides at the top level of the reporting hierarchy:

Report Name	Description
All Documentation	Detailed view of an organization's entity hierarchy, associated internal controls documentation, and counts of related issues, files and links in the current reporting period. This is filtered by business entity. There are detailed sub-reports for each count.

Administrative Reports Folder

Report Name	Description
Checked Out Files	Listing of attached Files in a checked out state in the current reporting period. You can sort by: - Name of File - Full Path of the folder where the File is stored - User who has the File checked out - Date the File was checked out.
Disassociated Objects	Listing of objects that do not have associated parent objects in the current reporting period. You can filter for specific object types and can sort by: - Name of object - Full Path of the folder where the object is stored.

Audit Reports Folder

In addition to the reports listed in the following table, the Audit Reports Folder contains the following sub-folders:

- Configuration (see “Configuration Folder” on page 85)
- Security (see “Security Folder” on page 85)

Report Name	Description
Audit Change	Lists all object changes that fulfill the user's run-time filtering criteria. Users can filter the report on Business Entity, Start Time/End Time, specific object type, and status. For an explanation of audit events and the values in the **Status** and **Item** columns of the report, see "Description of Audit Change Events and Values."
Audit Summary	Administrative summary of changes to documentation data, filtered by date/time range. You can also filter by Business Entity and object type and drill into a detailed Audit sub-report.

Description of Audit Change Events and Values

An audit event is a combination of an action and object aspect (that is, the object, a relationship, or attribute of the object) that was affected by the event. The Audit Change report exposes change events for any field value change.

Note: This information also applies to the detail sub-report from the Audit Summary report. If you did not upgrade to OpenPages 5.5 CommandCenter reports, see "About Audit Trail Reports for customers who did not upgrade to OpenPages 5.5 CommandCenter reports [QC 2269]" on page 84.

To fully understand the nature of each type of audit event it is useful to have the context of how objects are created, associated, and shared.

In the hierarchy of objects in the system, a child object (such as a Control) may be associated to more than one parent object (such as a Risk). Conversely, any one parent object (such as a Risk) may have several associations to different child objects (such as Controls). These associations or relationships are flagged as one of two types--either *Primary* or *Non-Primary*.

Although any one parent object (such as a Risk) may have multiple child objects (such as Controls), for any given child object the system allows only one of the object's parent-child relationships to be marked as "Primary". Primary associations are used to determine the path the system should follow when executing a number of operations that require object hierarchy traversal.

In the IBM OpenPages application, the following operations traverse the Primary Association path:

- SCOR rule execution
- Cascade Delete (including those requested by SCOR delete rules)
- Sign-offs, Locking and Un-Locking
- Hierarchical copy and move

In general, Audit Trail Reports are "parent object centric" when reporting on events that pertain to an object's associations. This means that for a given object, all association-related events are those where the object acts as a parent. Events where the object acts as a child are reported in context of the corresponding parent objects.

Table 13 lists the various audit change values that are listed in the **Action** column of the Audit Change Report with a brief description of the value and the affected object aspect.

Table 13. Audit Change Report Values

If the Status column has this value...	And the Item column has this value...	Then it indicates that...
Added	Association	An object was associated as a child object in the hierarchy.
	Object	A new object was created in the repository.
	Version	A new version of the object was created in the repository.
Changed	<property name>	The value of an object's system or extended property was modified.
Removed	Object	The object was logically deleted from the repository.
	Association	An object was removed as a child object.
Removed Primary	Association	The association has been changed to Non-Primary. This could happen if the user selects another object relationship to be the Primary parent-child association or the current Primary association was deleted.
Added Primary	Association	The association type has been set to Primary as described in the above section. This first association will always be set to Primary

About Audit Trail Reports for customers who did not upgrade to OpenPages 5.5 CommandCenter reports [QC 2269]

Table 14 describes object-related audit events exposed in the Audit Trail Reports for the following object system attributes only:

- Object Name
- Object Description
- Object storage folder (parent folder) location

Table 14 lists the various audit change values that are listed in the **Action** column of the Audit Change Report with a brief description of the value and the affected object aspect.

Table 14. Audit Change Report Values Prior to IBM OpenPages Version 6.1.0

Audit event operation (ACTION)	Audit event Object Aspect (WHICH_PROPERTY)	Explanation
CREATION	OBJECT	An object was created in the repository.
CREATION	VERSION	A new object version was created in the repository.
DELETION	OBJECT	The object was logically deleted from the repository.
CHANGE	<PROPERTY NAME>	Object's system or extended property value was modified.

Table 14. Audit Change Report Values Prior to IBM OpenPages Version 6.1.0 (continued)

Audit event operation (ACTION)	Audit event Object Aspect (WHICH_PROPERTY)	Explanation
ADDITION	ASSOCIATION	Object has been associated to a child object in the hierarchy.
DELETION	ASSOCIATION	Object was disassociated from another object in the hierarchy.
PROMOTION TO PRIMARY	ASSOCIATION	The association type has been set to Primary as described above. This first association will always be set to Primary.
DEMOTION TO NON-PRIMARY	ASSOCIATION	The association has been changed to Non-Primary. This could happen if the user selects another object relationship to be the Primary parent-child association or the current Primary association was deleted.

Configuration Folder:

Report Name	Description
Configuration Audit	Lists all configuration changes made to the IBM OpenPages application during the chosen date range.

Security Folder:

Report Name	Description
Administrator Permissions	Lists each administrator and their granted permissions for each Security Domain they administer.
Security Domain Role Assignments	Lists each Security Domain to which the selected roles are assigned.
Login Activity Summary	Lists all users who have accessed the IBM OpenPages system during the specified date range. Each user is listed with the last login time, when they last changed their password, and how many times they logged in.
Login Activity Log	Lists all user activity during the specified date range. Report users can filter on date range, operation (log in/log out), login status (Failed/Succeeded), and number of login attempts.
Roles by Security Domain	Lists each role assigned to the selected Security Domain.
Roles by User	Lists each user and group with their assigned role for the selected Security Domain.
User Role Assignments	Lists all the roles in the system with the assigned user or group for each Security Domain.

Issue Reports Folder

Report Name	Description
Issue List	Detailed listing of Issues and associated parent objects, filtered by reporting period and Business Entity. **Note:** This report shows a subset of the Issues present in the system. To appear in this report, Issues must be associated with objects that are accessible through direct relationships in the default namespace. For example, Issues associated with Controls that are indirectly associated with a Risk Assessment will not appear, while Issues associated with Risks that are directly associated in a chain, from Business Entity to Process or Sub-process to Control Objective, will appear.
Issues and Action Items	Lists Issues and associated Action Items for the chosen reporting period and Business Entity. **Note:** This report shows a subset of the Issues and Action Items present in the system. To appear in this report, Issues must be associated with objects that are accessible through direct relationships in the default namespace. For example, Issues associated with Controls that are indirectly associated with a Risk Assessment will not appear, while Issues associated with Risks that are directly associated in a chain, from Business Entity to Process or Sub-process to Control Objective, will appear.

Workflow Reports Folder

Report Name	Description
Active Tasks	Administrative listing of all active workflow jobs and the corresponding task name, creation date and assignee, grouped by Job.
Jobs and Tasks	Displays information about the jobs and tasks in the system (such as task status, task owner, job initiator, job identifier). Allows you to filter the results by Job ID, Job Type, Initiator, and a date range for when the job was created.

Adding CommandCenter Reports

About Adding CommandCenter Reports

To run a CommandCenter report from the IBM OpenPages application user interface, the CommandCenter report must have a corresponding report page published on the IBM OpenPages application server.

A report page does the following:

- Adds a link on the Reporting menu and All Reports page to launch the CommandCenter report from the IBM OpenPages application user interface
- Specifies the parameters for launching the report
- Specifies the keys used for localizing the report name and description in the IBM OpenPages application user interface

All CommandCenter Studio report pages are based on the `CommandCenter Report Redirect` page template, and all Go! Dashboard report pages are based on the `CommandCenter Dashboard Redirect` page template. These templates are located at the root of the 'Reporting' publishing channel on the IBM OpenPages server.

You can use one of the following methods to add new CommandCenter reports to the IBM OpenPages application user interface.

- **IBM OpenPages application user interface** - this method automatically generates the required report page and application text keys. This is the recommended method and requires IBM OpenPages 5.5 or later. For details, see "Using the Application User Interface to Add CommandCenter Reports."
- **IBM OpenPages server administrator interface** - this method involves using the publishing channels facility on the IBM OpenPages server to manually create the required report page and publish the report. This method is typically used for editing report pages, troubleshooting publishing issues, and for versions of IBM OpenPages prior to 5.5. For instructions on manually creating and publishing Report Pages, see "Manually Creating a New Instance of a Report" on page 91.

Using the Application User Interface to Add CommandCenter Reports

When you add a CommandCenter report from the IBM OpenPages application user interface, the following occurs:

- A corresponding report page is automatically generated on the IBM OpenPages server based on the `CommandCenter Report Redirect` page template.
- The report is published, by default, to the U.S. English locale.
- If the report name and description are not specified for a locale, the values in the U.S. English locale are used by default.
- Report name and description application text keys are automatically created in the 'Miscellaneous' folder on the Application Text page and populated with the specified values.

  These key values are used for localizing the report name and description on the 'My Reports' section of the Home page and on the Reporting menu and page. To modify these key values, see "Localizing Application Text" on page 238.

Example

A new unpublished CommandCenter report was created called 'My Control Summary' that resides in the 'OPENPAGES_SHARED' folder on the CommandCenter server. You want to publish the report to make it available for users in the U.S. English and Japanese locales.

From the 'Reports' page in the IBM OpenPages application, you click 'Add' and select the report from the listing. For the U.S. English locale (this locale is automatically selected by default), you type in 'My Control Summary' for the report name, and 'All controls assigned to me' as the description for the report. You then select the Japanese locale and type in a localized name and description.

The application text keys for the 'My Control Summary' report that are automatically generated under the 'Miscellaneous' folder on the Application Text page may look similar to these:
`report.name.openpages.shared.my.control.summary` and
`report.description.openpages.shared.my.control.summary`.

If wanted, you can use these keys to modify the report name or description that is displayed on the application user interface for a locale.

Before You Begin

Before you can add a CommandCenter report from the IBM OpenPages application user interface, you must have the following information available:

- The name of the report
- A description of the report
- The path and name of the folder to be deployed (the folder selection will be filtered to list report folders only). By default, the path is `/_cw_channels/Reporting/SOX`.

Limitations

Publishing report pages from the application user interface has the following limitations:

- You can publish only one report at a time.
- If you want to edit existing reports, you must use the publishing channels facility on the OpenPages server (for details, see "Modifying an Existing Report Template" on page 94).
- If the initial publishing process failed to publish a report to any locale other than English, you must use the publishing channels facility on the OpenPages server to add that report (for details, see "Manually Creating a New Instance of a Report" on page 91).

Accessing the Publish Report Page

Note: To access the **Add** button on the Reports page, you must have the **Add Pages** application permission set on your account (for details, see "Configuring Application Permissions" on page 18).

Procedure

1. From a browser window, log on to the IBM OpenPages application user interface as a user with the **Add Pages** application permission set.
2. From the menu bar, select **Reporting** and click **All Reports**.
3. Click **Add** to go to the Publish Report page.

Publishing a CommandCenter Report From the Application User Interface

The Report selection list contains all available CommandCenter reports that are not already published.

Procedure

1. Access the Publish Report page (see "Accessing the Publish Report Page").
2. Click the Report arrow and select a report from the list.
3. Select the check box for each locale in which you want the report to display. For example, German. The U.S. English locale is selected by default.
4. In the **Name** field for each selected locale, type the display name of the report.

This name will be displayed to users in the report selection list and on the Reports page, and, if configured on the Home page, in a tab or in a pane on the Classic tab.

5. In the **Description** field for each locale, type a description of the report. This description will be displayed to users on the Reports page.

   Note: Any locale for which you do not specify a localized name and description will, by default, contain the U.S. English name and description.

6. When finished, click **Save**.

   After the report is published, a link to launch the report is displayed on the Reports page along with a description of the report, and the report name is added to the list of selections on the Reporting menu.

About Modifying the Displayed Report Name or Description

You can localize and/or modify the name and description that is displayed to users on the IBM OpenPages for a report in a given locale. You do this by locating the application text keys that correspond to the name and description of the report and then modifying the value in the key for that locale.

For more information and instructions, see "About Modifying Display Text in the Application User Interface" on page 240.

Working With Reports

The information described in this section requires access to the IBM OpenPages server administrator interface.

Before you begin

Note: The applet in IBM OpenPages Server (typically `/opx`) requires the Java Runtime Environment 6 installed on the client where you launch the Internet Explorer.

Procedure

1. Launch Internet Explorer.
   a. If you already have 64-bit Java 6 installed, launch 64-bit Internet Explorer.
   b. If you already have 32-bit Java 6 installed, launch 32-bit Internet Explorer.
2. When you navigate to the pages in IBM OpenPages Server that requires the Java applet, a dialog displays asking you to run the applet.
   a. Click **Run** to run the applet.
   b. If you do not have Java installed on the client side, when you navigate to the pages in IBM OpenPages Server that requires the Java applet, you are prompted to install Java Runtime Environment 6 Update 11. Click **Install** to proceed with the installation.

      Once the installation is done, the browser automatically resumes and prompts you to run the applet on the browser.

      Note: The Internet Explorer Enhanced Security Configuration should be disabled in order to allow the installation of Java.

Understanding Reports

Reports are generated by combining report pages and page templates that provide necessary information about the filtering and sorting of the report contents, as well as the displayed name and description of the report.

Reports (both CommandCenter and JSP) are represented in a publishing channel by a page template which lists the parameters that the source file needs in order to create a report. A report page is an instance of a page template, and contains a set of values for the parameters specified in the page template.

In this manner, a single page template can be supplied with multiple sets of values for its parameters. This allows the IBM OpenPages application to create multiple reports based on the same layout and internal logic. Each report page represents a report as viewed in the IBM OpenPages application.

Report pages and page templates reside on the IBM OpenPages server.

Note:

- CommandCenter reports can be published through the application user interface. This method automatically generates a corresponding report page and application text keys for localizing the selected report. For details, see "About Adding CommandCenter Reports" on page 86.
- Reports that are placed under the `Reporting/SOX` folder structure on the application server are published to the U.S. English locale. To publish to a different locale, choose the `/SOX` folder under the locale you want (for example, `ja_JP/SOX` for the Japanese locale).
- All CommandCenter report pages are based on the `CommandCenter Report Redirect` page template, which is located at the root of the 'Reporting' publishing channel on the IBM OpenPages server.

Locating Report Files

Report files (such as report pages, page templates, and JSP reports) are located in the OpenPages repository on the OpenPages server.

The OpenPages repository handles the data storage and access capabilities for the IBM OpenPages application. In order to create, modify, or delete IBM OpenPages reports, you must have an IBM OpenPages account with permission to modify publishing channels. If you are not sure whether you have access to this functionality, see your IBM OpenPages Administrator for additional information.

Accessing Report Pages and Page Templates

Note: The following procedure applies to JSP reports and CommandCenter report pages.

Procedure

1. From a browser window, log on to the IBM OpenPages server (typically `/opx`) as a user with the correct Reporting permissions.
2. Click the **Browse channels** link under the **Publishing** heading in the left navigation Action menu. This displays a list of the available publishing channels.

Note: If you cannot see the Publishing heading, you do not have the correct permissions. See your IBM OpenPages Administrator.

3. Click the **Reporting** folder. A list of files and folders is displayed.

   Each folder represents a report grouping in the IBM OpenPages user interface. Each 'Page' file represents an IBM OpenPages report.

Manually Creating a New Instance of a Report

To manually create a new instance of a report, you must log on to the OpenPages server, and create a new report page based on a copy of an existing page template. The new report page will display clickable links in the IBM OpenPages application user interface for running the new report.

Note: The following procedure applies to JSP reports and CommandCenter report pages.

Note:

- CommandCenter reports can be published through the application user interface. This method automatically generates a corresponding report page and application text keys for localizing the selected report. For details, see "About Adding CommandCenter Reports" on page 86.
- Reports that are placed under the `Reporting/SOX` folder structure on the application server are published to the U.S. English locale. To publish to a different locale, choose the `/SOX` folder under the locale you want (for example, `ja_JP/SOX` for the Japanese locale).
- All CommandCenter report pages are based on the `CommandCenter Report Redirect` page template, which is located at the root of the 'Reporting' publishing channel on the IBM OpenPages server.

Identify the Page Template

Procedure

1. From a browser window, log on to the IBM OpenPages server (typically /opx) as a user with the correct Reporting permissions.
2. If you already know which page template you want to use, skip to the next task.

   Otherwise, do the following to determine which existing report page you want to copy from or use as the basis of the new report page:

   a. Click the **Browse channels** link under the **Publishing** heading in the Action menu.

   b. Click the **Reporting** channel link and navigate through the folder structure to the IBM OpenPages report you want to copy or use and modify as the basis of a new report.

   c. Click the name of the report page to open its detail page.

   d. In the **General Information** table on the detail report page, note the value of the **Template** field. You will need to either reference this template or make a copy of the referenced template.

Create a Report Page

Procedure

1. Click the **Browse channels** link in the Action menu.
2. Click the **Reporting** channel link and navigate to the folder where you want the report page to be created.

For example, a report page for a new CommandCenter report in the U.S. English locale would be placed in the `Reporting/SOX/OpenPages V6` folder.

If wanted, create a category folder for grouping the reports under the appropriate `/SOX` folder. For example, to create a new report grouping titled 'My Custom Reports' on the Reporting menu and Reports page in the IBM OpenPages application for the U.S. English locale, you could create a folder with the path `Reporting/SOX/My Custom Reports`. Any report pages placed in the folder will appear under that grouping in the reporting sections of the IBM OpenPages application.

3. Click the **Add Page** button at the top of the window.
4. In the 'Describe page' step of the **Add a Page** wizard, do the following:
   a. Type an informative name and description for the report.

      Note: You will not be able to change the name of a report after it is created.

   b. Choose the page template you will use to create the report.

      Note: The report pages for all CommandCenter reports developed in IBM Cognos:

      - Analysis, Query, or Report Studio use the `CommandCenter Report Redirect` page template
      - Go! Dashboard use the `CommandCenter Dashboard Redirect` page template.

   c. Click **Next**.
5. If this is a dashboard, skip to Step 6; if this is a JSP report, skip to Step 7.

   Otherwise, for a Studio report based on the `CommandCenter Report Redirect` page template, in the 'Specify page contents' step in the **Add a Page** wizard, do the following.
   a. Select a value for each of the following fields:

Table 15. CommandCenter Report Redirect Selection Fields

Field Name	Description
Report Type	The IBM Cognos Studio application used to develop the report. Valid values are: • `report` (for Report Studio, this is the default value) • `query` (for Query Studio) • `analysis` (for Analysis Studio) • `pagelet` (a type of dashboard that can contain multiple content pieces, including reports, on a single page)
Open with	The method for opening the report. Valid values are: • `CognosViewer` — opens the report in view-only mode, this is the default value; required for the 'pagelet' report type • `ReportStudio` — opens the report in Report Studio so it can be modified • `QueryStudio` — opens the report in Query Studio so it can be modified • `AnalysisStudio` — opens the report in Analysis Studio so it can be modified

Table 15. CommandCenter Report Redirect Selection Fields (continued)

Field Name	Description
Report Format	The display format for the report. Valid values are: • `HTML` (this is the default value) • `PDF` • `XLS` • `XLWA`
Show prompt page	Determines whether or not a prompt page is always displayed for a report. If the value is set to: • `Yes` — a prompt page is always displayed even if the report has no required prompts. • `No` — a prompt page only displays if it is required by the report design. This value is set by default.

b. Skip to Step 8.

6. For a dashboard based on the `CommandCenter Dashboard Redirect` page template, in the 'Specify page contents' step in the **Add a Page** wizard, do the following.
   a. Click the **Mode** arrow and select the method for opening the dashboard.
      Valid values are:
      • view (opens the dashboard in view-only mode, this is the default value)
      • edit (opens the dashboard in Go! Dashboard so it can be modified)
   b. Skip to Step 8.
7. For a JSP report, enter the sorting and filtering information for the report.
8. Enter values for all required fields (required fields have a red asterisk *) including key field information as follows:

Table 16. Report Page Key Fields

Key Field	Format	Description
Report Name Key	report.name.<user-defined> **Example** report.name.control.analysis	A key that references an application text string for localizing the title of the report.
Report Description Key	report.description.<user-defined> **Example** report.description.control.analysis	A key that references an application text string for localizing a description of the report.

Note: You can use the values in the 'Report Name Key' and 'Report Description Key' fields on the report page to manually create custom application text keys to localize the name and description of a report after it is created. For details, see "Using the Custom Folder" on page 245.

9. Click **Apply** to save the modifications.
10. Click **Finish** to create the new report page and exit the wizard.

Results

When you log on to the IBM OpenPages application user interface, the new report should be visible in the selections on the Reporting menu and on the Reports page.

Modifying an Existing Report Template

Important: If you want to modify one of the supplied report templates for your own purposes, you must copy the report template to a new location outside the SOX folder structure, and then modify the copied template. Otherwise, you will risk losing your changes when upgrading to a newer version of the IBM OpenPages application.

Procedure

1. From a browser window, log on to the IBM OpenPages server (typically /opx) as a user with the correct Reporting permissions.
2. Click the **Browse Channels** link under the **Publishing** heading in the left navigation Action menu.
3. Navigate to the report you want to modify and click the report name to display the detail page.
4. Find the section containing the information you want to change, and click the **Edit...** button above the section. An editable version of the information is displayed.
5. Change the desired settings. For JSP reports, if you are changing the parameter sorting information, you will need to click **Apply** before clicking **Save**.

   Note: You cannot modify the name of a report. In order to change the name of a report, you must delete the mis-named report and create an identical report with the new name.

   As an alternative, you can use the values in the 'Report Name Key' and 'Report Description Key' fields on the report page to manually create custom application text keys to localize the name and description of a report after it is created. For details, see "Using the Custom Folder" on page 245.
6. When finished, click **Save**. The modified information is saved and immediately applied to the report.

Deleting a Report

You can delete an instance of a JSP report or report page for a CommandCenter report.

Procedure

1. From a browser window, log on to the IBM OpenPages server (typically /opx) as a user with the correct Reporting permissions.
2. Click the **Browse Channels** link under the **Publishing** heading in the left navigation Action menu.
3. Navigate to the report page you want to delete and select the check box next to the report name.

   Important: Do not delete a page template! If a page template is deleted, all report pages based on that template are deleted as well.
4. Once the report is selected, click the **Delete** button at the top of the table. A confirmation dialog is displayed.
5. Click **OK** to delete the report page (or JSP report instance).

Creating Interactive JSP Reports

Overview

The IBM OpenPages application allows administrative-level users with the option to create interactive reports to prompt a user at run-time for parameter values. This section is used primarily for JSP reports and explains how to modify newly-created and existing JSP reports to prompt a user for needed information.

Creating an Interactive JSP Report

You can either modify an existing JSP report to be interactive, or specify an interactive parameter during report creation. In either case, follow the procedure below to create an interactive JSP report.

Procedure

1. From a browser window, log on to the IBM OpenPages server (typically /opx) as a user with the correct Reporting permissions.
2. Click the **Browse channels** link in the left navigation Action menu and navigate to the page template for the report you want to modify.
3. Click the name of the page template you want to modify. The detail page is displayed.
4. Click the **Edit...** button above the list of report parameters. The Edit Parameters applet is displayed.
5. Click the name of the parameter that you want to make interactive. The parameter information is displayed at the bottom of the page.
6. Select the check box marked 'Interactive Value' and click the **Apply** button.
7. Repeat steps 5 and 6 for each parameter you want to make interactive.
8. When you are finished, click **Save**.

Results

The next time the report is run, the user will be prompted to enter a value for each field marked as an interactive value.

Important: Reports with an interactive parameter named 'label' are a special case and will not display a dialog to enter a value for 'label.' The 'label' field is included to support reporting periods and should not be modified.

Note: Although any parameter type can be made an interactive value, the IBM OpenPages application only supports the following four modes of entering values into the value fields when the report is run:

- Date fields
- Text entry fields
- Enumerated drop-downs
- File browsers

Unsupported types may still be marked as interactive, but the value for the field must be entered manually via a text string at run-time. A valid value must be entered into the value field for the report to return the correct set of information.

Running an Interactive JSP Report

Note: Although any parameter type can be made an interactive value, the IBM OpenPages application only supports the following four modes of entering values into the value fields when the report is run:

- Date fields
- Text entry fields
- Enumerated drop-downs
- File browsers

Unsupported types may still be marked as interactive, but the value for the field must be entered manually via a text string at run-time. A valid value must be entered into the value field for the report to return the correct set of information.

Procedure

1. From a browser window, log on to the OpenPages application user interface (typically `/openpages`).
2. Select the **Reporting** menu on the menu bar, and choose the name of the report you want to run. If the report contains interactive parameters, a prompt page is displayed.
3. Enter the required information into the various fields.
4. After all of the required information has been entered, click the **Next** button to generate the report based on the supplied information. The report is displayed in a new window.

Restricting Access to Reports

To restrict access and set security on reports, you need to set permissions in both the IBM OpenPages server interface and in the CommandCenter portal.

Note: If you restrict access to reports only through the CommandCenter portal but not in the IBM OpenPages server interface, the reports may be displayed in a selection list to users in the IBM OpenPages application user interface. If a group or user who does not have permission selects the restricted report, the report will not run and an error message will be displayed to the user.

Setting Permissions on IBM OpenPages JSP and CommandCenter Reports

You can restrict users and/or groups from accessing and running JSP and CommandCenter reports from the IBM OpenPages application by setting Read, Write, Delete, and Manage permissions on selected report folders.

For example, if you want only administrators in a 'System Administrators' group to have access to administrative reports, you could set Read, Write, Delete, and Manage access on the 'Administrative Reports' subfolder (which is under the SOX >> CommandCenter folder). Once you grant access to administrative reports for the 'System Administrators' group, you could then break inheritance on the folder to restrict other users and groups from accessing these reports.

Procedure

1. From a browser window, log on to the IBM OpenPages server (typically /opx) as a user with administrative privileges.

2. Click the **Browse channels** link under the **Publishing** heading in the left navigation Action menu. This displays a list of the available publishing channels.

   Note: If you cannot see the Publishing heading, you do not have the correct permissions.
3. Click **Reporting**. A list of files and folders is displayed.
4. Expand the folder, if necessary, and select the `/SOX` folder you want.

   Note:
   - Each folder represents a report grouping in the IBM OpenPages user interface.
   - Reports that are under the `Reporting/SOX` folder structure are published to the U.S. English locale. To select a different locale, choose the `/SOX` folder under the locale you want (for example, `ja_JP/SOX` for the Japanese locale).
5. Under the selected `/SOX` folder, do the following:
   a. Select the box next to the name of the folder containing the reports to which you want to limit access through the IBM OpenPages application user interface.
   b. Click **Properties** to open the Folder Details page.
   c. On the **Access Controls** tab, click **Edit** to open the permissions window.
6. In the **Edit Permissions** applet window, select and grant access to the groups and users you want:
   a. Click **Add** to open the user or group selection box.
   b. Select a group or user to whom you want to grant permission and click **OK**.
   c. Select the permissions you want to allow or deny the group or user (Read, Write, Delete, Manage).
   d. When finished, click **Apply**. The selected group or user appears in the list.
   e. To select another group or user, repeat Steps a-d.
   f. To remove a group or user, select the group or user then click **Remove**.
   g. When finished, click **Close**.

      The **Access Controls** tab on the Folder Details page displays the selected groups and/or users with their assigned permissions.
7. Break inheritance on the folder so other groups or users cannot access these reports from the IBM OpenPages user interface:
   a. On the **Folder Details** tab, click **Edit** to open the edit window.
   b. In the edit window, clear the **Inherit access controls from parent folder?** box.
   c. Click **OK**.

      The status of the Inherit access controls row on the Folder Details tab displays changes from 'Yes' to 'No'.

Securing Access to the CommandCenter Portal

You can restrict which user groups are allowed to modify CommandCenter reports.

Use the following instructions to allow a group, in this example the 'OPAdministrators' group, to update, add, and delete reports, and to restrict other users from changing settings within the CommandCenter portal.

Note: OpenPages standard (out-of-the-box) reports could be overwritten during an upgrade. If you want to modify OpenPages standard reports, we strongly recommend that you copy the reports to your own folder structure where you can then modify and control access to these reports.

Create a CommandCenter Group in OpenPages with Administrator Permissions

Procedure

1. From a browser window, log on to the OpenPages application user interface as a user with administrative privileges.
2. Create a group in the OpenPages application to which you want to give CommandCenter administrative rights or use an existing group (such as, 'OpenPagesAdministrators').

   Note: For information on creating groups, see the "Creating a New Organizational Group" section in the *IBM OpenPages Administrator's Guide* .
3. Continue to the next task.

Restrict User Access to Administrative Functions Within the Cognos Portal

Procedure

1. From a browser window, log on to the CommandCenter portal as a user with administrative privileges (for example, OpenPagesAdministrator)

   By default, the URL is:

   `http://<hostname>/cognos8` (if you are using port 80 for CommandCenter)

   Where: `<hostname>` is the name of the Web server machine that contains the cognos8 virtual directory.
2. Launch the IBM Cognos Administration page:
   - If the CommandCenter splash page appears, click the **Administer IBM Cognos Content** link.
   - If the IBM Cognos Connection page appears, click **Launch** then select **IBM Cognos Administration**.
3. On the **Security** tab, click the **Cognos** link in the **Directory** list.
4. On the Directory > Cognos page:
   a. Locate the 'System Administrators' group in the list.
   b. Click the **More** link in the same row as the System Administrators group.
5. Under **Available Actions** on the Perform an Action page, click the **Set members** link.
6. On the **Members** tab of the Set Properties page, click the **Add** link.
7. On the Select entries (Navigate) page, do the following:
   a. Click the **OpenPagesSecurityRealm** link to find the OpenPages group or role to access CommandCenter administrative functions.
   b. Select a group. For example, 'OPAdministrators'.
   c. Click the green arrow to add the role and then click **OK**.
8. On the **Members** tab of the Set Properties page, remove the 'Everyone' group from accessing the administrative functions as follows:
   a. Select the 'Everyone' group.
   b. Click the **Remove** link.

      Note: There is no confirmation prompt.

c. Click **OK** to save your changes.

9. Continue to the next task.

Restrict Access to OpenPages Reports in Public Folders Procedure

1. On the **IBM Cognos Connection** page, click the **Public Folders** tab.
2. On the Public Folders page, click the **More** link in the same row as the OpenPages folder for which you want to restrict access (for example, OPENPAGES_REPORTS_V6).
3. Under **Available actions**, click the **Set properties** link.
4. On the Set properties page, select the **Permissions** tab and do the following:
   a. If not already selected, select the box to 'Override the access permissions acquired from the parent entry.'
   b. Click the **Add** link (located near the bottom of the page).
5. In the Select entries (Navigate) window, click the **Cognos** link, and do the following:
   a. Select the group to be added (for example, 'System Administrators').
   b. Click the green arrow to add the role.
   c. When finished, click **OK**.
6. On the **Permissions** tab of the Set Properties page, do the following:
   a. Select the box next to the newly added group (for example, 'System Administrators').
   b. Grant the group Read, Write, Set Policy, and Traverse permissions.
   c. Remove the Write and Set Policy permissions from the other groups.
   d. Click **OK** to save your changes.

      Now, if a user logs on to CommandCenter with a user name that is not in, for example, the 'OPAdministrator' group, and the user tries to delete, change, or save a report, for example, in the 'OPENPAGES_REPORTS_V6' package, an error message is displayed to the user.
7. Continue to the next task.

Restrict End Users From Running Report Studio and Query Studio but Still Run OpenPages Reports

Follow the steps in this task to restrict user access from within the Cognos portal to run Report Studio and Query Studio tools to modify CommandCenter reports.

Procedure

1. If not already logged on to the CommandCenter portal, log on to the CommandCenter portal as a user with administrative privileges (for example, OpenPagesAdministrator) and launch the IBM Cognos Administration page:
   - If the CommandCenter splash page appears, click the **Administer IBM Cognos Content** link.
   - If the IBM Cognos Connection page appears, click **Launch** then select **IBM Cognos Administration**.
2. Select the **Security** tab, and click the **Cognos** link in the **Directory** list.
3. On the Directory > Cognos page, click the **More** link in the same row as the 'Authors' role.
4. On the Perform an action page, under **Available Actions**, click the **Set members** link.
5. On the **Members** tab of the Set properties page, click the **Add** link.

6. On the Select entries (Navigate) page, do the following:
   a. Click the **OpenPagesSecurityRealm** link.
   b. Select the group you want (for example, OPAdministrators).
   c. Click the green arrow to add the group and then click **OK**.
7. On the **Members** tab of the Set Properties page:
   a. Select the 'Everyone' group
   b. Click **Remove**.
   c. Click **OK** to save the changes.
8. Repeat Steps 2 - 6 for the 'Query User' role.
9. When finished, return to the IBM Cognos Administration page and select the **Security** tab.
10. On the **Security** tab, click the **Capabilities** link, and do the following:
    a. Click the **Report Studio** link.
    b. Click the **Actions** arrow next to **HTML Items in Report** and select **Set properties**.
11. On the Set properties - HTML Items in Report page, do the following:
    a. Select the **Permissions** tab.
    b. If not already selected, select the box to 'Override the access permissions acquired from the parent entry.'
12. In the list on the **Permissions** tab, select the 'Everyone' group and grant the group Execute and Traverse permissions. Click **OK** to save the changes.

    Note: If the 'Everyone' group is not listed, then add it to the list as follows:
    a. Click the **Add** link.
    b. On the Select entries (Navigate) window, click the **Cognos** link.
    c. Select the 'Everyone' group.
    d. Click the green arrow to add the role.
    e. When finished, click **OK**.
    f. Select the 'Everyone' group and grant the group Execute and Traverse permissions.
    g. Click **OK** to save the changes.
13. Return to the **Security** tab and do the following:
    a. Click the **Capabilities** link again.
    b. Click the **Report Studio** link.
    c. Click the **Actions** arrow next to **Create/Delete** and select **Set properties**.
14. On the Set properties - Create/Delete page, do the following:
    a. Select the **Permissions** tab.
    b. If not already selected, select the box to 'Override the access permissions acquired from the parent entry.'
    c. Remove the 'Everyone' group, if it is listed there.
    d. Add the 'System Administrators' group with Read, Write, Set Policy, and Traverse permissions.
    e. Click **OK** to save the changes.

Results

After making the changes defined in this section, when a user logs on to CommandCenter, unless the user is a member of a group with proper

authorization, the user cannot modify reports but can still run out-of-the-box reports.

Chapter 7. Configuring Fields and Field Groups

This chapter contains the following topics:

About Fields and Field Groups

A field group is a container for fields and each field you create must belong to a field group. The IBM OpenPages GRC Platform application allows administrators to add new fields to object types (such as Business Entities, Processes, Risks, Controls, and so forth) and custom forms, and manage existing fields.

To extend the fields of an object type, you can either add new fields to an existing field group that you previously created, or create a new field group and then add these new fields to that group.

A field group is identified in the application by the Field Group  icon, and an object field is identified by the Object Field icon.

About Fields

An object field generally represents a particular item of information specific to an object type.

Fields can be object fields, computed fields, and/or report fragment fields.

By default, each object type within the IBM OpenPages GRC Platform application has a predefined field group that contains predefined fields specific to that object type. For example, the 'Effectiveness Rating' and 'Operating Effectiveness' fields belong to the Control object's `OPSS-Control` field group.

Fields can be added to new or existing field groups and then associated with a profile for display in various views.

If you create a new object type for a custom form or survey, you must add field groups to that object type. Field groups can be new field groups that you create, existing field groups, or some combination of both. For more information see, "Adding an Object Type for a Custom Form" on page 155.

Important: Do not use the four-byte characters as defined in the CJK Unified Ideographs EXTENSION-B Unicode Block Name (such as 𠂆, 𠂇, 𠂈, 𠂉, 𠂊, 𠂋, 𠂌, 𠂍, 𠂎, 𠂏 and 𠂐) in field values as these characters will not be saved.

Definition of a Field Group That is In Use

When a field group is associated to an object type, an instance of that object type is created and the field group is considered to be 'in use'. Once a field group is in use, you cannot delete the field group or any fields from that field group.

For example, let's say you create a new field group (called Extra Fields) with three object fields (called Field 1, Field 2 and Field 3). You then add the new field group to the Risk object type - even if you never display any of the three new fields on any Risk object's view page - the "Extra Fields" field group is now considered to be 'in use' and cannot be deleted.

Note: If the same management operation is being concurrently modified by another administrator, an error message is displayed requesting that you try again at a latter time.

Accessing the Field Groups Page

An administrator with the Administration **Field Groups** application permission can access the **Field Groups** menu item.

Procedure

1. From a browser window, log on to the IBM OpenPages GRC Platform application user interface as a user with the **Field Groups** permission set.
2. From the menu bar, select **Administration** and click **Field Groups**.

   From the **Field Groups** list page, you can:
   - Add a new field group
   - Delete a field group that is not in use (no instances of that object were created)
   - View descriptive information about a field group
   - Access the details page of a field group where you can:
     - Modify field group information
     - Add or delete unused field definitions from a field group
     - Access the details page of a field definition where you can manage the configuration of its properties, such as the default value or field entry requirement. If a field group includes fields with enumerated strings, you can also add new values to the list of enumerated string values, modify the display order of values in the list, and hide existing values that no longer reflect your current business needs.

Process Overview

Figure 6 on page 105 illustrates the flow of tasks for adding new fields to an object type and then displaying the new fields.

Fields can be object fields, computed fields, and/or report fragment fields.

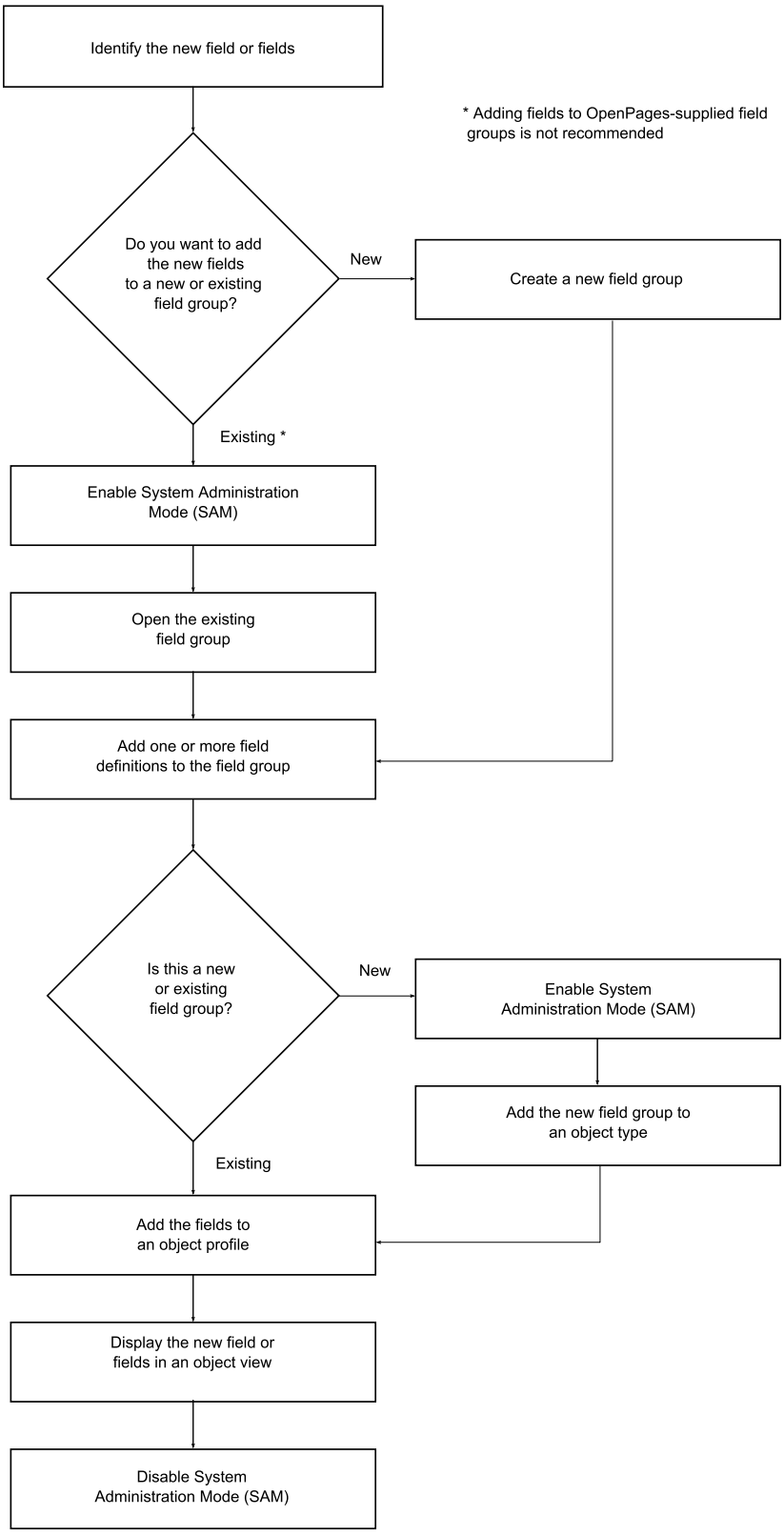


Figure 6. Tasks for Configuring New Fields

Table 17 on page 106 provides a reference for where to find information related to the various configuration tasks.

Table 17. Tasks for Configuring New Fields

Task	Task Description	Related Topic
1	Identify the new field.	See “Identifying New Fields” for a discussion of the type of information you need to identify before you create a new field.
2	Add a new field group or identify the existing group to which you want to add the field.	See “Adding New Field Groups” on page 110 for step-by-step instructions on how to create a new field group that will contain the new field (or fields).
3	Add one or more field definitions to the field group.	See “Adding Field Definitions to a Field Group” on page 110 for instructions on how to add new field definitions to a new field group.
4	If you created a new field group, add it to the appropriate object type.	See “Including Field Groups for an Object Type” on page 146 for information about how to add the new field group to a particular object type or custom form object type so the fields can be available for display.
5	Display the new field or fields in an object view.	See “About Object Type Views” on page 194 for information on selecting an object view, displaying the new field or fields in the selected view, modifying the display order of the fields in that view, and configuring a display type.

Identifying New Fields

Before you create a new field, you need to determine the characteristics of the field and identify the object types that will use the new field. Planning your changes ahead of time helps to minimize the necessary work and prevents duplication of effort.

The following list will help you identify some of the information you need to have before you create a new field:

- The affected object - Will the new field be added to a custom form or object? If an object, which object type or types will the new field be added to?
- The name - How will the new field be identified? The name of the field is important because it is also the initial label that will appear next to the field. Note that special characters cannot be used. For additional discussion, see “Considerations When Naming New Fields” on page 108.
- The label - What text will be displayed whenever this field appears on an object’s view page? The initial label text is the same as the name of the field. For example, if this field is added to the detail view page of an object, it will also appear on the add and edit pages for that object. If the field is added to a folder or list view, it will appear in those views. You can modify the label text at a future time (for details see the chapter, Chapter 11, “Localizing Text,” on page 235).

- The data type - What is the type of data (such as Boolean, Date, Enumerated String, Simple String, Reporting Fragment, and so forth) that will be captured by the field? For details see, "About Data Types" on page 111.
- The entry type - Will the user be required to enter data into the field or will data entry be optional? For details see, "Making Fields Either Required or Optional" on page 121.
- A default value - Will the field have a default value or will it be blank?
- The number of fields that will be included in the field group - how many new fields will the new field group contain? If you are creating more than one new field for an object, you may want to consider categorizing collections of object field definitions in the same field group for ease of maintenance.
- The object view - Which view page or pages (Detail, Folder, or List) will display the new field? Note that a custom form or survey can only have a detail view page. For details see, "About Object Type Views" on page 194.
- The display order - Where on a view page do you want the new field displayed? What field or fields should be listed before or after the new field? If no display order is set, the new field will automatically be displayed at the end of the list of fields. For details see, "Setting the Global Display Order of Object Types" on page 181.

Example

Suppose you want to add an 'Owner' field to several object types. You can either modify the field group for each object type by adding an 'Owner' field, or you can simply create a generic 'Owner' field and field group for all object types and re-use it later if you want to add it to an object.

To simplify the work, let's follow the generic approach and create a generic field that can be added to any object type.

The new field needs a field group and a generic name, so let's call the field group 'Custom Fields' and the name of the field 'Owner'. The name of the field is important because it is the initial label that will appear next to the field wherever the field displays in the application. If necessary, you can modify the label text at a future time. For details on modifying label text, see the chapter, Chapter 11, "Localizing Text," on page 235.

The 'Owner' field will be used to capture a name, so the data type for this field will be 'Simple String.' Since the 'Owner' field is considered important, we will make it a required field so the user must enter a name into the field before they can save and exit the page. No default value will be set for the field so the field will appear empty.

To complete the planning, let's say there are no other fields to be added to the 'Custom Fields' field group ('Owner' is the only field), and that the new 'Owner' field will only be displayed on the detail page of the Business Entity and Issue object types (this also includes the add and edit pages).

We now need to determine the display order on the Detail view page for both object types. The default order for new fields is at the end of the display list. For simplicity, let's place the 'Owner' field for both object types after the 'Modified By' field on the detail page. Because we are using the Platform schema that is supplied by default, the display order of the 'Owner' field will need to be set to '8', which is after the'Modified By' field (which is in position '7') on the Detail view page for both objects.

Now that all the necessary information has been identified, you can begin “Adding New Field Groups” on page 110 in the Task list. For details, see Table 17 on page 106.

Considerations When Naming New Fields

If you want to create an object field that you can use in reports, you need to consider the following factors when choosing a field definition name.

- Avoid using the object name in the field definition

  The IBM OpenPages GRC Platform application uses a three- or four-character prefix naming convention when generating the CommandCenter framework model. When CommandCenter reports are run, the prefix is converted to the object name in the column headers.

  Example

This prefix...	For this object type's fields...	Is displayed in a report column header as this...
RI_	SOXRisk	Risk
CN_	SOXControl	Control
TR_	SOXTestResult	Test Result

  For example, in the supplied (out-of-the-box) field definitions, the OPSS-TestResult field group contains a field named "Test Result".

  When the CommandCenter framework model is generated, the "Test Result" field becomes the query item "TR_TEST_RESULT".

  When the CommandCenter report is run, the "TR_TEST_RESULT" field column header displays as "Test Result Test Result" by default.

- Keep new field definition names to less than or equal to 20 (<=20) characters

  Note:

  – The object prefix is not counted in these 20 characters.

  – The framework generator reserves character positions 21 and 22 for a unique ID in the query item name, so field definition names that exceed 20 characters (>20) are truncated after the 20th character.

  If there are multiple long (>20 character) field definition names in which the only unique characters are beyond the 20-character limit, then recreate the Reporting Schema only when necessary. This is because the CommandCenter Reporting Schema generator may not generate the same two-digit unique ID for the same field definition from one generation to the next. As a result, reports that use these field definitions may not contain correct data as demonstrated in the following example.

  Example

This Reporting Schema generation...	For a field definition with this name...	May result in this...
Generation #1	Total Actual Financial Loss 2008	LE_TOTAL_ACTUAL_FINANCI01
Generation #2	Total Actual Financial Loss 2007	LE_TOTAL_ACTUAL_FINANCI01
Generation #3	Total Actual Financial Loss 2006	LE_TOTAL_ACTUAL_FINANCI01

If a long field definition name cannot be avoided, then try to create the name with the unique characters at the beginning of the name instead of at the end (for example, "2008 Total Actual Financial Loss" instead of "Total Actual Financial Loss 2008").

Determining the Number of Fields That Can be Added to an Object Type

Before you begin adding fields to an object type, we recommend that you run the Schema Analysis Report to determine the number of object fields that:

- Are currently configured for an object type
- Can "safely" be added to extend that object type

In general, 175 is the threshold limit for the number of fields that can be added to a given object type when the average of all field names is 22 characters in length. By keeping the average field name short, it may be possible to include more than the 175 threshold limit for the number of fields.

Important: Each currency field within an object type equates to 6 fields. This is because each currency field has 6 distinct columns within the Oracle 'RT_' table. These 6 columns equate to the following 6 fields: Amount, Currency, Exchange Rate, Base Amount, and Base Code.

The Schema Analysis Report is accessed through the CommandCenter portal. The Report lists all object types, in alphabetical order, that are in the schema. For purposes of illustration, Table 18 shows the name of each column in the Report and sample data for only the Control object type.

Table 18. Information in the Schema Analysis Report

Report Column Name	Example
Object type **Note:** All names start with the prefix 'rt_'	rt_control
Current number of fields	39
Current Field Length Statistics (Highest/Average)	22/14
Number of Additional Fields that can be added (assuming Maximum Field Lengths are used)	136
Potential Number of Additional Fields that can be added (if the Average Field Length for this Object Type does not increase)	187

Example

Let's say you want to add 3 currency fields to the Control object type. Because each currency field equates to 6 fields, you would be adding 18 fields to the Control object type (3 x 6).

Using the numbers from the 'Example' column in Table 18, the Schema Analysis Report indicates that the Control object type (rt_control) in the sample schema currently has 39 fields. Of those 39 fields, the largest field length is 22 characters, with an average field length (for all fields) of 14 characters.

The Report also indicates that you could add 136 additional fields with names that do not exceed 22 characters in length, or up to 187 additional fields if the field

names are 14 characters (or less). Adding the 3 currency fields (for a total of 18 fields) would be well within the threshold for this object type.

To run the Schema Analysis Report, use the following instructions.

Procedure

1. From a browser window, log on to the IBM Cognos 8 portal as a user with administrative privileges.

   By default, the URL is:

   `http://<hostname>/cognos8` (if you are using port 80 for CommandCenter)

   Where: `<hostname>` is the name of the Web server machine that contains the cognos8 virtual directory.
2. On the CommandCenter Home page, click the **Public Folders** tab.
3. On the Public Folders page, navigate through the links as follows:

   OPENPAGES_SHARED >> Administrative Reports
4. On the Administrative Reports page, click the **Schema Analysis Report** link to run the report.

Setting Up New Fields

Adding New Field Groups

A field group is a container for fields. Each field you create must belong to a field group.

Note:

- To perform these steps, System Administration Mode must be enabled in the application interface (see "Enabling and Disabling System Admin Mode" on page 58).
- You can add new fields to existing field groups - you do not have to create another new field group.

Procedure

1. Access the Field Groups page (see "Accessing the Field Groups Page" on page 104).
2. On the **Field Groups** table, click **Add**.
3. On the Field Groups page, do the following:
   a. In the **Name** box, type a name for the field group. For example, *Custom Fields*.
   b. In the **Description** box, optionally type a brief description of this field group.
   c. Click **Create**.
4. Add one or more field definitions to the newly created field group. For details, go to "Adding Field Definitions to a Field Group."

Adding Field Definitions to a Field Group

A field group can contain one or more field definitions. A field definition stores the data type and other properties of a field. For each new field you want to add to an object type, you must create a field definition that defines the properties of that field. You can add a field definition to a new field group or an existing field group that is not in use.

Note: To perform these steps, System Administration Mode must be enabled in the application interface (see "Enabling and Disabling System Admin Mode" on page 58).

Procedure

1. Navigate to the **Field Definitions** table of the field group you want.
2. Click **Add**.
3. On the field definition page:

Table 19. Field Definition Boxes

In this box...	Do this...
Name	Type a name for the field. **Important:** The name must start with a letter, and can only contain letters, numbers, spaces, and the underscore (_) character. Examples: `Owner, owner1, Owner1_Risk`
Description	Optionally type a description of the field.
Data Type	Select a data type for this field: 1. Click the down arrow and select a data type from the list. 2. Click the double arrows (>>) to display additional options for the selected data type. For details see, "About Data Types."
Computed **Note:** This additional option appears for most data types.	Select this box if you want this field to be a computed field. Additional boxes will be displayed. By default, the 'Computed' box is clear (not selected). For details, see, "Creating Computed Fields" on page 122.
Required **Note:** This additional option appears for all data types.	Optionally select this box if you want the field to require data entry. By default, the box is clear (not a required data entry field). For details, see, "Making Fields Either Required or Optional" on page 121.

4. Click **Create**. The new field definition is listed on the Field Definitions table of the selected field group.
5. To add another field definition to this field group, repeat Steps 2, 3, and 4.
6. When finished adding field definitions, add the field group to one or more object types. For details, go to "Including Field Groups for an Object Type" on page 146.

About Data Types

The IBM OpenPages GRC Platform application provides a variety of data types from which you can choose. Once you select a data type for a field and save it, only the parameters or settings for the data type can be modified; the data type itself cannot be changed.

To display additional parameters for a selected data type, click the double arrow

button next to the data type selector.

Table 17 on page 106 contains a description of the available data types with their corresponding settings.

Table 20. Data Types and Descriptions

Data Type	Description
Boolean	A logical operator that has the following predefined values: **true** (default) or **false**. To change the default value, click the **Default Value** arrow and select another value from the list.
Currency	• **Include Conversion** - this setting controls whether or not the exchange rate and base amount conversion are visible. If this value is set to: – **True** -- the following sub-items are displayed in the currency field (this is the default setting): Local Currency Code (drop down) Local Amount (text input) Exchange Rate (text input) Base Code (static text) Base Amount (static text) For example, you could use this setting when the field represents a currency amount relative to a specific point in time where the exchange rate is applicable, such as a financial loss on a given date. – **False** -- the following sub-items are displayed in the currency field: Local Currency Code (drop down) Local Amount (text input) For example, you could use this setting when the field represents a hypothetical currency amount not relative to a specific point in time, such as Inherent Severity on the Risk object. • The currency data type accepts numeric values with decimal places for the following settings: **Setting** Description **Minimum Value** The lowest allowable currency value that will be accepted for this field. **Maximum Value** The greatest allowable currency value that will be accepted for this field. If a user enters a value that is either below or above the specified value range, an error message displays. **Note:** • The Minimum Value and Maximum Value settings are expressed in terms of the base currency (base currency is set during installation). • You cannot use non-numeric characters when entering currency values. For example, either 125000 or 125,000 is legal, but not $125000. This format is set per user locale. For more information about working with currency, see "Using Currency Data" on page 116.
Date	The date data type default value is blank and this value cannot be changed. (The date picker pop-up box defaults to the current date.)

Table 20. Data Types and Descriptions (continued)

Data Type	Description
Decimal	The decimal data type accepts numeric values with decimal places for the following settings: **Setting** Description **Minimum Value** The lowest allowable decimal value that will be accepted for this field. **Maximum Value** The greatest allowable decimal value that will be accepted for this field. **Default Value** The default value of the field is blank. To display a default decimal value in the field, type a numeric value that is between the minimum and maximum allowable values. If a user enters a value that is either below or above the specified value range, an error message displays.

Table 20. Data Types and Descriptions (continued)

Data Type	Description
Enumerated String	The enumerated string data type accepts a list of string values and has the settings: **Setting** Description **Add Value** A string value that you want in a list of values. To add a value to the list: 1. In the Add Value box, type a string value. 2. Click Add. 3. To add another value to the list, repeat Steps 1 and 2. To remove a value from the list, select the value then click Delete only if the field is not in use. **Multi-valued** Sets whether or not a user is allowed to select more than one value from the list. If the box is: **Cleared** only one value can be selected from the list. This is the default setting. **Selected** multiple values can be selected from the list. You can convert a single value selection setting to a multi-value selection setting. You cannot convert a multi-value selection setting to a single value selection. **Default Values** The field, by default, is empty and has no value. To display a default value from the list, click the arrow and select a value from the list. To re-order the list of values, see "Modifying Enumerated String Values" on page 130. To set the display of the enumerated string data, such as a list, radio buttons or check boxes, you must do it through the profile, see "Configuring Display Types for Enumerated Strings" on page 232.

Table 20. Data Types and Descriptions (continued)

Data Type	Description
Integer	The integer data type accepts numeric values without decimals for the settings: **Setting** Description **Default Value** The field, by default, is empty and has no value. To display a default integer value in the field, type a numeric value that is between the minimum and maximum allowable values. **Minimum Value** The lowest allowable integer value that will be accepted for this field. **Maximum Value** The greatest allowable integer value that will be accepted for this field. If a user enters a value that is either below or above the specified value range or a non-integer value, an error message displays.
Long String	A long string is considered to be any text of length more than 4000 bytes. Long strings allow users to enter more than 4000 bytes in a single field. The long string has two sub types, medium and large. The size of the medium sub type is fixed to 32KB. The size of the large sub type set by default to 256KB. It can be increased by changing **OpenPages** ▸ **Platform** ▸ **Repository** ▸ **Resource** ▸ **Large Text** ▸ **Maximum Size** setting. Enter a value in bytes. The maximum size applies to all large sub-type long strings. **Important:** Once set, this value cannot be reduced. **Note:** The maximum size is a hidden setting. To show hidden settings set **OpenPages** ▸ **Applications** ▸ **Common** ▸ **Configuration** ▸ **Show Hidden Settings** to **true**. See "Working with Long String Fields" on page 142
Reporting Fragment	The fragment data type displays a component (such as a bar or line chart) from a CommandCenter report or dashboard in a field. For details, see "Configuring Reporting Fragment Fields" on page 133.
Simple String	The simple string data type, by default, displays data as text. The default value of the field is blank. The maximum size of a simple string is 4000 bytes. To display a default value in the field, type a string of either plain text or HTML-formatted text. To set the display of the string data to another type, such as a user drop-down, user or group selector, rich text area and so forth, you must do it through the profile. For details, see "Configuring Display Types for Simple String Fields" on page 221.
Single File	For internal use by workflow jobs. Do not use as this data type cannot be used in profiles.

Using Currency Data

This section describes how to work with currency data and how to modify existing data.

Accessing the Currencies Page

Procedure

1. Log on to the IBM OpenPages GRC Platform application interface (typically port 7009) as a user with the **Currencies** application permission set.
2. From the menu bar, select **Administration** and click **Currencies**. The Currencies page is displayed.

Modifying Currency Exchange Rates

Procedure

1. Access the Currencies page (see "Accessing the Currencies Page").
2. On the Currencies table, click **Edit**. The Edit Exchange Rates page is displayed.
3. Modify the desired exchange rates.
4. When finished, click **Save**.

Adding and Editing Currency Fields in a Field Group

This section describes how to add and modify one or more currency fields to an existing field group.

Adding a New Currency Field to a Field Group

Procedure

1. Access the Field Groups page (see "Accessing the Field Groups Page" on page 104).
2. In the **Field Groups** table, click the name of the field group to which you want to add a currency field. The page containing information for that field group appears.
3. In the **Field Definitions** table, click **Add**. The page containing the information to add field groups appears.
4. On the add page:
   a. In the **Name** box, type a name for the new currency field.
   b. In the **Description** box, optionally type a brief description of this field.
   c. Select Currency from the **Data Type** drop-down list.
   d. Check **Required** if the field is to be a required field.

      Note: The Currency data type does not support computed fields. See "Defining a Computed Field" on page 124 for information on computed fields.
   e. Check **Include Conversion** if the field is to include currency conversion.
   f. Click the >> button and type the minimum and maximum allowable currency values to be allowed in the field in the **Minimum Value** and **Maximum Value** boxes.
   g. Click **Create**. The system creates the new currency field.

Note:

- If a user enters a value that is either below or above the specified value range, an error message displays.

- You cannot use non-numeric characters when entering currency values. For example, either 125000 or 125,000 is legal, but not $125000.
- This format is set per User Locale.
- Object fields with this data type cannot be included in the profile of predefined objects or custom forms that use the supplied JSP file for rendering.

Editing Currency Field Information

Procedure

1. Access the Field Groups page (see "Accessing the Field Groups Page" on page 104).
2. In the **Field Groups** table, click the name of the field group that contains the currency field you want to edit, for example, OPSS-External Loss. The page containing information for that field group appears.
3. In the **Field Definitions** table, click the name of the currency field you want to edit, for example, Loss Amount. The page containing the information for this currency field appears.
4. Edit the information on this page.
5. When finished, click **Save**.

Viewing a Currency Display Type

You can view currency display type information for object types that contain a currency field.

Procedure

1. From the menu bar, select **Administration** and click **Profiles**. The Profiles page appears.
2. From the list on the **Profiles** table, click the name of the profile that contains both the object type and currency field you want to view.
3. From the list on the **Object Types** table, click the desired object type. For example, to view the currency display type for the **Inherent Severity** object field, select the **SOXRisk** object type.
4. From the list on the **Object Fields** table, locate and click the desired object field. The **Display Type** column of the selected field should be 'Currency'.

   On the detail page of the selected object field, the currency display information appears.

Editing a Currency Display Type

You can edit the currency display type for object types that contain a currency field.

Procedure

1. From the menu bar, select **Administration** and click **Profiles**. The Profiles page appears.
2. In the **Profiles** table, click the name of the profile that contains both the object type and currency field you want to view.
3. In the **Object Types** table, click the desired object type. For example, to view the currency display type for the **Inherent Severity** object field, select the **SOXRisk** object type.
4. In the **Object Fields** table, locate and click the desired object field. In the Object Field Information table, the Display Type field should be Currency.
5. Click **Edit**. The currency display information appears.

6. In the **Read Only** drop-down list, select either True or False.
7. Check the **Required** box if desired.
8. When finished, click **Save**.

Editing Currency Field Values in Individual Accounts

If you have OpenPages FCM (Financial Controls Management) installed, you can edit currency field values for individual accounts.

Procedure

1. Log on to the IBM OpenPages GRC Platform application.
2. From the menu bar, select **Financial** and click **Account**.
3. From the list, click the name of the account you want to open its details page.
4. Under Account Details, click the **Fields** link.
5. Select the Actions menu and choose **Edit this Account**.
6. In the **Annualized Value** field, change the Currency, Exchange Rate, or USD values as desired.
7. When finished, click **Save**.

Modifying Currency Exchange Rates

This section describes how to add, edit, and enable or disable currency exchange rates.

There are several methods for updating currency exchange rates. You can:

- Upload a CSV file with currency exchange rates from:
  - The IBM OpenPages GRC Platform application user interface. "Uploading a CSV File - User Interface Procedure" on page 119
  - An ObjectManager loader file. "Importing Exchange Rates" on page 523
- Manually edit the rates in the IBM OpenPages GRC Platform application user interface. "Editing Exchange Rates for an Existing Currency Code - User Interface Procedure"
- Upload currency exchange rates in an ObjectManager loader file. "Importing Exchange Rates" on page 523

Note: You cannot use these functions with a new currency. The currency must already exist.

Editing Exchange Rates for an Existing Currency Code - User Interface Procedure

Procedure

1. Access the Currencies page (see "Accessing the Currencies Page" on page 116).
2. On the Currencies page, click **Edit**.
3. On the Edit Exchange Rate page, edit the currency exchange rates as wanted.
4. When finished, click **Save**. The edited currency exchange rates appear on the Currencies page.

Uploading a CSV File With Currency Exchange Rates

Formatting a CSV File for Upload:

The file containing the exchange rate currency data must be in a comma separated value (.csv) file with the following format:

```
<currency code>,<exchange rate>
<currency code>,<exchange rate>
```

Where:

Field	Description
<currency code>	The 3-letter ISO Currency Code.
<exchange rate>	The numeric exchange rate value. The default value is '1.0'.
<start date>	Optional. The date the exchange rate was (or will be) applied. The format is: mm/dd/yyyy - or - mm/dd/yyyy HH:mm:sss If no historic date is supplied, the current date is used.

Example

The following data sample from a CSV file shows the ISO currency codes for Euros, Canadian dollars, Japanese yen, and Hong Kong dollars with the corresponding exchange rate for each currency, and the historical date the rate was applied for two of the four currencies.

```
EUR,0.1589,12/26/2007
CAD,0.8636
JPY,0.0083,5/8/2008
HKD,0.1289
```

Uploading a CSV File - User Interface Procedure:

Procedure

1. Access the Currencies page (see "Accessing the Currencies Page" on page 116).
2. On the Currencies page, click **Upload**.
3. Type the CSV file name into the **Exchange Rates File Name** box or select the appropriate file by clicking **Browse**.
4. When finished, click **Upload**. The new currency exchange rate appears in the Currencies table on the Currencies page.

Enabling Currency Exchange Rates - User Interface Procedure

You can enable disabled currency rates, making them available to the appropriate processes.

Procedure

1. Access the Currencies page (see "Accessing the Currencies Page" on page 116).
2. On the Currencies page, click **Enable**.
3. On the Enable Currencies page, check all the currencies you want to enable.
4. Optionally change the exchange rate for any listed currencies.
5. When finished, click **Save**. The enabled currencies appear on the Currencies table.

Disabling Currency Exchange Rates - User Interface Procedure

You can disable enabled currencies. When you disable a currency it is no longer available to the system. However, it is not deleted. You can enable it at any time.

Note: You cannot enable or disable the base currency, which is set during installation.

Procedure

1. Access the Currencies page (see "Accessing the Currencies Page" on page 116).
2. On the Currencies page, click the check box next to the currencies you want to disable. (You can re-enable these currencies at any time.)
3. Click **Disable**.

Modifying Field and Field Group Properties

Modifying Field Group Properties

You can modify the description property of any field group; however, the name of a field group cannot be changed.

Procedure

1. Access the Field Groups page (see "Accessing the Field Groups Page" on page 104).
2. Click the name of the field group that you want to modify to open its details page.
3. On the **Field Group Information** table, click **Edit**.
4. Modify the description as necessary.
5. When finished, click **Save**.

Modifying Object Field Definitions

After you create an object field, you can modify these field definition properties:

- For any type of object field - you can modify the description of the field, change whether or not the field is required or optional, and set a default value for the field (excluding the Date data type).
- For numeric fields - such as decimal or integer - you can change the minimum, maximum, and default values.
- For fields with enumerated strings, you can add, delete (if not in use), hide or unhide, and update the order of the values in the list. For details, see "Modifying Enumerated String Values" on page 130.

Note: You cannot modify the name of any object field or its data type.

Procedure

1. Access the Field Groups page (see "Accessing the Field Groups Page" on page 104).
2. Click the name of the field group containing the object field that you want to modify.
3. On the **Field Definitions** table, click the name of the field that you want to modify.
4. On the **Field Definition Information** table, click **Edit**.

5. To modify the field description, place the cursor in the **Description** box and type or edit the description.
6. To make object fields required or optional, go to the topic, “Making Fields Either Required or Optional.”
7. To set a default value for an object field, go to the topic, “Setting a Default Value for an Object Field.”
8. When finished, click **Save**.

Making Fields Either Required or Optional

By selecting or clearing the box for the **Required** option, you can globally set whether or not all users will be required to enter data in an object field. When you create a new object field, by default, the **Required** box is cleared (optional or non-required data entry).

Note: If you want to require a specific group of users (not all users) to enter data for a field, for maximum flexibility we recommend that you set the field as required in the profile and not in the field definition (see “Setting a Field in a Profile to Required or Optional” on page 182).

When you set an object field to be required, a red asterisk * displays after the field label in the **Add** and Edit pages of the object type. For example, if you were to change the setting of the optional "Additional Description:" field of the Account object to be a required data entry field, it displays to users as "Additional Description*:" Users are required to enter information in the field when they created a new Account object.

Procedure

1. Access the Field Groups page (see “Accessing the Field Groups Page” on page 104).
2. Click the name of the field group containing the object field that you want to modify.
3. On the **Field Definitions** table, click the name of the object field you want to modify.
4. On the **Field Definition Information** table, click **Edit**.
5. If you want this field to be:
   - A required data entry field - select the **Required** box.
   - A non-required (optional) data entry field - clear the **Required** box.
6. When finished, click **Save**.

   Note: Changing a field to Required also causes all profile references to the field to be required as well.

Setting a Default Value for an Object Field

With the exception of the Date data type, you can set a default value for any object field. When you create a new object field, by default, the **Default Value** property is empty (not populated).

Note: The Date data type always uses the current date as its default value. You cannot change this value.

When you set a default value for an object field, that value displays to users in that field. For example, if you were to set a default value for the "Additional

Description:" field of the Account object that contained the text "Enter any additional information here.", it displays to users when they created a new Account object.

Procedure

1. Access the Field Groups page (see “Accessing the Field Groups Page” on page 104).
2. Click the name of the field group containing the object field that you want to modify.
3. On the **Field Definitions** table, click the name of the object field you want to modify.
4. On the **Field Definition Information** table, click **Edit**.
5. In the **Default Value** box, either type a value or click the arrow and select an enumerated string value.
6. When finished, click **Save**.

Creating Computed Fields

You can create, edit, or view an object field whose value is computed from the values of other fields. These computed fields can exist on either the same object or on another, related object.

Computed fields have the following characteristics:

- Are always read-only
- Can be used in reports
- Can be added to Detail, List, and Folder view pages in the IBM OpenPages user interface

Note: Computed fields require an installed and active CommandCenter server as they use the CommandCenter Computation Handler. If a computed field is executed in the application and the CommandCenter server is not available, the following message is displayed to users, *CommandCenter is unavailable. Please contact your System Administrator*.

Process Overview

The following steps outline the process for setting up a new computed field.

Procedure

1. In CommandCenter Report Studio, model the computed field in a calculation object. For details, see “Modeling a New Computed Field in CommandCenter.”
2. In the IBM OpenPages GRC Platform application user interface:
   a. Define the computed field. For details, see “Defining a Computed Field” on page 124.
   b. Regenerate the reporting framework. For details, see “Updating the Reporting Framework” on page 64.

Modeling a New Computed Field in CommandCenter

This section assumes that you have experience using the CommandCenter Report Studio tool. It explains the steps required to model an equation in CommandCenter that can be used to define a computed field in the application.

Note: If you do not have knowledge of how to use the CommandCenter Report Studio tool, either seek the help of an experienced CommandCenter report author or call your IBM representative for assistance.

Procedure

1. Log on to the CommandCenter portal as an IBM OpenPages user with the locale set to 'Report Design Language'.
2. Create a new list report that you can use to model the computed field equation.
3. Drag the following ID query items onto the report page to establish a context for the calculation:
   - An object ID

     Example

     ```
     SOXBUSENTITY HIERARCHY >> SOXPROCESS–SOXCONTROLOBJECTIVE HIERARCHY
      >> [SOXRISK] >> [RI_RISK_ID]
     ```
   - A reporting period ID

     Example

     ```
     SOXBUSENTITY HIERARCHY >> SOXPROCESS–SOXCONTROLOBJECTIVE HIERARCHY
      >> [SOXRISK] >> [REPORTING_PERIOD_ID]
     ```
4. Click the **Toolbox** tab on the Insertable Objects pane:
   a. Drag a **Calculation** object onto the report page.
   b. At the prompt, type a name. For example, *Calc-Risk*.
   c. Click **OK**.
5. In the Expression Definition pane of the model:
   a. Enter an expression using model query items from the same namespace, function, or parameters.

      The CommandCenter SQL used to define this computed value can be an existing query item in the published CommandCenter framework or an equation involving multiple query items. Some of the predefined database functions may also be useful for computed fields (such as getting an exchange rate or localizing strings).

      Example

      The following equation returns a value representing the percentage by which the inherent severity of a risk was reduced after associated controls were applied to that risk. Sample output might be: `2.46`.

      ```
      total ([DEFAULT].[SOXCONTROL].[CN_INHERENT_SEVERITY_REDU]
      for [DEFAULT].[SOXCONTROL].[RISK_ID]) / 100
      ```
   b. Validate the expression, make any needed changes, and then click **OK**.
6. Run the report to make sure that you are receiving the intended results.
7. Click the **XML Show Specification** button on the toolbar to view the CommandCenter SQL (in an XML representation). Figure 7 on page 124 shows which sections of the report will be used to define the computed field in the IBM OpenPages GRC Platform application and the corresponding field name in the application.

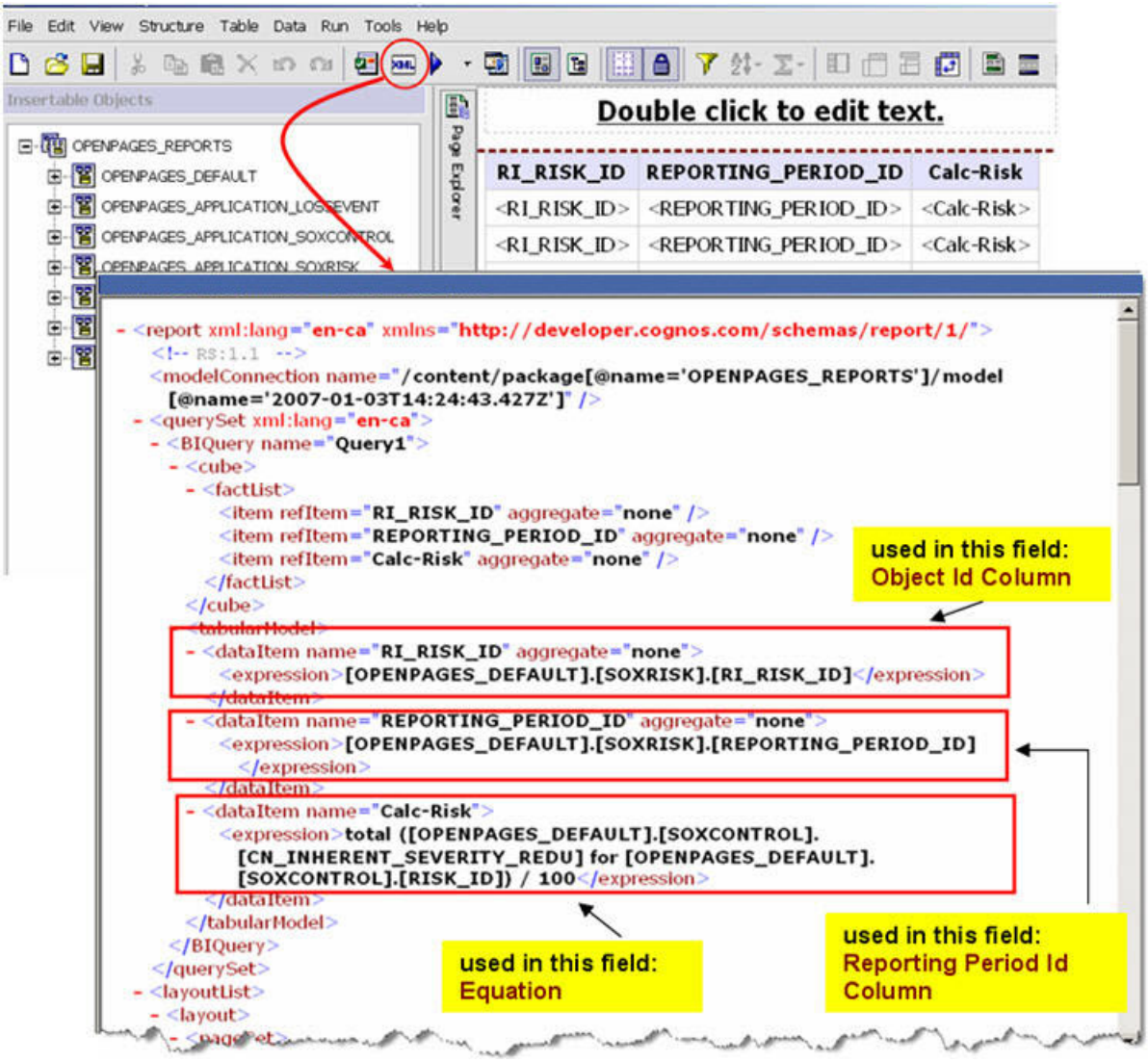


Figure 7. Sample XML Report Specification Showing Sections

Note: Because the values in the Report Specification XML window are not selectable, you can copy the report specification to the Clipboard (**Tools** | **Copy Report to Clipboard**) and then paste the information into a text document where you can then copy the attribute values into the application user interface. The value to be used in the application's **Equation** definition box can also be obtained from the Expression Definition pane of the calculation object.

8. In the IBM OpenPages GRC Platform application user interface, define the computed field. For details, see "Defining a Computed Field."

Defining a Computed Field

Note: The following data types do not support computed fields: Currency, Enumerated String, and Single File.

To define a computed field, follow these steps.

Procedure

1. Access the Field Groups page (see "Accessing the Field Groups Page" on page 104).
2. Click the name of the field group in which you want to include the new object field.
3. On the **Field Definitions** table, click **Add**.
4. In the **Name** box, type a name for the new computed field.
5. In the **Description** box, optionally type some descriptive text.
6. Click the **Data Type** arrow and use Table 21 to select a data type for the new computed field.

Table 21. Data Types for Computed Fields

Data Type	Return Value	When to Use
Boolean	TRUE or FALSE (case insensitive)	Takes a boolean string, parses it, localizes it, and displays it.
Date	Date in the format: yyyy-MM-dd'T'hh:mm:ss	Takes a date string, parses it, localizes it, and displays it.
Decimal	Any numbers	Takes any number string and parses it, localizes it, and displays it.
Integer	Whole numbers	Takes a whole number string and parses it, localizes it, and displays it.
Simple String	Any	Can be used for any computed field. Takes the result of the computation engine and displays it. This will not be localized - it displays the exact output of the computation.

   If the field is any other data type, use the 'Simple String' data type.

7. Click the double arrow  button next to the selected data type to display additional parameters.
8. Select the **Computed** option to make the new field a computed field.

   When you select **Computed**, the **Required** option disappears and the CommandCenter Computation Handler attribute fields appear.

   Note: Note for Steps 9, 12, and 13:

   If you modeled the computed field in CommandCenter Report Studio, the values displayed in the Report Specification XML window are not selectable (see Figure 7 on page 124). You can copy the report specification to the Clipboard (**Tools | Copy Report to Clipboard**) and then paste the information into a text document where you can then copy the attribute values into the application user interface. The value to be used in the application's **Equation** definition box can also be obtained from the Expression Definition pane of the calculation object.
9. Enter a value in the **Equation** box. The equation is the CommandCenter SQL used to define the computed value for the object field. It can be a reference to an existing query item in the published CommandCenter framework or an equation involving multiple query items.

   Example:

```
total ([DEFAULT].[SOXCONTROL].[CN_INHERENT_SEVERITY_REDU] for
[DEFAULT].[SOXCONTROL].[RISK_ID]) / 100
```

10. Enter a value in the **Primary Namespace** box. The Primary Namespace is the CommandCenter framework namespace in which the computation is to be performed.

    Note: All referenced query items in the values for 'Equation', 'Object ID Column', and 'Reporting Period ID Column' must be in the same namespace.

    Example: DEFAULT
11. Enter a value in the **Alternate Namespaces** box if necessary.

    The Alternate Namespace is the CommandCenter framework namespaces to which the computation will be added during reporting framework generation.

    Note: See "Using Computed Fields with Multiple Namespaces" for an explanation of why a computed field might need alternate namespaces.
12. Enter a value in the **Object Id Column** box. The Object ID Column is a reference to a CommandCenter framework query item that contains the Resource ID of the computed field's object type. This value must be the same for all computed fields in a given namespace for an object type.

    `Example: [DEFAULT].[SOXRISK].[RI_RISK_ID]`
13. Enter a value in the **Reporting Period Id Column** box. The Reporting Period ID Column is the CommandCenter framework query item that contains the Reporting Period Id of the computed field's object type. This value must be the same for all computed fields in a given namespace for an object type.

    Important: The Resource ID and Reporting Period ID must match within the field group and object type. If these values do not match, the validation will fail.

    Example: [DEFAULT].[SOXRISK].[REPORTING_PERIOD_ID]
14. Click **Create**. IBM OpenPages will then validate the equation against the primary and alternate namespaces.
15. Regenerate the reporting framework to make the computed field available to report authors. For details, see "Updating the Reporting Framework" on page 64.

Importing and Exporting Computed Field Definitions

If you want to import (load) and export (dump) computed field definitions, you must use the ObjectManager tool. For details, see "Importing and Exporting Computed Field Definitions" on page 526.

Using Computed Fields with Multiple Namespaces

The IBM OpenPages GRC Platform application allows multiple parent object types for a given child object type. The CommandCenter reporting engine cannot support objects with multiple parent's object types.

For example, in the `DEFAULT` namespace the only path to a Loss Event is through a Business Entity. This means that if a Loss Event is associated to a parent Risk but not a parent Business Entity, that Loss Event will not be displayed as a result in queries against that namespace. Each parent-child object type relationship that is not contained in `DEFAULT` is contained in its own namespace.

In order to make the calculation available in multiple namespaces for report writers, you can use the 'Additional Namespaces' attribute. This is a

comma-delimited list of alternate namespaces for which a 'Calculation' object should be created during the framework generation process. During this process, a calculation object is first created for the primary namespace using the value from the 'Equation' attribute. Then it creates other calculation objects in other namespaces by taking the equation and substituting the alternate namespaces for the primary namespace.

Note: While an equation may be valid in one namespace, it may not be valid in others. While in most cases this is not a problem, if the query subject name or query item name varies across namespaces you may need to create separate computed field instances with different equations.

Nesting Computed Fields

Computed fields can sometimes act as building blocks for other computed fields. These are referred to as intermediate computations. Currently the IBM OpenPages GRC Platform application does not support intermediate calculation definitions through the IBM OpenPages GRC Platform user interface. If you want to reference another computed field, you must replicate the equation used in that computed field inside the equation for the current field.

For example, if we have a computed field "A" and define it as "A = B x C" and we also know
"C = D + E", we would only create one computed field "A" in the application where the equation would be "B x (D + E)".

While this approach can be verbose, it is sometimes the simplest.

Troubleshooting Computed Fields

Validation

Computed fields validation is complex since they are only valid in relation to the IBM OpenPages GRC Platform reporting framework, which may change in response to a change in the IBM OpenPages object model. Therefore, we provide several forms of validation.

When creating or editing a computed field, it is validated against the primary namespace as well as all alternate namespaces. If any of the validation checks fail, then the IBM OpenPages GRC Platform application will not allow you to save the computed field until corrected. The IBM OpenPages GRC Platform application maintains strict validation checks in this area because a slight error here can have an extensive ripple effect that is hard to identify and correct.

Also, due to the complexity of the computation engine there are certain cases where two computed fields will be valid by themselves but invalid together. A common example is where two computed fields reference different Object ID columns. In order for the computations to be grouped correctly they must all have the same Object ID column value. Therefore, we provide validation functionality across both an entire Field Group definition as well as an Object Type definition.

Equation Length Limitation

Currently there is a limitation on the size of the computation attribute value that can be stored by the application. The main attribute of concern is 'Equation' where a complex equation could be very lengthy. There is a 20,000 byte limit on the size

of the entered text. Note that OpenPages supports multi-byte characters and so this may not be the equivalent of 20,000 characters if you are using a multibyte language.

Using Computed Fields with Cross Products

A cross product normally occurs when a table of data is joined with itself resulting in redundant data. In the case of computed fields as they relate to Cognos we encounter a slightly more complex version.

For example, in the out-of-the-box ORM schema we have computed fields on the Loss Event object type that aggregate associated Loss Impacts and Loss Recoveries. In effect we are joining the Loss Event data with itself because we have two associations (joins) from the same object type and this causes a cross product.

Say you have the following associations between Loss Event and Loss Impact:

- LE - LI1
- LE - LI2
- LE - LI3

And the following associations between Loss Event and Loss Recovery:

- LE - LR1
- LE - LR2

When a query is written to access all three object types the following data is returned:

- LE, LI1, LR1
- LE, LI2, LR1
- LE, LI3, LR1
- LE, LI1, LR2
- LE, LI2, LR2
- LE, LI3, LR2

In the case where we are aggregating values on the Loss Impact we end up with twice the desired value and on the Loss Recovery three times the value. One way to work around this is as follows:

Instead of:

```
total (Loss Impacts for Loss Events)
```

Use:

```
average (Loss Impacts for Loss Events) * count (distinct Loss Impacts for
Loss Events)
```

Mathematically, we can say that *average x distinct_count = total/count x distinct_count = total x distinct_count/count*.

So if we are trying to total the Loss Impacts for a Loss Event in the previous example we would be performing a total on the cross product result and then multiplying by 1/2 to factor out the cross product. If we are trying to total the Loss Recoveries for a Loss Event in the previous example we would be performing a total on the cross product result and then multiplying by 1/3 to factor out the cross product.

Optimizing CommandCenter Report Request Performance

With the addition of computed fields there is a large increase in the number of CommandCenter report requests and so it is important to make sure CommandCenter is set up correctly. One common pitfall is the number of processes configured for the 'ReportService'. This can be configured as follows.

Procedure

1. From a browser window, log on to the IBM Cognos 8 portal as a user with administrative privileges.

   By default, the URL is:

   `http://<hostname>/cognos8` (if you are using port 80 for CommandCenter)

   Where: `<hostname>` is the name of the Web server machine that contains the cognos8 virtual directory.
2. On the main page under the **Administration** heading, click the **Administrator IBM Cognos content** link.
3. On the **Status** tab, click the **System** link in the left pane.
4. In the Scorecard pane, do the following:
   a. Under **All servers**, click the name of the reporting server you want to tune.
   b. Under the reporting server, click the name of the dispatcher. For example, `http://<server_name>:9300/p2pd`

      Note: The dispatcher has the following icon  preceding its URI.
   c. In the list of services for the dispatcher, click **ReportService**.
5. In the Metrics - ReportService pane, do the following:

   Note: For information on performance metrics and additional settings that are not listed here, see the IBM Cognos 8 online Help.
   a. Expand **Process**.
   b. View and, if wanted, edit the settings for the **Number of processes high watermark** and **Number of processes low watermark** performance metrics. These metrics monitor the maximum and minimum number of active user sessions since the last reset.
   c. Expand **Queue**.
   d. View and, if wanted, edit the setting for the **Latency** performance metric. This metric specifies the average amount of wait time requests spend in the queue.
   e. Expand **Request**.
   f. View and, if wanted, edit the settings for the **Seconds per successful request** and **Successful requests per minute** performance metrics. These metrics specify the average number of seconds it takes to process a successful request and the average number of successful requests that can be processed in a minute.
6. In the Settings - ReportService pane, do the following:

   Note: For information on performance tuning and additional settings that are not listed here, see the IBM Cognos 8 online Help.
   a. Expand **Tuning**.
   b. Change the value of the **Maximum number of processes for the report service during peak period** and **Maximum number of processes for the report service during non-peak period** settings. These settings specify the

maximum number of child report service processes that can be started during peak demand and "off-peak" hours.

As a starting point, you should configure the value of these settings to be twice the number of CPUs on the CommandCenter server. For example, if your environment is always at peak and CommandCenter is running on a quad-CPU box, then you would set the maximum number of processes to 8 for each setting.

If slow computed fields performance is observed, you can visit the administration page again to observe the number of available processes as well as the latency. Note that these values are only meaningful on a system under load. If all the processes are consistently busy and there is a large latency to service a request, consider changing the number of processes.

Query Direction Performance

When exploring all the computation possibilities there is one large distinction in what can/should be done. While in CommandCenter it is possible to query up the relationship tree (i.e. compute values based on ancestors) it is strongly discouraged. The automatic framework generation is set up in such a way as to create joins that are conducive to better performance querying down the relationship tree. A query up the tree will result in bad computed field performance as well as place a large strain on the Database that can result in the entire application slowing down.

Modifying Enumerated String Values

For object fields with enumerated strings, you can add new values, delete (if not in use), hide or unhide, and update the order of the values in the list. The modifications you make to values in a list are globally applied to all instances wherever that field group is in use.

Adding New Enumerated String Values

You can add new values to an existing list of enumerated string values at any time.

For example, let's say you created an object field called "Rating" that was an Enumerated String data type. When the field was initially created, it was given the following values: High, Medium, and Low. Because of changing business needs, you want to add a new value of "Unknown" to the list. You could add this new value at any time and have it immediately displayed to users as a selection in the list of values.

When you add a new string value to an existing list of values:

- The value is immediately displayed to users for selection in the list of values
- The new value is added to the end of the value list

Procedure

1. Access the Field Groups page (see "Accessing the Field Groups Page" on page 104).
2. On the **Field Groups** table, click the name of the field group in the list that contains the field you want to modify.
3. On the **Field Definitions** table of the selected field group details page, click the name of the field that contains the enumerated string that you want to modify.
4. On the **Enumerated String Values** table of the field definition details page:

a. Click **Add**.
b. In the **Name** box, type a value for the new string.
c. Click **Create**.

5. To change the order number of the string values, see "Changing the Order of Enumerated String Values."

Changing the Order of Enumerated String Values

For object fields with an Enumerated String data type, you can modify the order in which string values are displayed to users. When you change the order number of a string value, all the string values following the changed order number are dynamically updated by the system.

For example, let's say that the display order of string values in a list is: High 1, Medium 2, Low 3, Unknown 4. If you want Unknown to be displayed first in the list, you would change the order number of Unknown from 4 to 1. The system will automatically re-order the other string values. The new order of the string values in the list displays as: Unknown 1, High 2, Medium 3, Low 4.

Procedure

1. From the menu bar, select **Administration** and click **Field Groups**.
2. On the **Field Groups** table, click the name of the field group in the list that contains the field you want to modify.
3. On the **Field Definitions** table of the selected field group details page, click the name of the field that contains the enumerated string that you want to modify.
4. On the **Enumerated String Values** table of the field definition details page:
   a. Find the rows containing the string value whose list order you want to change.
   b. In the **Order** boxes, type a new order number for the values.
   c. Click **Update Order**.

Hiding Enumerated String Values

You can hide obsolete or unwanted string values from a list of enumerated string values.

When you hide a string value from a list:

- For new instances of an object, the value or values are immediately hidden from selection by users on the list of values.
- For existing instances of an object, if the value or values were previously selected by users (that is, before the value was hidden), the value or values are still displayed in the list and are available during editing for selection by users.
- The "Hidden" column on the **Enumerated String Values** table changes from "false" to "true".

Procedure

1. Access the Field Groups page (see "Accessing the Field Groups Page" on page 104).
2. On the **Field Groups** table, click the name of the field group in the list that contains the field you want to modify.
3. On the **Field Definitions** table of the selected field group details page, click the name of the field that contains the enumerated string that you want to modify.
4. On the **Enumerated String Values** table of the field definition details page:

a. Select the box next to the value or values you want to hide from the list. The "Hidden" column for the value will be set to "false".
b. Click **Hide/Unhide**. The "Hidden" column for the value changes to "true".

Note: The **Hide/Unhide** button toggles between **Hide** and **Unhide** depending on the current setting.

Unhiding Enumerated String Values

If an enumerated string value was previously hidden from visibility by users, you can "unhide" the hidden value and make it again visible to users in the list.

When you unhide a string value from a list, the following occurs:

- The value is immediately displayed for selection by users on the list of values.
- The "Hidden" column on the **Enumerated String Values** table changes from "true" to "false".

Procedure

1. Access the Field Groups page (see "Accessing the Field Groups Page" on page 104).
2. On the **Field Groups** table, click the name of the field group in the list that contains the field you want to modify.
3. On the **Field Definitions** table of the selected field group details page, click the name of the field that contains the enumerated string that you want to modify.
4. On the **Enumerated String Values** table of the field definition details page:
   a. Select the box next to the hidden value or values you want to display from the list. The "Hidden" column for the value will be set to "true".
   b. Click **Hide/Unhide**. The "Hidden" column for the value changes to "false".

   Note: The **Hide/Unhide** button toggles between **Hide** and **Unhide** depending on the current setting.

Deleting Enumerated String Values

You can only delete an enumerated string value from a field definition if the field group containing the field is not in use. A deleted string value is permanently removed from the list and cannot be retrieved. If the field group is in use, **Delete** remains disabled and you can only hide any obsolete or unwanted string values from view. For details see, "Hiding Enumerated String Values" on page 131.

Procedure

1. Access the Field Groups page (see "Accessing the Field Groups Page" on page 104).
2. On the **Field Groups** table, click the name of the field group in the list that contains the field you want to modify.
3. On the **Field Definitions** table of the selected field group details page, click the name of the field that contains the enumerated string that you want to modify.
4. On the **Enumerated String Values** table of the field definition details page:
   a. Select the box next to the name of the value you want to remove - **Delete** becomes enabled.

   Note: If **Delete** remains disabled, the field group to which this field definition belongs is in use and you cannot delete the value.

b. Click **Delete**.
c. At the prompt, click **OK** to remove the value from the list.

Configuring Reporting Fragment Fields

About Reporting Fragment Fields

Reporting fragment fields are always read-only fields that typically display a component (such as a chart or table) from a larger CommandCenter report.

Once fragment fields are configured, these fields — like other fields in the IBM OpenPages GRC Platform application — can be:

- Associated with an object type
- Added to various object view pages
- Configured as dependent fields
- Have their display type modified

By default, fragment fields have a display type of 'Automatic' for Detail and Activity View pages and the report component is embedded directly on the page. If the display type is changed to 'On Demand', the report component is displayed in a pop-up window. Pop-up windows can be autosized through settings in the application or manually overriden when the fragment field is defined.

Limitations

Reporting fragment fields have the following limitations:

- You cannot use elements from JSP reports in reporting fragment fields; only components from CommandCenter reports are supported.
- Page breaks in reporting fragment fields are not supported.
- Tooltips in reporting fragment fields are not supported.
- A report that has required prompts other than Object ID and Reporting Period ID cannot be used as a reporting fragment field.

Note: See the *IBM OpenPages CommandCenter Report Author's Guide* on your documentation media for designing reports that can be used in fragment fields.

Planning Considerations for Reporting Fragment Fields

Before you add a fragment field, you need to identify the report with the component you want, and which object types, profiles, and object views will be associated with the fragment field. Planning your changes ahead of time helps to minimize the necessary work and prevents duplication of effort.

The following list will help you identify some of the questions you need to consider before you create a new fragment field:

- Report component — What report component data does the user need to see to accomplish their task? Which CommandCenter report contains the component?
- Field group — Will new fragment fields reside in new or existing field groups?
- Object type — Which object type will use the fragment field or fields?
- Views — Which view pages in a profile will use the fragment fields (such as Filtered List View, Detail View, Activity View, Classic tab)?

- Display — How many fragment fields will be included in a Detail or Activity View page? Will a fragment field be embedded (Automatic) on the page or displayed as a pop-up window (On Demand)?

Process Overview

Table 22 provides an overview of the configuration tasks for setting up new fragment fields and a reference to the related information.

Table 22. Tasks for Configuring Reporting Fragment Fields

✓	Task Description	Related Topic
☐	Identify the: • CommandCenter report and report component you want to use. • The field group you want to use.	"Planning Considerations for Reporting Fragment Fields" on page 133
☐	From CommandCenter, obtain the parameter information for the fragment field.	"Fields Requiring Parameter Information"
☐	In the IBM OpenPages GRC Platform application, define the fragment field.	"Defining a Reporting Fragment Field" on page 135
☐	Add the field group to an object type if it is not already included.	"Including Field Groups for an Object Type" on page 146
☐	Select a profile and add the fragment field to an object type in that profile.	"Configuring Fields for Object Types" on page 180
☐	Select an object view in that profile and add the fragment field to that view page.	"About Object Type Views" on page 194
☐	Optionally, change the display type and display characteristics.	"Configuring the Display Type for Reporting Fragment Fields" on page 220

Fields Requiring Parameter Information

Note: You must have administrative privileges set on your account so you can access:

- The CommandCenter portal and Report Studio for obtaining parameter information
- The IBM OpenPages GRC Platform application for defining the new fragment field

The process of creating a new fragment field for use in the IBM OpenPages GRC Platform application involves copying parameter information from CommandCenter and either pasting or entering it into fields on the Reporting Fragment data type field definition page in the IBM OpenPages GRC Platform application.

Table 23 on page 135 lists the various fields on the Reporting Fragment data type field definition page that require specific information from CommandCenter.

Table 23. Required Parameter Information

Fields in the IBM OpenPages application that require CommandCenter parameter information	Field description	Where to find the parameter information in CommandCenter
Report Path	Required. The file path of the selected CommandCenter report that contains the component you want to use. "Define the Report Path" on page 136	IBM Cognos Connection, Public Folders tab.
Fragment Name	Required. The unique name of the particular report component (such as a 'Pie Chart', 'List', 'Combination Chart', and so forth). "Define the Fragment Name" on page 137	Report Studio, Report Page
Object ID Prompt	Required only if the report prompts users to select a resource (such as 'Entity', 'Process', and so forth) before running the report. Otherwise, leave this field blank. "Define the Object ID Prompt" on page 138	Report Studio, Prompt Page
Reporting Period ID Prompt	Required only if the report prompts users to select a reporting period before running the report. Otherwise, leave this field blank. "Define the Reporting Period ID Prompt" on page 139	Report Studio, Prompt Page

Defining a Reporting Fragment Field

For purposes of illustration, the following tasks use examples from a sample Assessment Status report to configure a fragment field that will display the chart component of this report as an embedded report on a Risk Assessment Detail View page.

Find or Add a Field Group for the New Reporting Fragment Field

Note: This task is required.

You can use either an existing field group or create a new field group for the new fragment field.

In IBM OpenPages :

Procedure

1. Access the Field Groups page (see "Accessing the Field Groups Page" on page 104).
2. Do one of the following:
   - To include the fragment field in an existing field group, click the name of the field group to open its detail page.

- To include the fragment field in a new field group, see "Adding New Field Groups" on page 110.

3. On the detail page of the selected field group, navigate to the **Field Definitions** table and click **Add**.
4. On the field definitions detail page:
   a. In the **Name** box, type the name of the new object field.
   b. In the **Description** box, optionally type some brief descriptive text.
   c. Click the **Data Type** arrow and select **Reporting Fragment** from the list.
   d. Click the double arrow  button next to the data type selector to display additional parameters this data type.

   Note: Keep the IBM OpenPages GRC Platform application browser window open as you will need to return to it.

Define the Report Path

Note: This task is required.

The steps in this task require going back and forth between the CommandCenter portal and the IBM OpenPages GRC Platform application user interface to obtain the path information to the report containing the component.

In the CommandCenter Portal:

Procedure

1. Open another browser window and log on to IBM Cognos Connection as a user with administrative privileges.

   By default, the URL is `http://<servername>/cognos8`

   Where: `<servername>` is the name of the CommandCenter reporting server.
2. On the Public Folders tab, navigate through the folder hierarchy to where the report you want is saved.

   Example

   ```
   Public Folders > OPENPAGES_REPORTS_V6 > Risk Assessment Reports >
   Risk Assessment Status
   ```
3. Under the Actions column for the report you want, click the  icon. Hover text for the icon will display 'Set properties - <report name>'.

   Example

   The hover text for the Risk Assessment Status report Set properties icon would say:

   'Set properties - Risk Assessment Status'
4. On the Set Properties page of the selected report:
   a. Select the **General** tab if it is not already selected.
   b. Click the 'View the search path, ID and URL' link (found in the upper right section of the page).
5. In the View the search path, ID and URL window, copy the text in the 'Search path' box.

   The following example shows sample search path text for the Risk Assessment Status report.

Sample Search Path Text

```
/content/folder[@name='OPENPAGES_PLATFORM']/folder[@name='Risk
Assessment Reports']/report[@name='Risk Assessment Status']
```

In IBM OpenPages :

Procedure

On the Reporting Fragment field definitions detail page, paste the search path text into the **Report Path** box.

In the CommandCenter Portal:

Procedure

Close the View the search path, ID and URL window and exit the 'Set properties' page (do not exit CommandCenter).

Define the Fragment Name

Note: This task is required.

The steps in this task require going back and forth between the CommandCenter portal and the IBM OpenPages GRC Platform application user interface to obtain the name of the report component within the selected report.

In CommandCenter Report Studio:

Procedure

1. Open the report containing the component you want in Report Studio:
   a. On the Public Folders tab, navigate through the folder hierarchy to where the report you want is saved.

      Example

      ```
      Public Folders > OPENPAGES_PLATFORM > Risk Assessment Reports >
      Risk Assessment Status
      ```

   b. Under the Actions column for the report you want, click the  icon.Hover text for the icon will display 'Open with Report Studio - <report name>'.

      Example

      The hover text for the Risk Assessment Status report Set properties icon would say:

      'Open with Report Studio - Risk Assessment Status
2. In Report Studio (in Page Design mode), select the component you want to use for the Reporting Fragment field (such as a List, a Chart, a Crosstab, and so forth.)
3. Verify that the entire component is selected:
   a. In the Properties pane (on the left), look at the title bar. It should display the name of the selected component, such as 'Pie Chart', 'List', 'Combination Chart', and so forth.

b. If the Properties title bar displays the name of a subcomponent (for example 'List Column Body' or 'List Column Title'), then click the Properties up arrow icon on the Properties title bar and select the entire component (for example, 'List').

4. Once the entire component is selected, do the following:
   a. In the Properties pane, scroll to the **Miscellaneous** heading.
   b. Under the **Miscellaneous** heading, copy the value in the **Name** property.

      Example

      The Name property value for the Combination Chart component of the sample Risk Assessment Status report is `Combination Chart1`.

In IBM OpenPages :

Procedure

On the Reporting Fragment field definitions detail page, paste or type the value into the **Fragment Name** box.
Example
For the sample Risk Assessment Status report, you would paste or type `Combination Chart1`.

Note: If the report prompts for an object or reporting period ID, keep the report open in Report Studio.

Define the Object ID Prompt

Note: This task is required **only** if a report prompts users to select a resource (such as 'Entity', 'Process', and so forth) before running the report. Otherwise, skip this task and leave the field blank.

In CommandCenter Report Studio:

Procedure

1. In Report Studio for the selected report:
   a. Click the Page Explorer.
   b. Navigate to the prompt page of your report.
2. On the prompt page:
   a. Click the prompt for the object identifier (such as Entity, Process, and so forth).
   b. In the Properties pane (on the left), scroll to the **General** heading.
   c. Under the **General** heading, click the **Parameter** property icon and copy the value in the box (for example, `Entity`).

      Example

      The sample Risk Assessment Status report prompts users to select a Business Entity before running the report. On the sample Risk Assessment Status report 'PromptPage,' you would select the 'Value Prompt' object for Business Entity. The value in the 'Properties - Value Prompt' for the 'Parameter' field is `Entity`.

In IBM OpenPages :

Procedure

On the Reporting Fragment field definitions detail page, paste or type the value into the **Object ID Prompt** box.

Example

For the sample Risk Assessment Status report, you would paste or type `Entity` in the 'Object ID Prompt' box.

Define the Reporting Period ID Prompt

Note: This task is required **only** if a report prompts users to select a reporting period before running the report. Otherwise, skip this task and leave the field blank.

In CommandCenter Report Studio:

Procedure

1. In Report Studio for the selected report:
   a. Click the Page Explorer.
   b. Navigate to the prompt page of your report.
2. On the prompt page:
   a. Click the prompt for the reporting period identifier.
   b. In the Properties pane (on the left), scroll to the **General** heading.
   c. Under the **General** heading, click the **Parameter** property icon and copy the value in the box.

In IBM OpenPages :

Procedure

On the Reporting Fragment field definitions detail page, paste or type the value into the **Reporting Period ID Prompt** box.

Define the Reporting Fragment Size

Note: This task is optional. Use if you want to manually control the height and width of the pop-up window for a fragment field.

If you leave the pixel values for height and width blank (this is the default), the pop-up window will be sized automatically.

In IBM OpenPages :

Procedure

1. On the Reporting Fragment field definitions detail page:
   a. In the **Height** box, type a numeric value for the pixel height of the fragment.
   b. In the **Width** box, type a numeric value for the pixel width of the fragment.
2. When finished, click **Create**.

Configuring Save As Draft Fields

Configure the Save As Draft feature to display a **Save As Draft** button when editing or creating objects so users can save object data without filling in all of an object's required fields.

The **Save As Draft** button is displayed next to the **Save** button on the **Detail View** page of an object type when the object is in edit mode.

The Save As Draft configuration process requires the creation of a field group and an enumerated string field. Once the group and field are created, these values can be used in settings to enable the **Save As Draft** button. The group and field can then be associated to various object types in a profile. The field does not have to be associated with a particular view in a profile for the **Save As Draft** button to be displayed.

See the following topics for details on the Save As Draft configuration process:

- "Create a new field group and field"
- "Configure settings" on page 141
- "Add the field to the object type and profile" on page 141

For purposes of illustration, the field group in the "Create a new field group and field" procedure is called "DraftGroup" and the enumerated field is called "Draft Status" with values of "Draft" and "Published".

When the user clicks the **Save As Draft** button, the value of the "Draft Status" field is automatically set by the system to "Draft". When the user clicks the **Save** button, the required fields are automatically validated and the value of the "Draft Status" field is set to "Published". We recommend that the "Draft Status" field is hidden from object views in a profile. However, if you choose to make the "Draft Status" field visible in a profile's object view, it should be configured as Read only.

Using the Save As Draft Feature with Activity View Pages

If you plan to use the Save As Draft feature with **Activity View** pages, the **Save As Draft** button must be configured on the root or parent object type (this is the first object type listed in the Activity View).

If a child object type has the **Save As Draft** button configured but the parent object type does not have the button configured, the **Save As Draft** button will not be visible on the **Activity View** page.

The required field validation is skipped on child objects if they have the draft field in the profile. The required field validation on the child objects will NOT be skipped if the child object does not have the draft field in the profile, even though the user clicked the **Save as Draft** button.

Create a new field group and field

Procedure

1. Create a new field group and name it, for example, `DraftGroup` (see "Adding New Field Groups" on page 110).
2. Add a field definition to the new field group and name it, for example, `Draft Status`.

a. Select the **Enumerated String** data type.
b. Add a value for `Draft` and a value for `Published` (see "Adding Field Definitions to a Field Group" on page 110).

Configure settings

Procedure

1. Access the **Settings** page (see "Accessing the Settings Page" on page 268).
2. Set the value in the **Show Hidden Settings** setting to true (for details, see "Showing Hidden Settings" on page 273).
3. Expand the **OpenPages | Applications | Common | Configuration | Required Field Validation** folder hierarchy
4. Click the **Draft Status Field** setting to open its detail page.
   a. In the **Value** box, type the name of the field group and field. The format is `<field group>.<field name>`.

      For example: `DraftGroup.Draft Status`
   b. Click **Save**.
5. Click the **Draft Status Value** setting to open its detail page.
   a. In the **Value** box, type the system name of the draft value.

      For example: `Draft`
   b. Click **Save**.
6. Click the **Publish Status Value** setting to open its detail page.
   a. In the **Value** box, type the system name of the draft value.

      For example: `Publish`
   b. Click **Save**.

Add the field to the object type and profile

Procedure

1. Enable System Admin Mode (see "Enabling and Disabling System Admin Mode" on page 58).
2. For each object type that you want to have a **Save As Draft** button, include the new field group, for example `DraftGroup` (see "Including Field Groups for an Object Type" on page 146).
3. Disable System Admin Mode.
4. Include the new field, for example `Draft Status`, in a profile (see "Including Fields in an Object Type" on page 181).

   Note: Unless you want the field to be visible to users, the field does not have to be included on a **View** page for the **Save As Draft** button to be displayed.

Deleting Field Groups and Definitions

Deleting Field Groups

If a field group has never been associated with an object type (that is, it has never been used), you can then delete it.

When you delete a field group, the field group is removed from the list of available field groups on the Field Groups page and cannot be restored to the list.

Procedure

1. Access the Field Groups page (see "Accessing the Field Groups Page" on page 104).
2. Select the box next to the name of the field group that you want to delete.
3. Click **Delete** on the **Field Groups** table.

Deleting an Object Field Definition

When you delete a field, the definition of the field is removed from the field group to which it belongs. You can only delete field definitions from a field group that are not in use. Once a field definition is deleted, it cannot be restored.

Procedure

1. Access the Field Groups page (see "Accessing the Field Groups Page" on page 104).
2. Click the name of the field group you want to modify to open its details page.
3. Click the box next to the name of each field definition you want to delete.
4. When finished, click **Delete**.

Working with Long String Fields

Long string fields (data type is long string) are considered to be any text of length more than 4000 bytes. Long string fields allow users to enter more than 4000 bytes in a single field.

There are two sub types of long text fields: medium and large. The size of medium long string fields is fixed to 32KB. The size of the large long string fields is set by default to 256KB, but that can be increased by changing the **OpenPages | Platform | Repository | Resource | Large Text | Maximum Size** setting.

Note:

- For more information on long string data types, see "About Data Types" on page 111.
- For information on setting display types for long string fields, see "Configuring Display Types for Long String Fields" on page 227.
- For information on filtering on long string fields, see "Utilities for Filtering on Long String Field Content" on page 373.
- For information on concatenating simple string fields into a long string field, see "String Concatentation Utility" on page 378

Chapter 8. Managing Object Types

This chapter contains the following topics:

About Object Types

An object type is a container with metadata about a specific category of object, such as a Risk or Process object, or a custom form.

From an Object Type page, you can view and access:

- Property information about the object type (such as name, labels, description)
- Field groups (with their field definitions) that are included in this object type
- Allowed parent and child relationships (associations) to other object types
- Filters used to narrow the scope of data for this object type
- Dependent fields and picklists that have been defined for this object type
- Fields for this object type that have been excluded from one or more subsystems
- Facts and dimensions configured for this object type that can be generated by the reporting framework

An object type is identified in the application by the Object Type  icon. Each object type can include one or more field groups and associations to other objects.

For custom forms, such as surveys, you must add an object type for each custom form that you create. For more details, see "Setting Up Custom Forms" on page 154.

For additional information about:

- Configuring groups and fields for an object type, see Chapter 7, "Configuring Fields and Field Groups," on page 103.
- Customizing the display text labels for object types, see Chapter 11, "Localizing Text," on page 235.
- Configuring facts and dimensions in the reporting framework, see "Configuring Facts and Dimensions" on page 66.

Note: If the same management operation is being concurrently modified by another administrator, an error message is displayed requesting that you try again at a latter time.

About Platform Object Types

The IBM OpenPages object model is highly configurable and, depending on your particular business needs, can contain numerous object types.

Because the object types and schema vary widely from customer to customer, Table 24 lists only the Platform object types that are installed, by default, on all systems.

Table 24. Platform Object Types

Icon	Object Name	Singular Label
	SOXBusEntity	Business Entity
	SOXIssue	Issue
	SOXTask	Issue Action Item
	SOXDocument	File
	SOXExternalDocument	Link
	SOXSignature	Signature
	SOXMilestone	Milestone
	ProjectActionItem	Milestone Action Item
---	SOXProject	Project

Note: The SOXProject object type is for **system use only**; it is the "master" parent object type for all top level Business Entities and top level Milestones.

About Property Rendering JSP Files

Note: For AIX environments, see your IBM representative for assistance.

Note: The information in this topic applies only to Windows environments.

Every object type requires a property rendering JSP file. The JSP file controls the format of the various elements that comprise the layout of a form on a Web page.

The IBM OpenPages application supplies a generic property rendering JSP file, called properties.jsp, that is used by the various object types and cannot be changed. This file is located in the `<OP_Home>|applications|op-apps|sosa|activityview` folder.

Where:

`<OP_Home>` is the installation location of the OpenPages application. By default, this is `c:\OpenPages`.

Note: For backward compatibility with upgraded systems prior to the IBM OpenPages 5.5 release, the existing JSP file, called renderProperties.jsp, is still used by the standard objects' definitions. This existing file, however, maps to the properties.jsp file.

For custom forms, you can either create your own custom property rendering JSP file or use the supplied properties.jsp file. If you choose to use the supplied JSP file for a custom form or survey, when the form or survey displays on a page, it will have the standard look and feel of an object page.

If you choose to create custom property rendering JSP files to use with your custom forms or surveys, it is recommended that you create a "survey" folder under the \sosa folder path in which to store your custom JSP file or files. For example:

```
<OP_Home>\applications\op-apps\sosa\survey
```

For assistance in creating custom property rendering JSP files, see your OpenPages Managing Consultant.

When you create a new object type for a custom form, the path you provide for the JSP file will be relative to the ...\applications\op-apps\sosa folder.

Accessing Object Types

Note: To access the **Object Types** menu item, you must have the **Object Types** application permission set on your account (for details, see "Configuring Application Permissions" on page 18).

Procedure

1. Log on to the IBM OpenPages application as a user with the **Object Types** application permission set.
2. From the menu bar, select **Administration** and click **Object Types**.
3. To go to the detail page of an object type, click the name of the object type in the list (for example, SOXControl).

   From the detail page of an object type, you can configure properties, such as which field groups should be included or excluded, associate parent and/or child object types, manage filters, dependent fields, and so forth.

Configuring Object Type Properties

From the detail page of an object type, you can configure field groups, associate objects, and edit object type properties.

Editing Object Type Properties

You can edit the description of an object type and set whether or not you want to keep older versions of instances for that object type. The JSP Path can only be edited for custom forms.

Note: Do not use characters defined in CJK Unified Ideographs EXTENSION-B on Unicode in the description field of an object type.

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list, click the name of the object type you want to modify.
3. On the **Object Type Information** tab, click **Edit**.
4. On the edit page, make the necessary changes.
5. If you want to save an older version of this object type, select the **Save older versions of this object type?** check box.
6. When finished, click **Save**.

   Note: To change label text for an object type, see Chapter 11, "Localizing Text," on page 235.

Including Field Groups for an Object Type

A field group (either new or existing) must be added to an object type before any of the fields within the field group can be selected for display on an object's view page. To create a new field group, see "Setting Up New Fields" on page 110.

The object type can be a predefined object type (see the topic, "About Platform Object Types" on page 144, for a list of object types) or a custom form object type.

Note:

- Before you can add a field group to a custom form or survey, you must first create an object type for that custom form or survey and then add field groups to it (see the topic, "Adding an Object Type for a Custom Form" on page 155, for details).
- To perform these steps, System Administration Mode must be enabled in the application interface (see "Enabling and Disabling System Admin Mode" on page 58).

When you include a field group for an object type, the field group displays in the list on the **Included Field Groups** tab of the selected object. Once the field group has been included, you can then select which fields you want to make visible to users. For details, see "Setting Up New Fields" on page 110.

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list, click the name of the object type you want.
3. On the **Included Field Groups** table, click **Include**.
4. On the Select Field Group Information page, select the check box next to the field group you want to include. If wanted, you can select multiple boxes.
5. When finished, click **Add**.
6. To make the individual fields within the field group visible to users in an object view, see "About Object Type Views" on page 194.

Removing Field Groups From an Object Type

If a field group has become obsolete or is no longer wanted, you can remove it from an object type.

When you remove a field group from an object type:

- The field group is excluded from the list on the **Included Field Groups** tab of the selected object type.

- If any object fields from the field group have been included in the profile for the selected object type, these object fields are automatically removed from the profile.

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list, click the name of the object type you want to modify.
3. On the **Included Field Group** tab:
   a. Select the check box next to the field group you want to remove.
   b. When finished, click **Exclude**.
   c. At the confirmation prompt, click **OK**.
   The field group is removed from the list.

Disabling Associations Between Object Types

If an association between a parent or child object type is no longer wanted, you can disable the relationship between these object types.

Note: You must be in System Administration Mode (SAM) to perform this operation (see Chapter 4, "Using System Admin Mode," on page 57).

Example 1: If a survey becomes obsolete and you no longer want it associated with a specific object type (such as a Risk object), you can disable the association between the survey object and the parent object type (SOXRisk).

Example 2: If you do not want users to associate certain object types together, such as Accounts with Business Entities, you can disable the association between the child object type (SOXAccount) and the parent object type (SOXBusEntity).

When you disable an association between object types, the following occurs:

- For objects:
  - The entry for the child object type on the navigation pane is removed from the Detail View page of the parent object type.
  - The entry for the parent object type on the navigation pane is removed from the Detail View page of the child object type.
- For a custom form or survey, the custom form or survey is removed from the list of available form types that can be added from the **Associated Files and Forms** tab of a parent object.
- The **Disable** button on the **Association Detail Info** page for the child object type changes to **Enable**.
- The value of the **Enabled** property changes from "true" to "false".
- The object type is removed from the Audit Trail page and Audit reports, even if the object type is a child for a different parent.
- The value of the setting is displayed as Read-only on the Child Association Detail Info page.

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list, click the name of the object type you want to modify.
3. Depending on the association you want to disable, navigate to either the **Child Associations** tab or **Parent Associations** tab on the Object Type Information detail page of the selected object type.

4. From the list of associated object types, click the name of the object type that you want to disable.
5. On the Association Detail Info page, click **Disable**. The button changes to **Enable**.
6. To propagate the object relationship changes to reports, do the following:
   a. Update the Reporting Schema. For details, see "Creating or Re-creating the Reporting Schema" on page 60.
   b. Regenerate the reporting framework. For details, see "Updating the Reporting Framework" on page 64.

Enabling Associations Between Object Types

If you want to allow an association between a parent or child object type that was, for example, previously disabled, you can enable the association between these object types.

Note: You must be in System Administration Mode (SAM) to perform this operation (see Chapter 4, "Using System Admin Mode," on page 57).

When you enable an association between object types, the following occurs:

- The enabled child object type displays on the detail page of the parent object type.
- The **Enable** button changes to **Disable** on the Association Detail Info page.
- The value of the **Enabled** property changes from "false" to "true" on the Child or Parent Associations tab.
- The object type is included in the Audit Trail page and Audit reports
- The value of the setting is displayed as Read-only on the Child Association Detail Info page.

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list, click the name of the object type you want to modify.
3. Depending on the association you want to enable, navigate to either the **Child Associations** tab or **Parent Associations** tab on the detail page of the selected object type.
4. From the list of associated object types, click the name of the object type that you want to enable.
5. On the Association Detail Info page, click **Enable**. The button changes to **Disable**.
6. To propagate the object relationship changes to reports, do the following:
   a. Update the Reporting Schema. For details, see "Creating or Re-creating the Reporting Schema" on page 60.
   b. Regenerate the reporting framework. For details, see "Updating the Reporting Framework" on page 64.

About Object Relationship Types

The IBM OpenPages application requires that an object model must not contain relationship definitions that result in a loop (a cyclic relationship) when the object hierarchy is traversed.

Within the IBM OpenPages application, a relationship type can be defined as either 'Association' or 'Reference' between objects in the object model.

The ‘Association’ type relationship is the typical relationship that exists between parent and child objects in the object hierarchy. The ‘Reference’ type relationship is a non-parent-child relationship that can exist between objects.

For customers doing a first-time ("fresh") installation, the IBM OpenPages application will not allow loops to be created in the new model.

However, for customers that are upgrading from a version prior to IBM OpenPages 5.5, the object model may contain relationship definitions that create a loop or cyclic relationship between objects. If the IBM OpenPages application encounters such a loop between objects in the hierarchy, some pages may return incomplete results. For details about running a script to analyze your object model for unused and/or cyclic relationships, see "Correcting Cyclic Relationships" in the *IBM OpenPages Upgrade Guide*.

Figure 8 demonstrates how a path from SubAccount to Process in an object model can create a loop or cyclic relationship. That is, starting at Entity, as you traverse the hierarchy through the parent-child relationships, you enter a loop between SubAccount and Process. This is an invalid configuration.

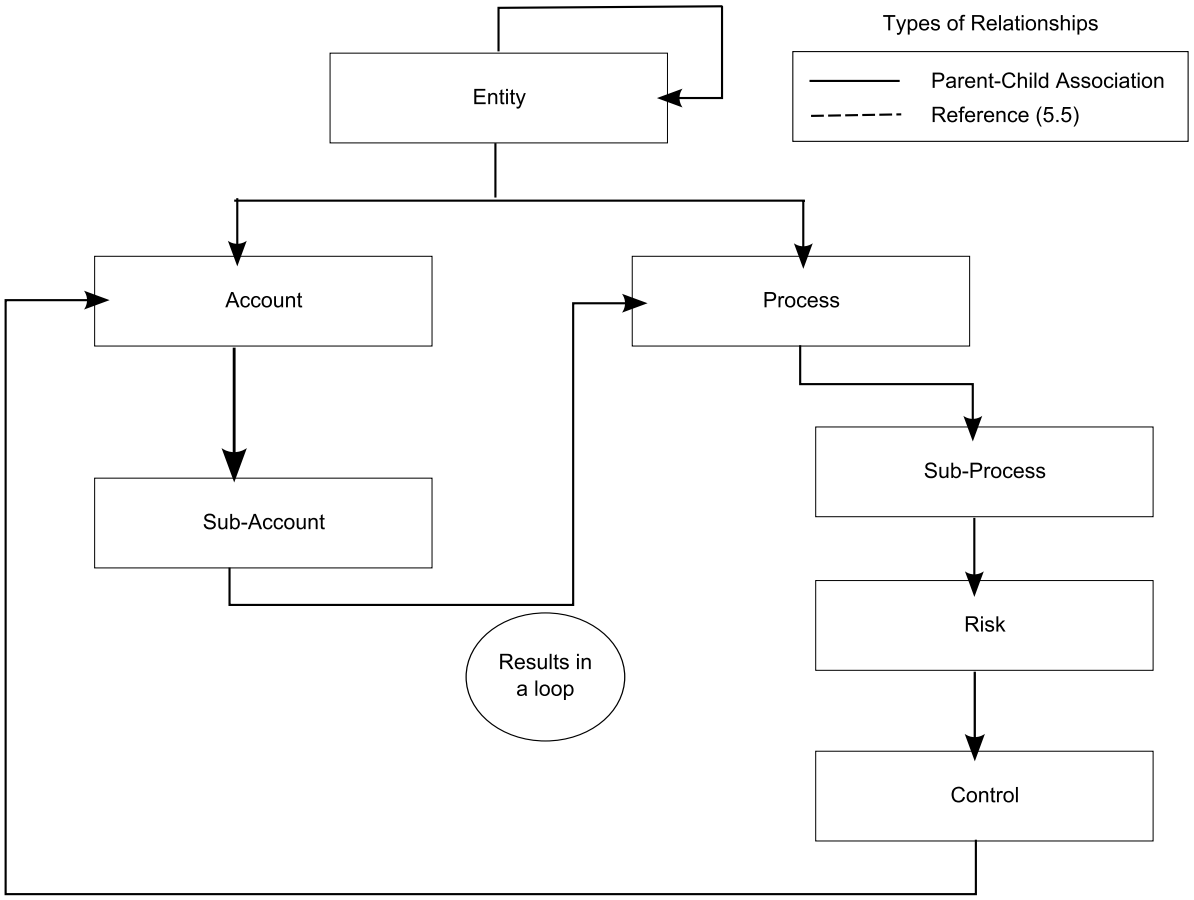


Figure 8. Sample Invalid Cyclic Relationship

To resolve a loop or cyclic relationship between objects in the hierarchy, upgrade customers can:

- Disable the relationship that creates the loop. For example, if the relationship defined in the object model is superfluous and is not being used (that is, there

exists no instance data in your database that has these relationships), then you should disable the relationship. For details, see “Disabling Associations Between Object Types” on page 147.

- Leave the relationship that creates the loop, but change its type. For example, if you need to retain the relationship that creates a loop because the object model accurately describes your business, you can leave it and change its type from ‘Association’ to ‘Reference’ (see Figure 9). For details on changing the reference type, see “Setting the Relationship Type.”

Figure 9 illustrates how a valid relationship between SubAccount and Process can be maintained without a loop by changing the Relationship Type between these objects from ‘Associative’ to ‘Reference’.

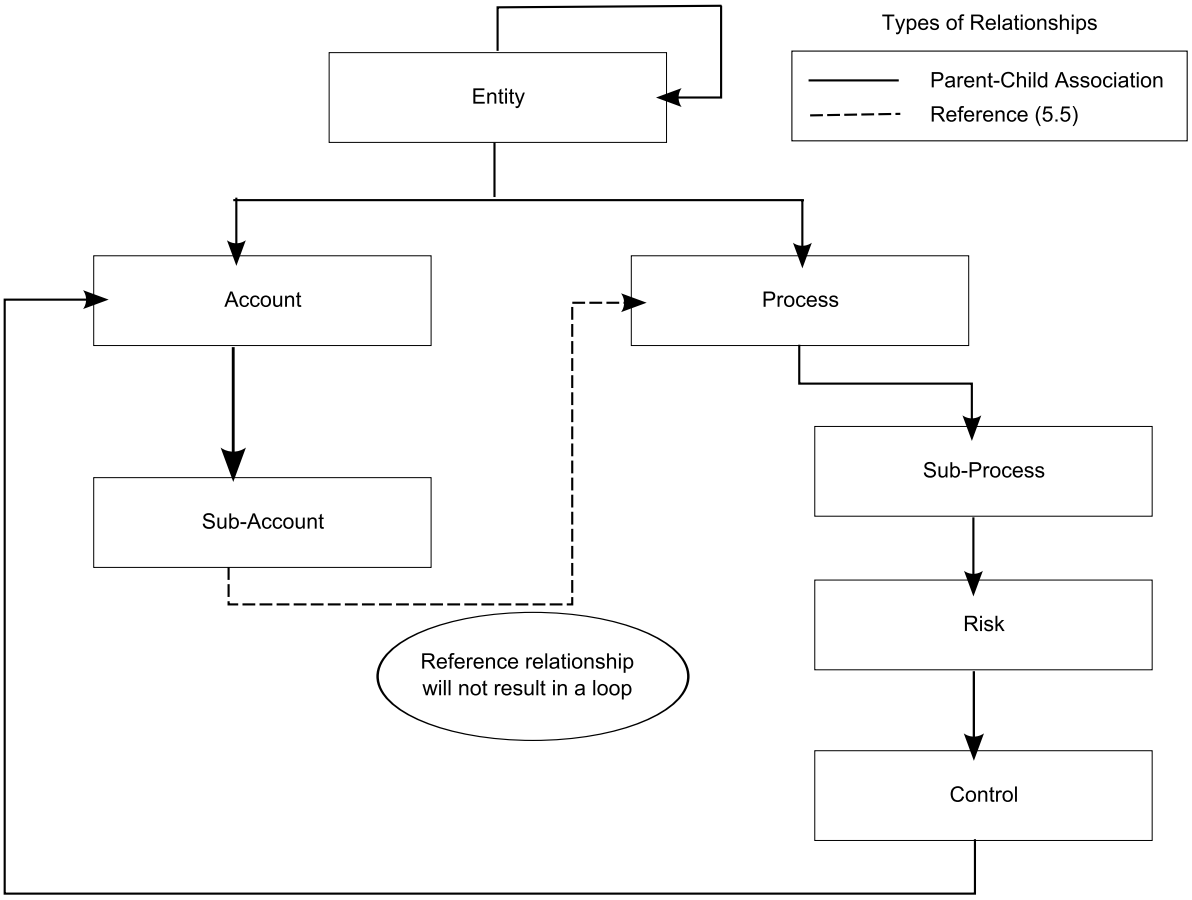


Figure 9. Sample Reference Relationship

Setting the Relationship Type

Note: You must be in System Administration Mode (SAM) to perform this operation (see Chapter 4, “Using System Admin Mode,” on page 57).

Procedure

1. Access the Object Types page (see “Accessing Object Types” on page 145).
2. From the list, click the name of the parent object type with the child relationship you want to modify.
3. On the **Child Associations** tab, select the child object whose relationship you want to modify.

4. On the **Association Detail Info** tab, click **Edit**.
5. Click the **Relationship Type** arrow and select a value from the list. If the selected value results in a loop, an error message is displayed.
6. When finished, click **Save**.

Modifying Cardinality Settings

Cardinality settings within the IBM OpenPages application are used to determine if a given object can be created as a standalone object and whether or not it can be shared by (associated to) more than one parent object.

Important: The setting values are used to control the presence of specific buttons on the user interface that allow users to create objects as either standalone or shared. The setting values are NOT currently used to enforce the number of associations between object instances.

In new IBM OpenPages installations, the default values for the minimum (Min Children = 0) and maximum (Max Children = 2147483647) number of children should not be modified.

Displaying the Add New Button for Standalone Objects

When you add a new child object type from the detail page of a parent object type, the child object type is created and automatically associated with that parent object type. A "standalone" object instance is a child object that is not associated with any parent object.

For example, if you select the **Risks** menu item on the **Assessments** menu, and then click the 'Add New' button on the Risk Folder View page to create a new child Risk object, that child object is created in the top-level Risk object type folder but would not be associated with any parent object.

You can control the ability of users to create standalone instances of an object type by configuring the value of the minimum parents cardinality setting.

If the value of the minimum parents cardinality setting, `Min Parents`, is set to:

- **0** -- the **Add New** button displays on the object's Folder View page and users are able to create standalone instances of a child object type. If a child object type has multiple parent relationships, the value of Min Parents must be set to zero for every relationship in which that object type is a child. You cannot create standalone objects from a Detail View or Activity View page.
- **1** -- the **Add New** button is removed from the object's Folder View page and users will not be able to create standalone instances of a child object type. This is the default value in new product installations.

Note: For data consistency, the minimum parent setting should always be set to either 0 or 1. A minimum parent setting greater than 1 is effectively the same as setting it to 1.

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list, click the name of the object type whose cardinality you want to modify.
3. On the **Parent Associations** tab, click the name of a parent object type.
4. On the **Association Detail Info** tab, click **Edit**.

5. In the **Min Parents** box, enter **0** (for standalone) or **1** (for not standalone).
6. When finished, click **Save**.

   Note: To return to the object type detail page, click the name of the object type in the breadcrumbs at the top of the page.
7. If there are multiple parent objects, repeat Steps 3 - 6 for each parent object.

   Example

   Let's say a company does not want users to create standalone Processes. You could remove the **Add New** button from the **Processes** Folder View page for all relationships that specify the Process child object type by doing the following.

   a. From the menu bar, select **Administration** and click **Object Types**.
   b. From the list, click **SOXProcess**.
   c. For each parent object listed under the **Parent Associations** tab, set the minimum number of parents to 1 in all the relationships that specify the Process child object type as follows:
      1) Click the name of a parent object to open its detail page.
      2) Click **Edit** and set **Min Parents** to **1**.
      3) Click **Save** to save the modified setting.

Displaying the Associate/Disassociate Buttons for Shared Objects

For object type relationships that contain a child object type, you can control the ability of users to associate instances of a child object type by configuring the value of the maximum parents cardinality setting.

If the value of the maximum parents cardinality setting, `Max Parents`, is set to:

- **2147483647** (infinity) -- the **Associate** and **Disassociate** menu items are displayed on the Action Menu of the object type on a detail page, and users will be able to associate that object to more than one parent object. The default value is 2147483647 in new product installations.
- **1** -- the **Associate** and **Disassociate** menu items are removed from the Action Menu of the object type on a detail page, and users will not be able to create shared instances of a child object type.

Note: There is currently no enforcement of the maximum parents setting on the number of parent associations that a given child object can have. For instance, if the maximum parents setting is 2, the application will still allow a given child object to be shared among 3 or more parent objects of the same type. A maximum parent setting of greater than 2 is effectively the same as setting it to infinity.

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list, click the name of the parent object type whose child relationships you want to modify.
3. On the **Child Associations** tab, click the name of the child object type you want to modify.
4. On the **Association Detail Info** tab, click **Edit**.
5. In the **Max Parents** box, enter 2147483647 (for shared) or **1** (for not shared).
6. When finished, click **Save**.

   Note: To return to the object type detail page, click the name of the object type in the breadcrumbs at the top of the page.

7. If there are multiple child objects for which you want to restrict the parent object relationship, repeat Steps 3 - 6 for each child object.

   Example

   Let's say a company does not want users to associate and share Processes among Business Entities. You could remove the **Associate** and **Disassociate** menu items from the Process Action Menu on the detail page by doing the following.

   a. From the menu bar, select **Administration** and click **Object Types**.
   b. From the list, click **SOXBusEntity**.
   c. Navigate to the **Child Associations** tab.
   d. Click **SOXProcess** to open its detail page.
   e. Click **Edit** and set **Max Parents** to **1**.
   f. Click **Save** to save the modified setting.

Configuring File Type Information

A file type describes the structure or format of a file and is typically reflected in the file name extension. Some common examples of file name extensions include .RTF (Rich Text Format), .TXT (ASCII text), .DOC (Microsoft Word), .PDF (Portable Document Format), .XLS (Microsoft Excel), .HTM (Hypertext Markup Language), and .JSP (Java Server Page).

Note: Only the SOXDocument object type supports file types.

Each file type has a corresponding MIME (Multipurpose Internet Mail Extension) type associated with it, which is a standardized data exchange method used by Web browsers to associate files with helper applications that display files of that type. For example, a MIME type of image/gif, informs the browser to handle the data as an image. The IBM OpenPages application supplies a number of predefined MIME types.

Adding a New File Type

Before you add a new file type to the application, verify that the file type does not already exist.

To view a list of supplied file types, click **Include** on the **File Types Information** tab of the SOXDocument object type. If the file type that you want to add is:

- Displayed in the list - go to "Associating a File Type with an Object Type" on page 154.
- Not displayed in the list - click **Cancel** and proceed with the instructions in this section.

When you add a new file type to the application, it is automatically added to the File Type Information selection list.

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list, click the **SOXDocument** object type.
3. On the **File Types Information** tab, click **Add New**.
4. On the add page:
   a. In the **MIME Type** box, enter a MIME content type and subtype. For example, image/cgm.

b. In the File Extension box, type a file extension that corresponds to the MIME Type. For example, cgm.
c. When finished, click **Create**.

5. To associate the new file type with the SOXDocument object type, see "Associating a File Type with an Object Type."

Associating a File Type with an Object Type

You can associate various file types with the SOXDocument object type. If you have added a new file type, you will need to associate it with the object type before it can be used.

Note: When you attach a file to an object, the file extension is case sensitive and must match the extension specified in the File Types Information section of the SOXDocument object type.

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list, click the **SOXDocument** object type.
3. On the **File Types Information** tab, click **Include**.
4. From the list on the Select File Type Information page:
   a. Select the check box next to the name and MIME type you want to add. If wanted, you can select multiple boxes.
   b. When finished, scroll to the bottom of the page and click **Add**.
   The newly associated file type is listed on the **File Types Information** tab of the SOXDocument object type.

Removing a File Type From an Object Type

You can remove a file type from the SOXDocument object type if file type is not in use. Removing a file type from an object type does not remove the file type from the File Type Information selection list.

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list, click the **SOXDocument** object type.
3. On the **File Types Information** tab:
   a. Select the check box next to the name and MIME type you want to remove.
   b. Click **Exclude**.
   c. At the prompt, click **OK** to remove the file type.

Results

The associated file type is removed from the list on the **File Types Information** tab of the SOXDocument object type.

Setting Up Custom Forms

Process Overview

Table 25 on page 155 outlines the tasks you need to follow for setting up a new custom form, such as a survey, for use by object types in the application.

Note: If you imported a custom form, such as a survey, through the ObjectManager, then you only need to perform Task 6.

Table 25. Tasks for Adding Custom Forms

Task	Task Description	Related Topic
1	Create an object type for the custom form.	See "Adding an Object Type for a Custom Form" for step-by-step instructions on how to create an object type for a custom form.
2	Add a field group for the custom form object fields.	See "Adding New Field Groups" on page 110 for step-by-step instructions on how to create one or more field groups that will contain the fields for the custom form.
3	Add one or more field definitions to the new field group.	See "Adding Field Definitions to a Field Group" on page 110 for instructions on how to add new field definitions to a new field group.
4	Add the new field group to the custom form object type.	See "Including Field Groups for an Object Type" on page 146 for information about how to add the new field group to a custom form object type so the fields can be available for display.
5	Associate the custom form object type with a parent object type.	See "Associating a Custom Form to an Object Type" on page 156 for information about how to associate a child object type (custom form) with a parent object type.
6	Include the new custom form object type in a profile.	See "Including Object Types in a Profile" on page 180 for information about how to include the custom form object type on an object's view page.
7	(optional) If you want to run CommandCenter reports against a custom object type, specify a custom prefix for the real-time reporting schema tables	See "Enabling Reporting for Custom Forms" on page 310 for information about adding a custom prefix.

Adding an Object Type for a Custom Form

If you want to add a custom form, such as a survey, to an object, you must first create an object type for that custom form. Once the object type is created, you can include field groups and associate parent objects to it.

Note: To perform these steps, System Administration Mode must be enabled in the application interface (see "Enabling and Disabling System Admin Mode" on page 58).

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. On the **Object Types** tab, click **Add**.

3. On the add page, do the following:
   a. In the **Name** box, type a name for the new object type.

      Important:
      - The name must start with a letter, and can only contain letters, numbers, and the underscore (_) character.
      - The name is also used as the initial label for the object type and cannot be modified after it is created.

      Examples:

      `RiskSurvey, survey1, Survey1_Risk`
   b. In the **Description** box, optionally type a description.

      Note: Do not use characters defined in CJK Unified Ideographs EXTENSION-B on Unicode in the description field of an object type.
   c. In the **JSP Path** box, type the folder path and name of the .jsp file that will be used by the object type to render the layout and presentation of the object on the Web application page. The default path is /propertyForm/renderProperties.jsp.

      Note: The path of the JSP file is relative to the ...\openpagesdomain\applications\sosa\ folder.
      If you are using, for example, a custom JSP file, the folder and file name might look similar to this: /Survey/MySurvey.jsp.
   d. When finished, click **Create**.
      The object type is created, and the Object Type detail page displays where you can configure properties. For details see, "Configuring Object Type Properties" on page 145.
4. If you want to run CommandCenter reports against this custom object type, you must configure a custom prefix for the real-time reporting schema tables. For details, see "Enabling Reporting for Custom Forms" on page 310.

Deleting a Custom Object Type

You can only delete custom object types that are not in use in the application.

Note: You must be in System Administration Mode (SAM) to perform this operation (see Chapter 4, "Using System Admin Mode," on page 57).

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list, select the check box next to the object type you want to delete. If wanted, you can select multiple boxes.
3. On the **Object Types** tab, click **Delete**.
4. At the confirmation prompt, click **OK** to delete the object type.

Associating a Custom Form to an Object Type

If you want a custom form or survey to be associated with a specific type of object, you can add this object association from either the detail page of an object type or the detail page of a custom form or survey.

Note: You must be in System Administration Mode (SAM) to perform this operation (see Chapter 4, "Using System Admin Mode," on page 57).

From the Details Page of a Parent Object

Note: You can only add child object associations to object types; you cannot add child associations to custom form or survey object types.

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list, click the name of the object type you want to modify.
3. On the **Child Associations** tab, click **Add**.
4. On the **Available Custom Forms** page, select the check box next to each custom form you want to associate with the selected parent object type.
5. When finished, click **Add**.

From the Details Page of a Custom Form Object

Note: You can only add parent object associations to custom form or survey object types; you cannot add new parent object associations to an object type.

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list, click the name of the object type you want to modify.
3. On the **Parent Associations** tab, click **Add**.
4. On the Available Object Types page, select the check box next to each parent object to which you want to attach this object type.
5. When finished, click **Add**.

Managing Filters for an Object Type

Overview

Filters are specific to an object type and are typically used to narrow the scope of data that will be returned in a particular view for that object type. When you create a filter for an object type, you can select which fields to use to search for data. Only the objects that match the specified search criteria will be returned for that object type.

Filters are used with Filtered List Views, Activity Views, and the Home page. An object type can have multiple filters.

Table 26 provides an overview of the flow of tasks for adding filters to object types and views.

Table 26. Tasks for Configuring Filters and Views

Task	Task Description	Related Topic
1	Determine the purpose and characteristics of the filter.	"Before You Begin - Filter Considerations" on page 158
2	Add the filter to an object type.	"Adding Filters to Object Types" on page 158
3	Select a profile and associate the filter to a view.	"Associating Filters With Views" on page 163

Before You Begin - Filter Considerations

Before you create a new filter, you need to determine the characteristics of the filter and identify the object type on which the new filter will be used. Planning your changes ahead of time helps to minimize the necessary work and prevents duplication of effort.

For instructions on creating a filter, see “Adding Filters to Object Types.”

The following list will help you identify some of the information you need to have before you create a new filter:

- Object type - Which object type will the filter be used with?
- Name - How will the new filter be identified? The name of the filter is important because it is also the initial label that will appear for the filter in the application.
- Profiles - Which profile (or profiles) will be associated with the filter?
- Filtering criteria - Which fields should be used in the filter criteria to narrow the scope of data returned by the search?
- Views - Which type of view page in a profile will use the filter (Filtered List View, Home page, Activity View)?

Example

Let’s say you create a filter for risk assessments called "In Progress" that displays all risk assessments due within the next three months, and has the following selected fields and values:

Field	Value
Status	In Progress
Start Date	On this date
End Date	In the next 90 days

If you associate this filter to a **Filtered List View** in the "Assessors" profile, application users who are assigned the ‘Assessors’ profile would then be able to select this filter from the Risk Assessment Filtered List View filter selection list.

You could also create a personalized "My In-Progress Risk Assessments" filter for use on the Home page from the "In Progress" filter. You would do this by making a copy (see “Copying Filters” on page 164) of the "In Progress" filter, renaming it to "My In-Progress Risk Assessments", and selecting "End User" as the ‘Assessor’. When you configure the "My In-Progress Risk Assessments" filter for the **Home** page, application users who were assigned the "Assessors" profile would only see their assigned risk assessments that were due within the next 3 months on their Home page.

Adding Filters to Object Types

Filters are specific to an object type and are typically used to narrow the scope of data that will be returned in a particular view for that object type. When you

create a filter for an object type, you can select which fields to use to search for data. Only the objects that match the specified search criteria will be returned for that object type.

For up-to-date results of filters that include long string fields, the text index for the long string field must have been synchronized with the values in the field. Synchronization depends on when the index was created or the setting of scheduled synchronization. For details on the index creation and synchronization utilities provided for long string filtering, see "Utilities for Filtering on Long String Field Content" on page 373.

Note: Text that you enter into text boxes is not case sensitive.

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list, click the name of the object type you want to modify.
3. On the **Filters** tab of the selected object type, click **Add**.
4. On the **Add Filter** page:
   a. Click the **Field** arrow and select a key field from the list. Common fields are listed at the top, followed by fields specific to the object type.
   b. In the same row as the key field, specify a search condition. The available search conditions change depending on the selected field. For example, for a name field, the options are **Starts with**, **Contains**, and **Equals**, with a following text box in which to enter a value.

      Note: Text that you enter into text boxes is not case sensitive.

Table 27. Search Conditions

If a field has a...	You can do this...
	Click to select a value from a phonebook.
	Click to search for a user.
End User link	Click to insert "End User" into the value. The value "End User" will resolve to the currently logged-on user. For details on the currently logged in user, see "Filtering on the Currently Logged On User" on page 163
Select Values link	Select from a list of values.
Text box for alphanumeric values	Select a search condition (such as **Starts with**) and then enter a value.
 or a text box for date ranges.	Click the calendar icon to select specific dates, or select a search condition (such as **Within the last**) and then enter a value.
Text box for numeric values (used in computed fields)	Select a search condition (such as =) and then enter a value.
	Click the **true** or **false**.

Important: For limitations on the special characters in filters for long string fields, see "Limitations on Using Special Characters in Filters for Long String Fields" on page 160.

c. To add another row and key field on which to search, click the **Add** link and repeat step 4.

   By default, all the rows are connected (by their sequential number) with an `AND` operator (for example `1 AND 2 AND 3`). That is, all of the conditions specified must be true.

   For details on specifying more complex logic for your filters, see "Using Complex Logic in a Search Filter" on page 162.

d. When finished, click **Save**.

5. To associated the filter with a view, see "Associating Filters With Views" on page 163.
6. To create a duplicate filter using the new filter as a template, see "Copying Filters" on page 164
7. To localize the display name of a filter, see "Modifying Display Text for Public Filters" on page 238.

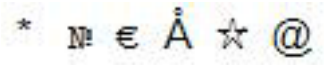
Limitations on Using Special Characters in Filters for Long String Fields

When creating filters for long string fields, there are limitations on some special characters and how they are used.

Do Not Use as First or Last Character

When you use a filter to search for text in long string fields, the following special characters and symbols may not return the expected results if these characters are the first or last character in the text to be searched:

- Characters in languages such as Chinese, Japanese and Thai
- Some three-byte Unicode characters and symbols such as:



Note: When searching for text containing these special characters, you must use the **Contains** search condition in the filter.

Example

Let's say you want to search for text that has the phrase 'maximum € 120'. For the selected text field, you would choose the **Contains** search condition, and in the **Text box**, type the words: `maximum € 120`.

The search results would return the following: "The maximum € 120 is the upper limit" because the special character appears in the middle of the text and not at either the beginning or end.

The search results would NOT include the following: "€ 120 is the maximum upper limit" or "The maximum upper limit is 120 €" because the special character is the first or last character in the text.

Do Not Use

The following special characters are not supported in the search filter and should not be used:

Special Character	Description
&	Ampersand
@	At symbol on keyboard
*	Asterisk
!	Exclamation point or bang
\	Backward slash
/	Forward slash
^	Caret or circumflex
:	Colon
;	Semicolon
,	Comma
-	Dash
_	Underscore
>	Greater than sign
<	Less than sign
(	Opening parenthesis
)	Closing parenthesis
=	Equal sign
%	Percent sign
|	Pipe or vertical bar
+	Plus sign
#	Pound or number sign, hash symbol
?	Question mark
~	Tilde or equivalency sign
`	Grave accent
[	Opening bracket
]	Closing bracket
{	Opening brace
}	Closing brace
$	Dollar sign
¥	Yen sign
₩	Won sign
	Yi syllable IT
	Double vertical lines

The following reserved words are not supported in the search filter and should not be used:

ABOUT, ACCUM, AND, BT, BTG, BTI, BT, EQUIV, FUZZY, HASPATH, INPATH, MDATA, MINUS, NEAR, NOT, NT, NTG, NTI, NTP, OR, PT, RT, SQE, SYN, TR, TRSYN, TT, WITHIN

Note: Reserved words are not case-sensitive.

Using Complex Logic in a Search Filter

You can add complex logic to filters to help refine searches using logical operators such as OR, NOT, and parentheses. By default, the system uses only the `AND` operator to return results from a filtered search.

When you create a filter (see "Adding Filters to Object Types" on page 158) you select object fields and define the search criteria for each selected field. These key fields are then used by the system to search the database for objects that meet the specified criteria.

Every key field that is selected in a filter is displayed in a row that is sequentially numbered. This number of the row is its identifier. For example, the first key search field is displayed in row number 1, the next key search field is in row number 2, the next one in row number 3, and so forth. You use the row identifier with a logical operator to create a complex logic search expression. Although row identifiers are sequential, the identifier can appear in any order within the expression.

Use the logical operators described in the following table to define filtered searches. The operators are not case sensitive.

Table 28. Logical Operators for Complex Logic

Operator	Purpose	Example
AND	Narrow the search for objects that meet all the search criteria. This is the default operator used to return results from a search filter.	`1 AND 2 AND 3`
OR	Broaden the search for objects that meet one or the other key search criteria.	`1 OR 2 OR 3`
NOT	Narrow the search for objects by excluding the specified key search criteria.	`1 AND NOT 2`
( )	Group search criteria together to show the order in which the query should be applied.	`1 AND (2 OR 3)`

Procedure

1. In a **Filter** window (adding or editing a filter), click **Use Complex Logic**.
2. In the **Logic** text box, modify the search expression as wanted using the logical operators. To close the **Logic** text box and revert to the default search logic, click **Clear Complex Logic**.
3. When finished, click **Save** or select from **Actions** menu.

Example

An Example Using the OR Operator

Let's say you have 3 search fields defined in your filter. By default, the system uses only the `AND` operator so it would retrieve objects that only matched all 3 fields (`1 AND 2 AND 3`). If, however, you wanted to broaden the search so it included field 1

and either fields 2 or 3, use the OR operator to modify the search to retrieve all objects that matched field 1 and matched either fields 2 or 3.

To do this, create the logical expression: `1 AND (2 OR 3)`.

An Example Using the NOT Operator

Let's say you want to find open Issue objects that are not assigned to you. To create such a filter, you would select the "Issue Status" field and choose the "Open" value (this is field 1). Then select the "Assignee" field and choose your name from the **Select the user** window or click the **End User** link (this is field 2).

To exclude your name from the search results, in the **Logic** text box, you would type `1 AND NOT 2`.

Note: The NOT operator does not return objects that have an empty, blank, or null value in the selected field criteria. This means that any unassigned Issue objects (that is, the "Assignee" field was empty or blank), would be excluded from the search results.

Associating Filters With Views

Once you create a filter for an object type, you can associate it to a profile and an object view.

Table 29. Associating Filters

If you want to do this...	Then, go here for details...
Display the filter for selection by application users in the filters list under 'Public filters' on a Filtered List View page for an object type.	"Associating Filters to Filtered List View Pages" on page 207
Use the filter to personalize the Home page for users who are assigned a particular profile.	"Configuring Filtered Lists on the Classic Tab" on page 190
Use the filter in an Activity View page to limit the scope of listed child objects.	"About the Layout of Activity Views" on page 208 or "Modifying an Activity View" on page 215

Filtering on the Currently Logged On User

If you want to create a filter that scopes the search to the currently logged on user for specific object type fields (such as "Process Owner" or "Control Owner"), you can do one of the following:

- Change the display type of the field from "Text" to one of the following display type options:
  - User Selector
  - User Dropdown
  - User/Group Selector
  - Group Selector

    and then click the **End User** link. The value "End User" that is displayed in the box will resolve to the currently logged-on user. For details on modifying a display type for a field, see "Selecting a Display Type for Simple String Fields" on page 221.

- Type the following code into the text box of the object-specific field:
  ```
  ##{logged in user}##
  ```

Copying Filters

You can save an existing filter with a new name to use as a template. Once the new filter is created, change the search criteria to suit your needs.

Note: Because filters contain object-specific fields, you can only copy filters within the same Object type; you cannot copy filters between Object types.

Procedure

1. Access the **Object Types** page (see "Accessing Object Types" on page 145).
2. From the list, click the name of the Object type you want to modify.
3. On the **Filters** tab, click the filter you want to copy. The **Edit** window opens for the filter.
4. Select **Save as** from the **Actions** menu to copy the settings of the selected filter to a new filter.
5. In the **Save As** window:
   a. Type a unique name (required) and optional description for the new filter.
   b. Click **Apply**.

Results

The new filter is now available in the **Filters** tab for any changes you want to make. For instructions on specifying filters and using complex logic in filters, see "Adding Filters to Object Types" on page 158 and "Using Complex Logic in a Search Filter" on page 162.

To display the new filter in the list of 'Saved Filters' on an object's Filtered List View page, add it to a profile. For details, see "Associating Filters to Filtered List View Pages" on page 207.

Modifying Filters

Once you create a filter, you can modify it as necessary. The modifications, once saved, are immediately effected in the application.

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list, click the name of the Object type you want to modify.
3. On the **Filters** tab, click the filter you want to edit. The **Edit** window opens for the filter.
4. In the **Edit** window, make the required changes.
5. When finished, click **Save**.
6. To modify a localized display name of a filter, see "Modifying Display Text for Public Filters" on page 238.

Results

For instructions on specifying filters and using complex logic in filters, see "Adding Filters to Object Types" on page 158 and "Using Complex Logic in a Search Filter" on page 162.

To display the filter in the list of 'Saved Filters' on an object's Filtered List View page, add it to a profile. For details, see "Associating Filters to Filtered List View Pages" on page 207.

Deleting Filters

When you delete a filter for an Object type, it is permanently deleted from the system and cannot be restored.

If the filter is associated to one or more object views in a profile (such as a Filtered List View or table on the Classic tab of a Home page), the filter, when deleted, is immediately removed from the view and is no longer available to users who are assigned that profile.

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list, click the name of the object type you want to modify.
3. On the **Filters** tab, select the check box next to the filter or filters you want to delete.
4. Click Delete.
5. At the prompt, click **OK** to delete the all the checked filters.

Configuring Dependent Field Behavior

You can configure a field so that its behavior - Visible, Editable, or Required - is dependent upon some value selected by a user in another field or set of fields. The dynamic behavior of dependent fields can be used to help guide users during the creation or editing of an object.

Example

Let's say you want to know who will perform a control activity if a user selects 'No' to the question 'Does the Control Owner perform the Control?'.

You could configure the behavior of the field 'Who Performs the Control?' to be dynamic so that the field is both visible and required only if the user selects 'No' to the question 'Does the Control Owner perform the Control?'. If the user selects 'Yes', then the 'Who Performs the Control?' field would remain hidden from the user.

The 'Who Performs the Control?' field is considered the *dependent* field as the behaviors of this field (Required and Visible) depend on the value (No) selected in the *controller* field, 'Does the Control Owner perform the Control?'.

Adding Dependent Fields

A dependent field can have multiple behaviors and multiple controlling fields. When you add a dependent field, you first configure the field and a behavior, and then select the field and value (or values) that will control that behavior.

If you want a dependent field to have multiple behaviors, such as Required and Visible, you must configure the field separately for each behavior. Only behaviors that have not been previously selected for that dependent field are available for selection.

If you have multiple controlling fields for a specific behavior, you can configure whether one or all conditions must be met before the behavior of the dependent field is triggered.

Note:

- Dependent fields cannot include System Fields.
- Dependent field behavior is not supported for custom forms.
- Controller fields must be enumerated string lists (single or multi-selectable). If you configure a controller field with multiple values, the selection of one or more of these configured values by an application user will trigger the dependent field behavior.
- Computed fields and report fragment fields can only have a behavior of 'Visible'.

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list, click the name of the object type you want to modify.
3. On the **Field Dependencies** tab, click **Add**.
4. On the Select Dependent Field page:
   a. Click the **Select Dependent Field** arrow and choose a field from the list.
   b. In **Dependent Field Behavior**, select one of the following behaviors:

Select this value...	If you want...
Required	to require the user to enter a value in the dependent field only if the controlling field is selected. If the user tries to save the page without entering a required value, a message is displayed saying the field is required.
Editable	the user to be able to modify this dependent field only if the controlling field is selected. Otherwise, the dependent field will be read only.
Visible	the dependent field to be displayed to the user only if the controlling field is selected. Otherwise, the dependent field will be hidden from view.

   c. When finished, click **Next**.
5. On the Select Controller(s) page:
   a. Click the **Controlling Field** arrow and choose a field from the list.
      In the **Controlling Values** box, select one or more values from the list.

      Note: To select multiple values from the list, press and hold the **Ctrl** key while clicking the mouse pointer.
   b. When finished, click **Add**.
   c. To select another controller field from the list, repeat Steps a - c.

d. If you have multiple controller fields, click the **Operator** arrow and choose one of the following logical operator values:

Select this value...	If you want...
And	all the selected controller fields to be used to meet the condition. This is the default operator value.
Or	only one (either/or) of the selected controllers to be used to meet the condition.

e. When finished, click **Finish** to save your changes.

6. To create additional dependent fields:

If you want to...	And the Controllers are...	Then...
Add another behavior to the same dependent field - OR - Create another (different) dependent field	the same as those selected in Step 4	**Note:** Only behaviors that have not been previously selected for this dependent field are available. Do one of the following: • Copy the controller conditions to the new dependent field (see "Copying Controller Conditions") • Repeat Steps 3 and 4
Add another behavior to the same dependent field - OR - Create another (different) dependent field	different from those selected in Step 4	Repeat Steps 3 and 4

The newly created dependent fields are listed on the **Field Dependencies** tab.

Copying Controller Conditions

If you have many field dependencies that use the same controller conditions, you can use the 'Copy Controllers to' function to quickly duplicate existing controller conditions to the same or different dependent fields within the same object type. This method will save you time as it is generally faster and easier than individually adding multiple dependent fields that all have the same controller fields.

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list, click the name of the object type you want to modify.
3. On the **Field Dependencies** tab:
   a. Select the check box next to the controller field you want to copy.
   b. Click the **Copy Controllers to** button.
4. In the Dependent Field pane of the controller (or controllers) you want to copy, select one or more behaviors for each dependent field.
5. When finished, click **Create**.

The newly created dependent fields with the copied controllers are listed on the **Field Dependencies** tab.

Modifying Controllers for a Dependent Field

After you create a dependent field, you can add, remove, or modify the fields that control the behavior of the dependent field. In the case of multiple controllers, you can also change the operator that determines whether one or all the controller conditions must be met before the dependent field behavior is triggered.

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list, click the name of the object type you want to modify.
3. On the **Field Dependencies** tab:
   a. Select the check box next to the dependent field you want to modify.
   b. Click **Edit**.
4. To modify the values of an existing controller field:
   a. Click **Edit** under the **Actions** column.
   b. In the **Edit Controller** box, modify the selected values as necessary.
   c. When finished, click **Save**.
5. To add another controller:
   a. In the Add Controller pane, click the **Controlling Field** arrow and select a field from the list.
   b. In the **Controlling Values** box, select one or more values from the list.
   c. Click **Add**.
6. To remove a controller:
   a. Select the check box next to the controller field you want to remove.

      Note: To select all the controllers for removal, select the check box next to the Controlling Field column heading.
   b. When finished, click **Delete**.
7. To change the operator when there are multiple controllers, click the **Operator** arrow and select a value from the list.
8. When finished, click **Save**.

Enabling and Disabling Field Dependency Behavior

Dependent fields can be enabled or disabled. By default, dependent fields are enabled when created.

When a dependent field is disabled, the following occurs:

- The dependent field remains in the list on the **Field Dependencies** tab, and the value in the **Enabled** column changes from 'true' to 'false'.
- The application does not enforce the conditions that control the behavior of the dependent field.

If you select multiple dependent fields to enable or disable, the application switches the values accordingly. For example, if you select two dependent fields - the first field is enabled with a value of 'true' and the second field is disabled with a value of 'false' - the value of the first dependent field would switch to 'false' making it disabled, and the second would switch to 'true' making it enabled.

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list, click the name of the object type you want to modify.
3. On the **Field Dependencies** tab:
   a. Select the check box next to the dependent field you want to enable or disable. If wanted, you can select multiple boxes.
   b. When finished, click **Enable/Disable**.

      The value in the **Enabled** column on the **Field Dependencies** tab for the selected dependent field changes as follows:
      - If disabled, the value changes from 'true' to 'false'
      - If enabled, the value changes from 'false' to 'true'

Deleting Dependent Fields

When you delete a dependent field, it is permanently removed from the list on the **Field Dependencies** tab, and all corresponding records for the dependency are deleted and cannot be restored.

Important: If a dependent field is also used as a controller in other dependencies, you must first remove the dependencies on that field before deleting it.

If you want to keep a dependent field but do not want its behavior, you can disable it instead. For details, see "Enabling and Disabling Field Dependency Behavior" on page 168.

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list, click the name of the object type you want to modify.
3. On the **Field Dependencies** tab:
   a. Select the check box next to the dependent field you want to delete. If wanted, you can select multiple boxes.
   b. When finished, click **Delete**.
   c. If prompted, click **OK**.

      The selected dependent field is removed from the list on the **Field Dependencies** tab.

Configuring Dependent Picklists

You can configure a list of items (drop-down or list box) so that the items in the list are filtered based upon some value selected by a user in another list. The filtering of lists can be used to help guide users in the selection of relevant values from lists during the creation or editing of an object.

Example

Let's say that both the 'Category' and 'Subcategory' fields of a Risk object (SOXRisk) have many items in their respective lists from which a user can choose, and you want only the values of 'Theft and Fraud' and 'Security Systems' to be displayed in the Subcategory list when a user selects 'External Fraud' from the Category list.

To filter the list, you would map the 'Subcategory' values of 'Theft and Fraud' and 'Security Systems' to the 'Category' value of 'External Fraud'.

The 'Subcategory' field with its selected values is considered the *dependent picklist* as the behavior of this list depends upon the value selected in the 'Category' field or *controller picklist*.

Adding Dependent Picklists

When you create a dependent picklist, you map one or more dependent field list values to one or more controlling field list values.

Note: Dependent picklist behavior is not supported for custom forms.

Figure 10 shows a partial Picklist Mapping grid for the 'Category' and 'Subcategory' drop-down lists - both are Risk object (SOXRisk) type fields.

Each column represents a value in the controlling picklist ('Category' in this example), and each row represents a value in the dependent picklist ('Subcategory' in this example).

In Figure 10, the 'Subcategory' values of 'Unauthorised Activity' and 'Theft and Fraud' are selected for the 'Internal Fraud' value, and 'Theft and Fraud' and 'System Security' are selected for the 'External Fraud' value. If a user selects 'Internal Fraud' as the category, only the 'Unauthorised Activity' and 'Theft and Fraud' values will be displayed on the Subcategory list. Similarly, if a user selects 'External Fraud' as the 'Category', only the 'Theft and Fraud' and 'Systems Security' values will be displayed on the Subcategory list.

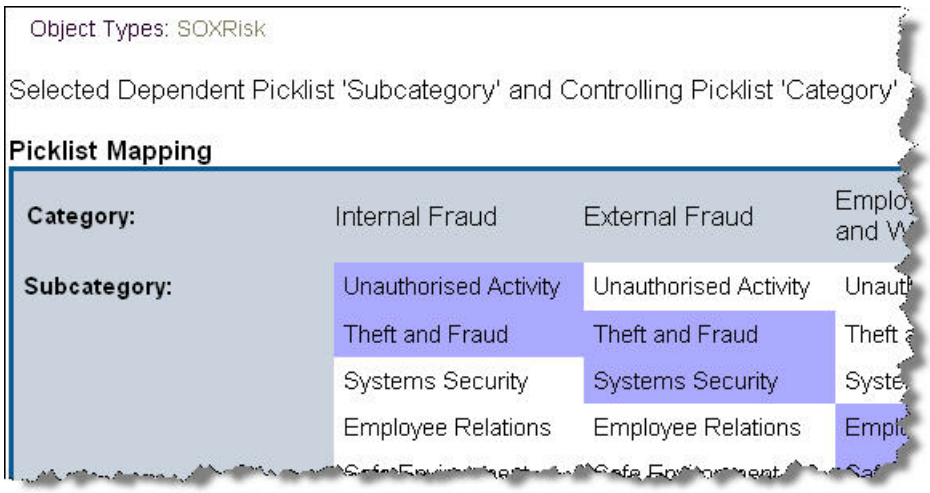


Figure 10. Sample Picklist Mapping Grid

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list, click the name of the object type you want to modify.
3. On the **Dependent Picklists** tab, click **Add**.
4. On the Add Dependent Picklist page:
   a. Click the **Select Controlling Picklist** arrow and choose a controlling field from the list.
   b. Click the **Select Dependent Picklist** arrow and choose a dependent field from the list.

5. On the Picklist Mapping page, for each controlling value in a column heading for which you want to create a filtered list, select one or more dependent field values in the corresponding column row.

   Note: To select or clear a value from a row, click the name of the value.
6. When finished, click **Finish** to save your changes.

   The newly created dependent picklists are listed on the **Dependent Picklists** tab.

Modifying Picklist Dependency Behavior

After you create a dependent picklist, you can modify the values that are displayed in the dependent picklist.

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list, click the name of the object type you want to modify.
3. On the **Dependent Picklists** tab:
   a. Select the check box next to the dependent picklist you want to modify.
   b. Click **Edit**.
4. To modify the values that are displayed in a dependent picklist by a controlling value:
   a. Navigate to the column heading with the controlling value.
   b. Click a value in the column row to either select or clear a value.
5. When finished, click **Save**.

Enabling and Disabling Picklist Dependency

Dependent picklists can be enabled or disabled. By default, dependent picklists are enabled when created.

When a dependent picklist is disabled, the following occurs:

- The dependent picklist remains in the list on the **Field Dependencies** tab, and the value in the **Enabled** column changes from 'true' to 'false'.
- The application does not enforce the conditions that control the behavior of the dependent picklist.

If you select multiple dependent picklists to enable or disable, the application switches the values accordingly. For example, if you select two dependent picklists - the first picklist is enabled with a value of 'true' and the second picklist is disabled with a value of 'false' - the value of the first dependent picklist would switch to 'false' making it disabled, and the second would switch to 'true' making it enabled.

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list, click the name of the object type you want to modify.
3. On the **Dependent Picklists** tab:
   a. Select the check box next to the dependent picklist you want to enable or disable.
   b. When finished, click **Enable/Disable**.

The value in the **Enabled** column on the **Dependent Picklists** table changes as follows for the selected dependent picklist:

- If disabled, the value changes from 'true' to 'false'
- If enabled, the value changes from 'false' to 'true'

Deleting a Dependent Picklist

When you delete a dependent picklist, it is permanently removed from the list on the **Dependent Picklists** tab and cannot be restored.

Note: If you want to keep a dependent picklist but do not want its behavior, you can disable it instead. For details, see "Enabling and Disabling Picklist Dependency" on page 171.

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list, click the name of the object type you want to modify.
3. On the **Dependent Picklists** tab:
   a. Select the check box next to the dependent picklist you want to delete. If wanted, you can select multiple boxes.
   b. When finished, click **Delete**.
   c. If prompted, click **OK**.

   The selected dependent picklist is removed from the list on the **Dependent Picklists** tab.

Excluding Fields from a Subsystem

The OpenPages product contains multiple subsystems or components that comprise a larger software system. These subsystems (for example, Workflow and Reporting Framework), typically use field definitions. In some situations, a field that is applicable to one subsystem may not be applicable to another.

Example

Let's say you want to streamline the number of fields that are used for generating Test (`SOXTest`) object reports. You are not required, for example, to produce a report on 'Testing Steps' a field that is part of the Text object. You could exclude the 'Testing Steps' field from the Reporting Framework subsystem. When you regenerate the reporting framework, the Framework Generator will ignore the 'Testing Steps' field and will be excluded from the generated framework.

Adding Fields for Exclusion

When you exclude a field from a subsystem, the subsystem ignores the excluded field.

If fields are excluded from this subsystem...	**Then...**
Reporting Framework	Any CommandCenter reports (existing or future) that reference these fields will fail unless the excluded field is also removed from the report.

If fields are excluded from this subsystem...	Then...
Workflow	Existing job type templates that reference these fields will continue to work as is (the excluded field will continued to be present in the UDA map). To remove the excluded field from a job type template, you need to refresh the UDA map as follows: • Open the existing job type in edit mode. • Click **Save**. This will result in an automatic refresh of the UDA map.

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list, click the name of the object type you want to modify.
3. On the **Field Exclusions** tab for the selected object type, click **Exclude**.
4. On the Exclude Fields page:
   a. In the **Select Field** box, select one or more fields from the list. The fields you select will be excluded from the subsystem.

      Note: To select multiple values from the list, press and hold the **Ctrl** key while clicking the mouse pointer.
   b. In the **Select Subsystem** box, select one or more subsystems from the list.
5. When finished, click **Exclude**.

   The newly excluded fields are listed on the **Field Exclusions** tab.
6. To exclude fields from a different object type, repeat Steps 1 - 4.
7. If you excluded fields from the Reporting Framework subsystem, update the reporting framework to propagate the changes to CommandCenter. For details, see "Updating the Reporting Framework" on page 64.

Changing the Subsystem for an Excluded Field

If wanted, you can change the subsystem for individual fields that have been excluded from a subsystem.

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. Select the name of the object type you want to modify.
3. On the **Field Exclusions** tab:
   a. Select the check box next to the excluded field you want to modify.
   b. Click **Edit**.
4. In the **Select Subsystem** box, modify the subsystem as wanted.
5. When finished, click **Save**.

Deleting Excluded Fields

When you delete an excluded field, it is permanently removed from the list on the **Field Exclusions** tab and cannot be restored.

Procedure

1. Access the Object Types page (see "Accessing Object Types" on page 145).
2. From the list, click the name of the object type you want to modify.
3. On the **Field Exclusions** tab:
   a. Select the check box next to the excluded field you want to delete. If wanted, you can select multiple boxes.
   b. When finished, click **Delete**.
   c. If prompted, click **OK**.

      The selected excluded field is removed from the list on the **Field Exclusions** tab.
4. If you deleted fields that were excluded from the Reporting Framework subsystem, update the reporting framework to propagate the changes to CommandCenter. For details, see "Updating the Reporting Framework" on page 64.

Chapter 9. Managing Profiles

This chapter contains the following topics:

About Profiles

Profiles provide end users with a localized view of information that is directly related to their responsibilities. You can use profiles to configure the use of objects, custom forms, fields, and object views throughout the IBM OpenPages application. When you change a setting in a profile, the change is dynamic and the effect of the change is immediate.

You can restrict individual users to view a specific set of object types and the fields in each object that are visible to them. If an object type is absent from a profile, that object type is hidden from users of that profile.

You create new profiles by cloning them from existing profiles, then modifying the new profile as desired. OpenPages supplies a standard profile, called 'Default', that you can use as a template for creating other profiles. The profiles that you create and assign to users are standalone, that is, there is no inheritance from one profile to any other profile, including the 'Default' profile.

Each user can have one and only one profile actively in use for a given logon session. You can change a user's profile during that user's logon session.

You can also designate any profile as the:

- Default profile (see "About the Default Profile" on page 177)
- Fallback profile (see "About the Fallback Profile" on page 177)

Important:

- If you assign a user to a different profile, the change becomes effective *immediately* with no action required on the part of the user.
- You should not create or edit profiles while the Framework Model is being generated.

You can associate available objects with any profile and disassociate them later. However, each profile contains a group of required objects that you cannot disassociate from the profile. The following table lists these required object types.

Table 30. Required Object Types

Object Type	Label
SOXBusEntity	Business Entity
SOXSignature	Signature

Table 30. Required Object Types (continued)

Object Type	Label
SOXDocument	File
SOXExternalDocument	Link (this is an external URL link)

Accessing Profiles

Note: To access the **Profiles** menu item, you must have the **Profiles** application permission set on your account (for details, see "Configuring Application Permissions" on page 18).

Procedure

1. Log on to the IBM OpenPages application as a user with the **Profiles** application permission set.
2. From the menu bar, select **Administration** and click **Profiles**.
3. To display the detail page of a profile, click the name of the profile you want from the list.

Results

From the detail page of a profile, you can modify profile information, associate users, groups, and reports, access the detail page of an object type where you can configure views and the display order of fields for the selected object type, and so forth.

Creating and Managing Profiles

This section describes how to work with profiles.

Creating a New Profile

You can create a new profile based on any existing profile, including the OpenPages supplied 'Default' profile. After you create the new profile you can modify it the same way you modify existing profiles.

Procedure

1. Access the Profiles page (see "Accessing Profiles").
2. On the **Profiles** table, click **Add**.
3. On the Add Profile page:
   a. In the **Name** box, type a name for the new profile.
   b. In the **Description** box, optionally type a brief description of this new profile.
4. Click the **Based on Profile** arrow and select the profile that you want to use as a template for the new profile.
5. If you want the new profile to be the Default Profile, select the **Default** box (see "About the Default Profile" on page 177).

   Important: Creating a new Default Profile may affect the way in which the IBM OpenPages application handles objects and profiles.
6. If you want the new profile to be the Fallback Profile, select the **Fallback** box (see "About the Fallback Profile" on page 177).

7. Click **Create** to create the new profile.
8. To configure the profile, do any of the following:

If you want to do this...	Then see this topic for details...
associate users	"Setting Up Users or Groups with a Profile" on page 179
configure object types	"Configuring Object Types in Profiles" on page 179
set up a Home page	"About the Home Page" on page 183
configure views for an object type	"About Object Type Views" on page 194

Designating a Default or Fallback Profile

The IBM OpenPages application uses the Default Profile as the initial profile attribute setting unless a profile is already set for the user being edited.

About the Default Profile

There can only be one profile designated as the Default profile, and you can designate any profile as the Default profile. Any previously designated profile loses this default designation when another profile is selected as the Default profile.

When you create new users and add new (clone) profiles, the Default profile serves as the profile that will be used if no other profile is selected. If no profile is specifically designated as the Default profile, the supplied OpenPages 'Default' profile is used.

Note: In an application upgrade, the Default profile includes all the object properties of the previous version of the application. All profiles are standalone; there is no inheritance from the Default profile.

About the Fallback Profile

You can designate any profile as the Fallback profile.

The Fallback profile allows a user who is either not associated with any profile, or whose profile has been disabled or deleted, to log on to the IBM OpenPages application. If no Fallback profile is defined, these users cannot log on.

The Fallback profile is optional. There can only be one Fallback profile. If you choose to designate a profile as the Fallback profile, the existing Fallback profile (if there is one) loses this designation.

Setting a Default or Fallback Profile

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. On the **Profile Information** table, click **Edit**.
4. On the Edit Profile page:
   a. Select one of the following options:
      - **Default -** to make this profile the Default profile
      - **Fallback** - to make this profile the Fallback profile
   b. Optionally, enter or change the description of the profile.
   c. When finished, click **Save**.

Editing a Profile

You can modify the description of a profile or designate the profile as the Default Profile or Fallback profile.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. On the **Profile Information** table, click **Edit**.
4. Make your edits.
5. When finished, click **Save**.

Deleting a Profile

Important: If you delete a profile it *immediately* disappears from the system and is not available to either currently logged in users or to users who subsequently log in. You cannot retrieve it. If you are not sure if you will need the profile again, disable it instead. See also "About the Fallback Profile" on page 177.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. Select the box next to each profile you want to delete.
3. On the **Profiles** table, click **Delete**.
4. At the confirmation prompt, click **OK** to delete the profile.

Disabling or Enabling a Profile

Disabling a Profile

When you disable a profile:

- The profile remains in the system (it is not deleted), and the status of the profile changes from 'Active' to 'Inactive'.
- It immediately becomes unavailable to users who are assigned that profile - either currently logged on users or to users who subsequently log on.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. On the **Profile Information** table, click **Disable**.

   The 'Disable' button changes to 'Enable'.

Enabling a Profile

When you enable a profile:

- The status of the profile changes from 'Inactive' to 'Active'.
- It immediately becomes available to users who are assigned that profile - either currently logged on users or to users who subsequently log on.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. On the **Profile Information** table, click **Enable**.

   The 'Enable' button changes to 'Disable'

Setting Up Users or Groups with a Profile

A specific profile can be associate with one or more users or groups. However, a user can be associated with zero or one profile. When you associate a profile with a user, the object types in that profile are available to that user. Additionally, you can select the fields within each object type that users of this profile can view.

Associating Users and Groups to a Profile

Table 31 highlights the results of associating users and groups to a profile.

Table 31. Associating Users and Groups

If you select a...	Then this occurs...
user who has no profile	the currently selected profile is assigned to that user.
user who already has a profile assigned	the former profile setting is overwritten with the new setting when you associate the user to the selected profile.
group	all the members of that group are selected and each member is individually assigned the selected profile and listed on the **Associated Users** tab.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. On the **Associated Users** table, click **Associate**.
4. In the **Associate users/groups with profile** box:
   a. Select the users or user groups you want to associate with the profile. You can view individual users within a group by clicking the + box to the left of the group.
   b. When finished, click **Associate**.

Disassociating Users or Groups from a Profile

When you disassociate a user from a profile, that profile becomes immediately unavailable to that user. If no Fallback profile has been assigned to the user, the user will not be able to log on to the application.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. From the **Associated Users** table listing:
   a. Select the box next to each user you want to disassociate from this profile.
   b. Click **Disassociate**.
   c. At the prompt, click **OK**.

Configuring Object Types in Profiles

You can include or exclude certain object types from individual profiles. When you exclude an object type from a profile, it is not visible to any user associated with that profile. There is no provision for including or excluding an object type from all profiles simultaneously.

Note: Certain object types are required. You get an error message if you try to exclude them.

Including Object Types in a Profile

When you include an object type in a profile, that object type is immediately visible to users who are assigned the selected profile.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. On the **Object Types** table, click **Include**.
4. On the Available Object Types page:
   a. Select the box next to each object type you want to include in this profile.
   b. When finished, click **Include**.
5. To configure views for an object type, see "About Object Type Views" on page 194.

Results

The selected object types appear on the list of object types.

Excluding Object Types From a Profile

When you exclude an object type from a profile, that object type is removed from the views in which it is used and is no longer available to users who are assigned that profile.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. From the **Object Types** table:
   a. Select the box next to each object type that you want to exclude from the profile.
   b. Click **Exclude**.
   c. At the prompt, click **OK** to remove the object type from view.

Results

The selected object type is removed from the list of object types for this profile. The IBM OpenPages application stores an excluded object, along with any associated data, in the repository. You can view it through reports.

Configuring Fields for Object Types

The availability of a field for configuration within any view depends on whether or not that field is included or excluded in the object type for that profile.

Including and Excluding Fields in an Object Type

Note: Including or excluding fields for object types in one profile does not affect object-type fields in other profiles.

Including Fields in an Object Type

Including object fields for an object type in a profile makes those object fields available for selection within the various views.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. From the **Object Types** table listing, click the name of the object type whose fields you want to modify (for example, SOXIssue).
4. On the **Object Fields** table, click **Include**.
5. On the Available Object Fields page:
   a. Select the box next to the name of each object field you want to include.
   b. When finished, click **Include**.

      The included object field now appears in the list of available fields for this object type in this profile.
6. If wanted, configure the object field in a view. Depending on the view, see either "Configuring Navigational and Association Views" on page 203 or "About Configuring Fields in Detail and Activity Views" on page 215.

Excluding Fields From an Object Type

Excluding an object field from an object type in a profile immediately removes that object field from the views in which it is used, and that field is no longer available for configuration in a view or to users who are assigned that profile.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. From the **Object Types** table listing, click the name of the object type whose fields you want to modify (for example, SOXIssue).
4. From the **Object Fields** table:
   a. Select the box next to the name of each object field you want to exclude.
   b. Click **Exclude**.
   c. At the confirmation prompt, click **OK** to remove the fields from the selected object type.

Results

The excluded object fields are now absent from the list of available fields for this object type in this profile.

Setting the Global Display Order of Object Types

With the exception of the Business Entity object type, you can modify the order in which object types are globally displayed in a profile. When you change the number of the list order of an object type, the system dynamically updates all the object types (except Business Entity).

Example

Let's suppose that the current display order for the following object types is: Business Entity 1, Process 2, Sub-Process 3, and Account 4.

However, you want to globally display Account (instead of Process and Sub-Process) after Business Entity, you could set the order number of Account to 2. When you click 'Update Order', the system automatically re-orders the Process number to 3 and Sub-Process to 4.

Now, wherever these object types are found together in the application, they would appear in the following order: Business Entity 1, Account 2, Process 3, and Sub-Process 4.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. From the **Object Types** table:
   a. In the box under the **Order** column, change the order value of the object types as wanted.

      Note: The maximum value allowed in the Order field is 999.
   b. When finished, click **Update Order**.

      The object types in this profile now appear in the new order.

Setting a Field in a Profile to Required or Optional

You can set a specific field to required or optional for a particular profile and object type by following the instructions in this section. Setting a field to required in a profile affects only the users who are assigned that profile.

Note: If a field is not listed in the **Object Fields** table, you must include it before you can modify it (see "Including Fields in an Object Type" on page 181).

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. In the **Object Types** table for the selected profile, click the name of the object type that has the field you want to modify.
4. In the **Object Fields** table, click the name of the field you want to modify (for example, 'Description').
5. On the **Object Field Information** table for the selected field, click **Edit**.
6. In the **Required** box on the edit page, do one the following:
   - Select the box if you want the field to be required.
   - Clear the box if you want the field to be optional.
7. When finished, click **Save**.

Chapter 10. Managing the Home Page and Object Views

This chapter contains the following topics:

About the Home Page

The Home page is the initial page that users see when they log on to the OpenPages application.

The Home page supports a tabbed interface for displaying selected reports and information. For each profile, you can configure one or more tabs to personalize the information on the page for users who are assigned that profile.

Typically, the number and types of tabs you configure on a Home page will vary by profile and depends on the particular business needs of users. If the number of tabs on a Home page extend beyond the size of the current browser window, right and left arrows are automatically displayed so users can scroll horizontally through the tabs.

Except for the Classic tab, a tab on a Home page displays the name of the configured report or dashboard.

The type of tabs that can be configured on the Home page include:

- CommandCenter reports
- Go! Dashboard reports
- JSP Reports
- The Classic tab, a default Home page tab provided by IBM OpenPages , Inc., that contains configured panes (sections of a page) for predefined lists, filtered lists, and embedded reports.

You can control the order in which tabs (including the Classic tab) are displayed on the Home page.

Example

A 'Testers' profile might have the following tabs configured: 'My Tests - Performer' (report) as tab 1, the Classic tab as tab 2, 'Test Notifications' (report) as tab 3, and the 'FCM Dashboard' (report) as tab 4.

Additionally, you can hide, show, add, or delete tabs from the Home page quickly and easily without interruption to users who are assigned that particular profile.

Note:

- In a first-time installation, by default, the Classic tab is enabled.
- A report (or report fragment) that is embedded in a tab on the Home page executes when a user:
  - First clicks the tab containing the report
  - Navigates away from the Home page to other menus and then returns to that report tab on the Home page
  - Logs off and then logs on to the application again
- Switching between multiple tabs on the Home page and then returning to the original report tab does not rerun the report. To refresh report data, you must click the Refresh button on the report tab.
- If the Classic tab is empty of content (no panes are configured) but other tabs are configured for display on the Home page, then a message, similar to the following, is displayed on the Classic tab to users who are assigned that profile:

  ```
  OP-50544: There is no information configured for display on this Home
  page tab. Please contact your System Administrator.
  ```

- If the Classic tab is empty of content (no panes are configured) and no other tabs are configured for display on the Home page, then a message, similar to the following, is displayed on the Home page to users who are assigned that profile:

  ```
  OP-50536: There is no information configured for display on your home
  page. Please contact your System Administrator.
  ```

About the Layout of Tabs on a Home Page

The number of tabs displayed on a Home Page for a given profile has no set limit and will vary according to your users business needs. Figure 11 shows the basic layout of tabs on a Home page.

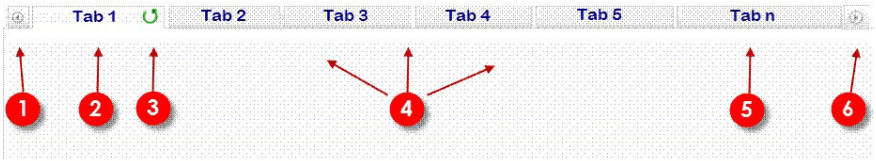


Figure 11. Layout of Tabs on a Home Page

Table 32 contains a key to the above illustration with a brief description of the various Home page elements.

Table 32. Description of Home Page Elements

Key	Description
1	Left horizontal scroll arrow. If the number of tabs that are configured for a Home page do not fit in the browser window, an arrow is automatically displayed so users can scroll horizontally through the tabs.
2	Active tab. When multiple tabs are configured, only the currently selected tab is highlighted and becomes the active tab.
3	Refresh button. When clicked, refreshes the data on the selected tab.

Table 32. Description of Home Page Elements (continued)

Key	Description
4	Inactive tabs. Except for the Classic tab, a tab typically displays the name of the configured report or dashboard.
5	'n' represents a number. There is no limit to the number of tabs that can be configured on a Home page.
6	Right horizontal scroll arrow. If the number of tabs that are configured for a Home page do not fit in the browser window, an arrow is automatically displayed so users can scroll horizontally through the tabs.

Guidelines for Selecting Reports to Run in Tabs

To avoid performance issues and cluttering the Home page with too many tabbed reports, consideration should be given to determining:

- Which reports or dashboards are best related to the type of tasks or activities a particular group of users have to accomplish
- Which profile (or profiles) should contain these reports or dashboards
- If any of the selected reports or dashboards already configured for display on the Classic tab. If so, should these be removed?

Configuring Tabs on the Home Page

To configure tabs on the Home page, you use the **Home Page Tab Configuration** table on the detail page of the selected profile.

Table 33 describes the type of information displayed on the Home Page Tab Configuration Table.

Table 33. Columns on the Home Page Tab Configuration Table

This column...	Displays this...
Name	The name of each configured tab. Typically, the name reflects the name of the selected report or dashboard. 'Classic' is the default Home page tab provided by IBM OpenPages , Inc. and is always displayed in the list.
Description	A brief description of the report, if available.
Status	The status of the tab. If the status is: • Visible - the tab is displayed on the Home page • Hidden - the tab is hidden from the Home page
Order	The position of the tab as it is displayed on the Home page. By default, the Classic tab is in position 1. **Note:** Tabs that are disabled or hidden cannot be ordered and the box is not displayed.
Actions	The type of actions that can be used on a tab. The actions are: • Hide - hides the tab from display on the Home page • Show - unhides the tab and displays it on the Home page • Delete - permanently removes the tab from the list and Home page. **Note:** The Classic tab cannot be deleted.

For information on localizing display text, see “Localizing Application Text” on page 238.

Adding New Tabs for Reports or Dashboards

Note: For details about configuring the Classic tab, see “Configuring the Classic Tab” on page 187.

When you select one or more reports or dashboards for display in a tabbed format on the Home page, each selected report or dashboard is immediately:

- Displayed in a tab on the Home page of users who are assigned that profile.
- Listed under the **Home Page Tab Configuration** table on the Profile detail page.

Procedure

1. Access the Profiles page (see “Accessing Profiles” on page 176).
2. From the list, click the name of a profile to open its detail page.
3. On the **Home Page Tab Configuration** table, click **Add**.
4. From the list of reports and/or dashboards:
   a. Expand a report folder to display a list of available reports.
   b. Select the check box next to each report you want displayed in a tab on the Home page.

      Note: Selecting multiple reports results in multiple tabs (one tab for each selected report).
   c. When finished, click **Associate**.
5. If wanted, change the order in which tabs are displayed on the Home page (see “Setting the Display Order of Tabs”).

Setting the Display Order of Tabs

By default, the Classic tab is in position 1 on the Home page, and each tabbed report or dashboard that you add is displayed in the order in which it was added.

If wanted, you can change the order in which tabs (including the Classic tab) are displayed on the Home page. When you change the position of tabs on a Home page, the change is immediately reflected in the application user interface.

Procedure

1. Access the Profiles page (see “Accessing Profiles” on page 176).
2. From the list, click the name of a profile to open its detail page.
3. On the **Home Page Tab Configuration** table, under the **Order** column, type over the existing number with the new number you want for positioning each tab on the Home page.
4. When finished, click **Update Order**.

Hiding and Unhiding Tabs

You can control whether or not configured tabs are displayed or hidden from users in a profile. A tab that is disabled is hidden from users with the selected profile and can be unhidden by enabling it at a future time.

By default, newly added tabs are enabled and displayed to users who have the selected profile.

When you hide or unhide a tab, the following occurs:

- The value of the Status column changes for that tab.
- The value of the link toggles between **Hide** and **Show** depending on the selection.
- The tab is immediately hidden or unhidden from users on the Home page of the selected profile.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. On the **Home Page Tab Configuration** table, under the **Actions** column do one of the following:

To do this...	Click this link...
Hide a tab on the Home page for users of the selected profile	**Hide** in the row of the tab you want to hide.
Show a previously hidden tab	**Show** in the row of the tab you want to unhide.

Deleting Tabs

When you delete a tab for a report or dashboard from a profile, the tab is immediately removed from the Home page of that profile, and from the list of tabs on the **Home Page Tab Configuration** table.

Note: You cannot delete the Classic tab from the **Home Page Tab Configuration** table; you can only hide it.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. On the **Home Page Tab Configuration** table, under the **Actions** column, click the **Delete** link for the tab you want to permanently remove.

Configuring the Classic Tab

The Classic tab is a default tab provided by IBM OpenPages , and contains the following panes (sections of a page) that can be configured in a profile for display to users:

- Predefined Lists - these panes display a list of predefined items that are tailored to the logged on user, such as My Checked-Out Files or My Tasks. Predefined lists also includes the My Reports pane, which can be configured with links to reports. For details, see "Configuring Predefined Lists" on page 188.
- Filtered Lists - these panes display a list of items based on a filter that you define for the selected object type. In addition, you can select object and/or report fragment fields (the data is displayed in columns), and set the order in which columns are displayed in the pane. For details, see "About Filtered Lists on the Classic Tab" on page 188.
- Embedded Reports - each embedded report is displayed in a separate pane on the Classic tab. For details, see "About Configuring Reports" on page 191.

Note: The Classic tab can be enabled or disabled for a profile but cannot be deleted.

In a first-time installation, the Classic tab, by default, is enabled but empty of content (no panes are configured), and a message, similar to the following, is displayed to users who are assigned that profile:

```
OP-50536: There is no information configured for display on your home page.
Please contact your System Administrator.
```

Configuring Predefined Lists

Table 34 lists the predefined lists that are available for display on the Classic tab.

Table 34. Available Predefined Lists

This predefined list...	Displays this on the Home page...
My Tasks	a **My Tasks** pane that includes a list of tasks assigned to the logged on user. The table includes such information as the status, name, and description of the task, and any attachments associated with each task.
My Checked-Out Files	a My Checked-Out Files pane that includes a list of files that were checked out by the logged on user.
My Jobs	a My Jobs pane that includes any jobs owned by the logged on user. The table includes such information as the name and description of the job, and attachments associated with each job.
Report Listing	a My Reports pane on the Home page for which you can configure links to reports. For embedded reports, see "Working With Embedded Reports" on page 192 for details.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. On the **Classic Tab Configuration** table, click **Add Predefined Lists**.
4. On the Available Predefined Lists page:
   a. Select the box next to each predefined list you want to display on the Classic tab.
   b. When finished, click **Include**. The included items are listed in the **Classic Tab Configuration** table.
5. If you selected 'Report Listing' and want to populate the My Reports pane with a list of links to reports, see "Configuring a My Reports Listing" on page 191 for details.

About Filtered Lists on the Classic Tab

Filtered lists contain selected object type information based on the filter you defined for that object type.

Each filtered list that you configure is displayed in a table format within a pane on the Classic tab. For example, if you configured three filtered lists for the Classic tab, that tab would contain three separate panes - one for each filtered list.

Filtered lists can include one or more:

- Object fields

- Report fragment fields

Each field that you include in a filtered list is displayed as a column in that table.

Example

If you defined a filtered list for ineffective controls, and included (in addition to 'Name' and 'Description') an object field for 'Classification' and a report fragment field containing a 'Control Analysis bar chart', the table would display four columns (one for each field).

Note: By default, filtered lists on the Classic tab:

- Automatically include the 'Name' and 'Description' object fields.
- Use 'Reports' as the name of the column heading for report fragment fields, and a clickable icon is displayed under the column for opening a single report fragment field. If multiple report fragment fields are configured for an object type, the icon displays a clickable down arrow with a selection list.
- Support only one column layout per object type. When multiple filtered lists are configured for the same object type, you cannot define different columns for display per filtered list on the Classic tab.

  Example

  The Risk object type has filtered lists 'A', 'B', and 'C' configured for display on the Classic tab. If the 'Name' and 'Description' fields were defined for filtered lists 'A' and 'B', and an additional field, 'Domain', was the last field defined for filtered list 'C', then all the filtered lists, including 'A' and 'B' would include 'Domain' for display on the Classic tab.

For each filtered list that you configure on the Classic tab for an object type, you can include or exclude fields, and set the order of columns in the table. If report fragment fields are configured, these are always the last column of the table.

When you configure a filtered list for display on the Classic tab, all filters that are defined for an object type are displayed in a selection list. Once you select a filter, it no longer appears in the list of available filters.

The Classic tab supports only one column layout per object type. When multiple filtered lists are configured for the same object type, you cannot define different columns for display per filtered list on the Classic tab.

Example

The Risk object type has filtered lists 'A', 'B', and 'C' configured for display on the Classic tab. If the 'Name' and 'Description' fields were defined for filtered lists 'A' and 'B', and an additional field, 'Domain', was the last field defined for filtered list 'C', then all the filtered lists, including 'A' and 'B' would include 'Domain' for display on the Classic tab.

Before You Begin

Before you can configure a filtered list, you must have the following already defined for an object type:

- One or more filters for the selected object type. See "Managing Filters for an Object Type" on page 157.

- Any report fragment fields and/or object fields that are in addition to the predefined standard IBM OpenPages object fields for that object type. See Chapter 7, “Configuring Fields and Field Groups,” on page 103.

Configuring Filtered Lists on the Classic Tab

To configure filtered lists on the Classic tab for object fields and/or report fragment fields, do the following.

Note:

- A clickable icon is displayed for opening a single report fragment field under the ‘Reports’ column. If multiple report fragment fields are configured for an object type, the icon displays a clickable down arrow with a selection list.
- If report fragment fields are configured, the ‘Reports’ column, by default, is always the last table column and its column position cannot be changed.

Procedure

1. Access the Profiles page (see “Accessing Profiles” on page 176).
2. From the list, click the name of a profile to open its detail page.
3. On the **Classic Tab Configuration** table, click **Configure Filtered List**.
4. On the Select a Filter page:
   a. Select a filter from the list.
   b. Click **Next**.
5. On the Select Fields page, do any of the following:

Table 35. Summary of Filter Actions

If you want to do this...	Then...
Include a field as a column in the filtered list	On either the **Included Object Fields** or **Included Reporting Fragment Fields** table: 1. Click **Include**. This opens a field selection page. 2. Select the box next to each field you want to display as a column. 3. When finished, click **Include**.
Exclude a field as a column	On the **Included Object Fields** or **Included Reporting Fragment Fields** table: 1. Select the box next to each field you want to remove as either a column or report. 2. Click **Exclude**. 3. At the confirmation prompt, click **OK**.
Change the order in which object fields are displayed as columns	On the **Included Object Fields** table: 1. In the **Order** column, change the order number of the field you want. 2. Click **Update Order**. When you change the number of a field, the system dynamically updates all the other numbers.
Include a field as a column that displays a report fragment	On the **Include Reporting Fragment Fields** table: 1. Click **Include**. This opens a field selection page. 2. Select the box next to each report fragment field that you want to display. 3. When finished, click **Include**.

6. When finished, click **Finish**.

Editing Filtered Lists on the Classic Tab

You can modify the fields in a filtered list and the order in which they are displayed.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. On the **Classic Tab Configuration** table, click the name of the filtered list table you want to modify.
4. On the table for included objects or report fragment fields, modify the information as necessary (for details, refer to Step 5 in "Configuring Filtered Lists on the Classic Tab" on page 190).
5. When finished, click **Finish**.

About Configuring Reports

You can use the following methods to configure reports on the Classic tab:

- **Report Listing** - this method creates a **My Reports** pane in which a list of selected reports can be displayed. Each listed report name is a link that, when clicked, opens the report in a separate window. For details, see "Configuring a My Reports Listing."
- **Embedded reports** - this method embeds each specified report in a separate pane on the Classic tab. For details, see "Working With Embedded Reports" on page 192.

Note:

- Only published CommandCenter reports are displayed in the list of available reports (under the CommandCenter folder) for association on a Classic tab (either as a link in a list or as an embedded report). If you want to add a new CommandCenter report, you must first publish that report. For details, see "About Adding CommandCenter Reports" on page 86.
- Although JSP reports are available for selection as embedded reports on the Classic tab, only CommandCenter reports can be embedded (JSP reports cannot be embedded) on the Classic tab. A JSP report that is selected as an embedded report will result in a reporting error on the Classic tab.

Configuring a My Reports Listing

You can configure links to reports in the My Reports pane on the Classic tab by either clicking the 'Add Predefined List' button or through the wizard by clicking the 'Configure Reports' button.

You can globally control the maximum number of reports that are listed on the Classic tab through the **Maximum Reports Listing** setting (for details, see "Setting the Number of Report Listings" on page 307).

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. On the **Classic Tab Configuration** table, do one of the following:

Click this button...	Then...
Add Predefined Lists	On the Available Predefined Lists page: 1. Select the box next to **Report Listing**. 2. Click **Include**. 3. On the **Classic Tab Configuration** table, click the **Report Listing** link. 4. Continue to Step 4. **Note:** If you already added a My Reports pane on the Classic tab but need to populate the list with reports, do not click the button and skip directly to Step c.
Configure Reports	In the Configure Home Page Reports wizard: 1. In the **Select Report Type** step, select **Report Listing** as the report type. 2. Click **Next**. 3. Continue to Step 4.

4. Click **Associate** to open the Reports list page.
5. On the **Reports** list page:
   a. Select the box next to each report you want to include as a link in the My Reports pane.
   b. When finished, click **Associate**.
6. Click **Finish**.

Working With Embedded Reports

When you embed a report on the Classic tab, the report is displayed in a pane on the Classic tab of users who have the selected profile.

You can globally control the maximum number of embedded reports to show on the Classic tab through the **Maximum Embedded Reports** setting (for details, see "Defining the Number of Embedded Reports" on page 307).

Performance Considerations: Although embedded Classic tab reports provide a convenient mechanism to present users with useful CommandCenter report data upon logon to the IBM OpenPages application, report execution times can vary depending on the report.

When configuring embedded reports, administrators should be careful not to configure the Classic tab with large or resource-intensive reports, as this will contribute to the overall load on CommandCenter resources. Some factors that can affect utilization of CommandCenter system resources include:

- The number of concurrent users logged on to the system
- The percentage of users executing reports or viewing computed fields
- The frequency with which users return to their respective Home pages

The following are some guidelines for configuring reports on the Classic tab:

- Only embed reports that are well-scoped and execute in less than <10 seconds for the typical application user.
- Configure no more than one (1) embedded report on the Classic tab for the majority of application users.

Configuring Embedded Reports:

Use the following steps to embed one or more reports on the Classic tab.

Note: You may need to modify the report to accommodate differences in the Classic tab display area and page targets. We recommend that you make a copy of the desired report before you update the display details and targets to suit rendering within the Classic tab display area.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. On the **Classic Tab Configuration** table, click **Configure Reports**.
4. In the Configure Home Page Reports wizard:
   a. In the **Select Report Type** step, select **Embedded Reports** as the report type.
   b. Click **Next**.
5. On the **Choose Reports** step, click **Associate** to add reports to the list.
6. On the **Reports** page:
   a. Select the box next to each report you want to embed in a pane on the Classic tab.
   b. When finished, click **Associate** (you may need to scroll to the bottom of the page to see the button).

      The selected reports are listed in the Associated Embedded Reports pane of the wizard.
7. If you want to remove any of the newly associated reports from the list (for example, a report was accidentally added), you can:
   a. Select the box next to each report you want to remove.
   b. When finished, click **Disassociate**
8. To exit the wizard, click **Finish**.

Modifying Configured Reports

You can use the Configure Reports wizard to add or remove reports (both embedded reports and My Report links) from the Classic tab.

Note: You can also remove embedded reports directly from the **Classic Tab Configuration** table (without using the wizard). For details, see "Removing Items From the Classic Tab" on page 194.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. On the **Classic Tab Configuration** table, click **Configure Reports** to open the wizard.
4. In the **Select Report Type** step, select the report type you want to modify.
5. On the Associated Reports page:

To do this...	Then click this button...
add more reports	1. Click **Associate**. 2. On the **Reports** list page, select the box next to each report you want to include. 3. When finished, click **Associate**.
remove existing reports	1. Select the box next to each report you want to remove. 2. When finished, click **Disassociate**.

6. Click **Finish**.

Removing Items From the Classic Tab

You can remove previously configured tables (including embedded reports) from the Classic tab. When a user with the modified profile either logs on to the application, refreshes or returns to the Classic tab on the Home page, the removed items may no longer be displayed.

Note: To remove links from the My Reports pane, see "Modifying Configured Reports" on page 193.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. On the **Classic Configuration** table listing:
   a. Select the box next to each item you want to remove from the Classic tab.
   b. When finished, click **Disassociate**.
   c. At the confirmation prompt, click **OK**.

About Object Type Views

For each object type that you include in a profile, you can configure various views of data for that object. A view displays information about an object type in hierarchical format and provides a means for customizing and filtering information on a page for objects and custom form objects.

Table 36 on page 195 provides a summary of the various standard (out-of-the-box) views that you can configure to meet your business needs. In addition, you can create your own Activity view pages for an object type in which users can edit, view, and manage multiple associated objects on the same page. Depending on the view type, information is displayed as either a page (such as a Folder View or Detail view page) or in a section of a page (such as a Context pane).

Fields that you configure for a specific object type and view page are displayed to users who have that profile, and fields that you exclude from that object type and view are hidden from users.

Fields can be object fields, computed fields, and/or report fragment fields.

When you modify an object view for a particular object type (including custom forms), the change is immediate and displays everywhere the object type appears in a table within the IBM OpenPages application. Changes that you effect for one profile do not result in changes to other profiles.

Example

Let's say you create two new fields for the Risk object type and want to display these fields to users with the 'Manager' profile on the detail page of Risk objects. You would open the 'Manager' profile, select the Risk object type from the list, select the Detail view page, and then choose the new fields to include on the Detail view page.

When users with the 'Manager' profile view, create or modify a risk, the two new fields will be displayed on a Risk Detail view page. For users who have a different profile (not 'Manager'), the new Risk fields are hidden unless you also include these fields in that profile.

The IBM OpenPages application categorizes object views as follows:

Table 36. Summary of View Types

View Type	Description
Navigational Views	
Overview	This standard view displays a hierarchical tree-view of objects on a page. For details, see "About Overview Pages" on page 196.
Folder	This standard view displays folders (including any sub-folders) on a page for the selected object type. For details, see "About Folder View and Filtered List Views" on page 196.
Filtered List	This standard view displays a page with search filter options that you can use to display objects of the same type that match your search criteria. For details, see "About Folder View and Filtered List Views" on page 196.
Association Views	
List	This standard view displays objects of the same type in a list format. For details, see "About List Views" on page 198.
Context	This standard view displays the context of an object on an object's detail page. By default, the business entity and primary association paths are displayed. For details, see "About Context Panes" on page 198.
Object Views	
Detail	This standard view displays the properties of a custom form or an object with any associations it has to other objects. For details, see "About Detail Views" on page 199.
Activity View	This view is created and configured by you and can be tailored to suit specific business needs. For details, see "About Activity Views" on page 199.

Note:

- For Filtered List, Folder, and List views:
  - The **Name** field is always displayed in column 1 and its position cannot be changed.
  - If report fragment fields are configured, the 'Reports' column is always the last column in the table and its position cannot be changed.
  - List and Detail object views are available for all objects.
  - Custom forms (such as surveys) can only have a Detail object view (no Activity View).

  - The width of the table columns in an object view cannot be modified.
- The Currency and Single File data types require additional support. For details see, "About Data Types" on page 111.

Overview of Navigational Views

Navigational Views assist users in finding instances of specific objects and include the following standard view types:

- Overview
- Folder
- Filtered List

When you add, remove, or modify Navigational Views in a profile for a specific object type, the following occurs:

- A menu item with the name of the selected object type, is dynamically added to or removed from the appropriate menu on the menu bar for users who are assigned that profile.
- Users with the assigned profile who are already logged on to the application may have to refresh the page to see the changes.

About Overview Pages

An Overview page displays a hierarchical object-tree view of an object type. For example, if you wanted to include an Overview page for Control Objectives, you could do so through a profile.

Object types that have Overview pages appear on a menu before other Navigational Views (such as a Folder or Filtered List View) of the same object type.

Example

Let's say you configure an Overview page for the Control Objective object type in addition to a Filtered List view page. The 'Control Objective Overview' menu item would appear in the 'Assessments' menu list before the 'Control Objectives' menu item.

As an administrator, you can:

- Control which object types are included or excluded in the object-tree hierarchy on an Overview page (see "Including and Excluding Object Types on Overview Pages" on page 205 for details)
- Enable or disable an Overview page for an object type (see "Managing Views for Object Types" on page 200 for details)

Note:

- By default, the Business Entity, Account, Risk Assessment, Service, Process, Mandate, and Loss Events objects have Overview pages.
- An Overview page is not supported for the following object types: SOXProject, SOXDocument, SOXExternalDocument, Report, SOXMilestone, SOXIssue, SOXTask, SOXSignature, and ProjectActionItem.

About Folder View and Filtered List Views

A **Folder View** displays a page view of folders (including sub-folders) containing the selected object type and displays the information in columns on the page.

A **Filtered List View** displays a page with search filter options. This view can be used to filter objects of the same type that match specified search criteria.

Note: For Filtered List and Folder views:

- You cannot configure a Folder or Filtered List view for the following object types: Milestones (SOXMilestone), Project Action Items (ProjectActionItem), Signatures (SOXSignature), and custom forms.
- When you configure either a Folder or Filtered List view for Business Entities (SOXBusEntity), the List view for this object type is not available.
- The **Name** field is always displayed in column 1 and its position cannot be changed.
- If report fragment fields are configured, the 'Reports' column is always the last column in the table and its position cannot be changed.

If you enable either a Folder View or Filtered List view page for an object type, only that view page is displayed when the user clicks the menu item for the selected object type. If you enable both Folder View and Filtered List view pages, then both pages, in a tabbed format, are displayed. You can also configure which view page you want displayed first to users.

Example

Let's say you previously disabled both the Folder View and Filtered List view pages for Control Objectives in a profile, and want to make that object type and its children directly accessible again through the 'Assessments' menu to users who are assigned that profile. You could enable the Folder View and/or Filtered List View for the Control Objective object type. Enabling either view page would cause the 'Control Objectives' menu item to be dynamically displayed on the 'Assessments' menu. However, only the view page that was enabled would be displayed when the menu item was selected. If you enabled both view pages, you could set, for example, the Filtered List view page to be displayed first to users.

As an administrator, you can:

- Control which fields are displayed as table column headings in a Folder or Filtered List view (see "Configuring Fields in Navigational and Association Views" on page 203)
- Set the display order of the table column headings (see "Setting the Display Order of Fields in a View" on page 202)
- Enable or disable a Folder and/or Filter List view page for an object type (see "Managing Views for Object Types" on page 200 for details)
- Control which view page (Folder or Filter List View) is displayed first to users when both views are configured (see "Setting a Default View" on page 202 for details)

Overview of Association Views

Association Views typically display a list and include the following standard view types:

- List
- Context

When you add, remove, or modify Association Views in a profile for a specific object type, users with the assigned profile who are already logged on to the application may have to refresh the page to see the changes.

About List Views

A **List View** displays objects of the same type in a table format, with objects generally listed in ascending order. Depending on the object type, List Views may be displayed as either a page or pane.

By default, List Views are displayed as pages for the following object types: Business Entities (SOXBusEntity), Milestones (SOXMilestone), and Tasks (SOXTask), and as panes on a Detail view page for listing associated parent or child objects.

Note: For List views:

- When you configure either a Folder or Filtered List view for Business Entities (SOXBusEntity), the default List view for this object type is not used.
- You cannot add a List view to a custom form object or remove a List view from an object.
- The **Name** field is always displayed in column 1 and its position cannot be changed.
- If report fragment fields are configured, the 'Reports' column is always the last column in the table and its position cannot be changed.

As an administrator, you can:

- Control which fields are displayed as table column headings in a List View (see "Configuring Fields in Navigational and Association Views" on page 203)
- Set the display order of the table column headings (see "Setting the Display Order of Fields in a View" on page 202)

About Context Panes

A **Context pane** can provide information about an object that assists a user in understanding how the object fits into the current environment.

For example, you could use a Context pane to include System Fields such as, 'Business Entity Structure' and 'Primary Association Path', or a report fragment field that displayed a line chart showing trends.

As an administrator, you can:

- Control which fields are displayed as table column headings in a Context pane (see "Configuring Fields in Navigational and Association Views" on page 203)
- Set the display order of the table column headings (see "Setting the Display Order of Fields in a View" on page 202)

Overview of Object Views

Object Views provide detail instance data for an object and include the following page view types:

- Detail
- Activity

When you add, remove, or modify Object Views in a profile for a specific object type, users with the assigned profile who are already logged on to the application may have to refresh the page to see the changes.

About Detail Views

A **Detail View** displays data on the same page for the selected object including fields and any associations it has to other objects. By default, this is the view you see when you click the linked name of an object from an Overview, Folder, Filtered List, or List view page.

From an object's Detail page, application users can edit and/or view object-specific fields for the selected object, and add or associate other objects to it.

Fields can be object fields, computed fields, and/or report fragment fields.

Note:

- The Detail view is required for objects and custom forms and can be disabled but not removed. When you add a new object type to the Default profile, a Detail view is automatically configured for that object type.
- When users export data from a Filtered List View to an Excel spreadsheet, the data that is exported directly corresponds to the fields that are configured in a Detail view for the selected object type.

As an administrator, you can:

- Control which fields are displayed in the table rows of a Detail view (see "About Configuring Fields in Detail and Activity Views" on page 215)
- Set the display order of the fields (see "Setting the Display Order of Fields in a View" on page 202)
- Set specific fields to be view only or editable (see "Setting Object Fields as Read-Only or Editable" on page 219)
- Set specific fields to span the 2-column table layout of the Detail page (see "Spanning Table Columns" on page 219)
- Insert section headings on a page to delineate a set of fields (see "Using Section Headings" on page 217)
- Configure how report fragment fields are displayed to users (see "Configuring the Display Type for Reporting Fragment Fields" on page 220)
- Configure how string data is displayed to users (see "Configuring Display Types for Simple String Fields" on page 221)

About Activity Views

Activity Views are multi-object views focused on performing a specific task, such as control assessments. An Activity View page provides a way for users to concurrently view and edit specific fields for an object, including any child objects that have been defined for this view, with minimal navigation.

An Activity View can display up to three levels of objects (the current object, list and detail panes for child objects, and objects under a selected child object).

In an Activity View, you can choose child object types at any level in the hierarchy for display in an Activity View. For example, if users need to determine the effectiveness of a particular control, you could select **Control** and **Test Result** (skipping the **Test** object) under a **Risk** object so only objects relevant to performing the task are displayed in an Activity View. You can also sort how object types are displayed and select paths to scope or limit the objects that are returned.

By default, an Activity View is enabled and is automatically added to the list of views that can be selected from the **Current View** selection arrow at the top of an object's detail page. Users who are assigned the selected profile have immediate access to the new Activity View.

For more details on using Activity Views, see "Configuring Object Views" on page 208.

As an administrator, you can:

- Create, modify, or delete Activity Views (see "Configuring Object Views" on page 208)
- Control which fields are displayed in the table rows of an Activity View (see "About Configuring Fields in Detail and Activity Views" on page 215)
- Set the display order of the table rows containing the fields (see "Setting the Display Order of Fields in a View" on page 202)
- Set specific fields to be view only or editable (see "Setting Object Fields as Read-Only or Editable" on page 219)
- Set specific fields to span the 2-column table layout of the activity page (see "Spanning Table Columns" on page 219)
- Insert section headings on a page to delineate a set of fields (see "Using Section Headings" on page 217)

Managing Views for Object Types

You can enable, disable, and set a default view for certain object types that are configured in a profile. You can also set the display order of fields in a view.

Note: For information about configuring specific object types in a profile, see "Configuring Object Types in Profiles" on page 179.

Enabling a View

The process of enabling a view for an object type in a profile is the same for Navigational and Object Views. It does not apply to Association Views.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. From the **Object Types** table listing, click the name of the object type (for example, SOXControl) for which you want to enable a view.
4. Navigate to the type of view you want (such as **Navigational Views** or **Object Views**).
5. Click the **Enable** link under the **Actions** column in the row containing the particular view you want to enable.

   Note:

   - The link changes from **Enable** to **Disable**.
   - The value in the 'Enabled' column changes from 'false' to 'true'.
6. If wanted, configure the selected view:
   - To add or remove object types for display in an object-tree hierarchy on an Overview page, see "Configuring Object Types in Profiles" on page 179 for details.

- To add or remove fields for a specific view, see "Configuring Navigational and Association Views" on page 203 or "Configuring Object Views" on page 208.
- To control which view is displayed first to users when multiple views for a page are configured, see "Setting a Default View" on page 202 for details.
- To associate a filter that will narrow the scope of data that is returned from a Filtered List view page, see "Associating Filters to Filtered List View Pages" on page 207 for details.

Disabling a View

The process of disabling a view for an object type in a profile is the same for Navigational and Object Views. It does not apply to Association Views.

Note:

- For **Overview** views - when you disable an Overview for an object type, the 'Overview' menu item that corresponds to that object type is dynamically removed from the menu list.

  For example, if you enabled a 'Control Objectives Overview' page and then decided you no longer wanted it, you could remove the Overview page for that object through the profile. When you disable the Overview view, the 'Control Objectives Overview' menu item would be dynamically removed from the 'Assessments' menu list for all users who are assigned that profile.
- For **Folder View** and **Filtered List View** - you can disable a Folder View or Filtered List View from object types that, by default, have both a Folder and Filtered List View (such as Risk, Control, Process). If only a Folder View or Filtered List View is enabled, only that view page is displayed when the user clicks the menu item for the selected object type.

  If you disable both the Folder and Filtered List view pages from an object type, the corresponding menu item with the name of the object type, is dynamically removed from the menu list for all users who are assigned that profile. Although the object type and its children are still accessible from other view pages, the object type would no longer be directly accessible to users from a menu.

  For example, if you disabled both the Folder View and Filtered List view pages in a profile for the Process object type, application users who were assigned that profile would still be able to access Process objects from a Process Overview page, a Business Entity Overview page, or the detail page of a parent or child object. However, the 'Processes' menu item would be removed from the 'Organization' menu.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. From the **Object Types** table listing, click the name of the object type (for example, SOXControl) for which you want to disable a view.
4. Navigate to the type of view you want (such as **Navigational Views** or **Object Views**).
5. Click the **Disable** link under the **Actions** column in the row containing the particular view you want to disable.

Results

Note:

- The link changes from **Disable** to **Enable**.
- The value in the 'Enabled' column changes from 'true' to 'false'.

Setting a Default View

On pages where multiple views are enabled for an object type, you can select which view you want as the default view for that page.

For example, if you have a Folder and Filtered List View enabled for Control object types, you could set the Filtered List view page to display first when user select the 'Control' menu item from the 'Assessments' menu.

The process of setting a default view for an object type in a profile is the same for Navigational and Object Views that contain a 'Make Default' link. It does not apply to an Overview view or Association Views.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. From the **Object Types** table listing, click the name of the object type (for example, SOXControl) for which you want to set a default view.
4. Navigate to the type of view you want (such as **Navigational Views** or **Object Views**).
5. Click the **Make Default** link under the **Actions** column in the row containing the particular view you want to display as the default view.

   Note:

   - The **Make Default** link is removed from the selected view.
   - The value in the 'Default' column changes from 'false' to 'true'.

Results

If you later decide to change the default view to another view, click the **Make Default** link in the row containing the view you want to display as the default view.

Setting the Display Order of Fields in a View

You can dynamically change the order in which fields are displayed for object types in a view.

Fields can be object fields, computed fields, and/or report fragment fields.

Note: The following applies only to **Filtered List**, **Folder**, and **List** views:

- The **Name** field is always displayed in column 1 and its position cannot be changed.
- If report fragment fields are configured, the 'Reports' column is always the last column in the table and its position cannot be changed.

Example

If the "Classification" object field on the property table of a Risk object Detail View page is in position 9 on the list and you wanted it to precede the "Location" object field, which is in position 3, you would change the display order number for the "Classification" field from 9 to 3. All the other object fields after position 3 are automatically re-ordered - so the display order for the "Location" field would become 4, the next field that followed would become 5, and so forth.

When you re-order fields in a view, the change is visible immediately to all users.

The process of setting the display order of fields for an object type in a profile is the same for all views.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. From the **Object Types** table listing, click the name of the object type you want to modify (for example, SOXControlObjective).
4. Select the view you want:

Navigate to this tab...	To select a link for this view...
Navigational Views	**Folder** or **Filtered List**
Association Views	**List** or **Context**
Object Views	**Detail** or **Activity**. If **Activity Views** are defined, click the name of an activity view link then click **Next** until the 'Specify Field Settings' screen is displayed in the Activity View wizard.

5. On the **Included Object Fields** table, locate the field whose order you want to change:
   a. In the **Order** box in the row of the selected field, type the new display order number for that field.
   b. Click **Update Order**.
   c. For **Detail Views** only - click **Save** to save your changes and return to the object type detail page.
   d. For **Activity Views** only - click **Next** and **Save** to save your changes and exit the wizard.

      The fields are automatically re-ordered as specified.

Configuring Navigational and Association Views

Configuring Fields in Navigational and Association Views

For each **Folder**, **Filtered List**, **List View** and Context pane that you configure for an object type within a profile, you can include, exclude, and set the order of fields.

Fields can be object fields, computed fields, and/or report fragment fields.

For information and examples about these views, see the following topics:

- **Filtered List** and **Folder Views** - see "About Folder View and Filtered List Views" on page 196

- **List Views** - see "About List Views" on page 198
- **Context Panes** - see "About Context Panes" on page 198

Including and Excluding Fields in Navigation and Association Views

When you include or exclude object fields in a Folder, Filtered List, List, and Context view, the change immediately affects all users who are assigned that profile.

Fields can be object fields, computed fields, and/or report fragment fields.

Each object type has a set of predefined object fields that consist of both shared and object-specific fields. The shared object fields (such as *Name*, *Description*, *Created By*, and so forth) are common to all object types and belong to the 'System Field' field group. With the exception of the **Name** field, which is required and always in position 1, you can choose which system and object-specific fields to include or exclude from an object view. In addition to object fields, you can also include report fragment fields that you define. In this way, you can tailor each view to accommodate changing business needs.

Note:

- For Overview pages, see "Including and Excluding Object Types on Overview Pages" on page 205 for details.
- For Detail and Activity view pages, see "About Configuring Fields in Detail and Activity Views" on page 215 for details.

Including Fields:

Before you can include an object field or report fragment field in a Navigational or Association view, the field must be visible in the object field or report fragment table listing for the selected object type or custom form. If the field is part of a field group, make sure you include the field group for the selected object type. For details, see "Configuring Fields for Object Types" on page 180.

When you include object fields or report fragment fields in a Navigational or Association view for the selected object type, the fields are displayed as table column headings in that view. By default, the column heading for report fragment fields is called 'Reports'.

You cannot modify the parameters of the table itself. Therefore, any information you add to a view must share the same table width as the rest of the table. For example, if a table has three columns and you add three more columns for a total of six, the table still takes up the same horizontal width as the original three columns. This can produce an awkward screen layout and unusual table formatting. It is good practice to display only the most important information using the table columns.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. From the **Object Types** table listing, click the name of the object type you want to modify (for example, SOXControlObjective).
4. Select the view you want:

Navigate to this tab...	To select a link for this view...
Navigational Views	**Folder** or **Filtered List**
Association Views	**List** or **Context**

5. To add field columns to the selected view:
   a. On either the **Included Object Fields** or **Included Reporting Fragment Fields** table, click **Include**. The available fields selection page is displayed.
   b. Select the box next to each field you want to display.
   c. When finished, click **Include**.
6. To modify the order in which the fields are displayed in columns in a Navigation or Association View, see "Setting the Display Order of Fields in a View" on page 202.

Excluding Fields from Views:

When you exclude object fields or report fragment fields from either a Navigational or Association View for the selected object type, the fields are removed from the table column headings in that view page.

With the exception of the required **Name** field, you can exclude any field from an object view. For example, if you exclude the 'Description' object field from a Filtered List View for an object type, the 'Description' table column and its associated data are dynamically removed from the Filtered List view page and the change is immediately visible to all users.

Note: If you exclude object fields that are referenced by JSP reports, the report may fail or return unexpected results.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. From the **Object Types** table listing, click the name of the object type you want to modify (for example, SOXControlObjective).
4. Select the view you want:

Navigate to this tab...	To select a link for this view...
Navigational Views	**Folder** or **Filtered List**
Association Views	**List** or **Context**

5. To remove object field columns from the selected view:
   a. From either the **Included Object Fields** or **Included Reporting Fragment Fields** table, select the box next to each object field you want to remove.
   b. When finished, click **Exclude**.
   c. At the confirmation prompt, click **OK**.

Including and Excluding Object Types on Overview Pages

For each Overview page that you configure for an object type within a profile, you can select which object types you want to include or exclude in the object-tree hierarchy for the selected object type.

Including Object Types on an Overview Page

When you include an object type for display in the object-tree hierarchy on an Overview page, the following occurs:

- The object type and any associated child object types are dynamically displayed to users (who are assigned that profile) in the object-tree hierarchy.
- The modification is effective immediately and there is no need to restart any IBM OpenPages services.

You can optionally display the 'Description' column on an object's Overview page by modifying its object view information. The 'Name' column is required and cannot be hidden.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. From the **Object Types** table listing, click the name of the object type you want to modify (for example, SOXControlObjective).
4. On the **Navigational Views** table of the selected object type, click the **Overview** link.
5. On the **Included Object Types** tab, click **Include**.
6. On the Available Object Types page:
   a. Select the box next to each object type you want to include in the object-tree hierarchy.
   b. When finished, click **Include**.
7. To show or hide the 'Description' column on the Overview page:
   a. On the **Object View Information** tab, click **Edit**.
   b. Click the **Show Description** arrow and select either:
      - **True** - to display the 'Description' column.
      - **False** - to hide the 'Description' column.
   c. When finished, click **Save**.

Excluding Object Types From an Overview Page

When you exclude an object type from display in the object-tree hierarchy on an Overview page, the following occurs:

- The object type and any associated child object types are dynamically removed from users (who are assigned that profile) in the object-tree hierarchy - think carefully before removing an object type from an Overview page.
- The modification is effective immediately and there is no need to restart any IBM OpenPages services.

Example:

If you exclude Controls from the Business Entity Overview page, the Control object - including any associated object types - will no longer be displayed when you expand the object-tree hierarchy on the Business Entity Overview page. The IBM OpenPages structure will appear to stop at the Risk level. In addition, Tests and Test Results will no longer be displayed, since the Controls they are associated with are hidden and not visible on the Business Entity Overview page.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. From the **Object Types** tab:
   a. Select the box next to each object type you want to exclude from the Overview page object-tree hierarchy.

      Note: Remember that excluding an object type also hides its children. For example, if you exclude Risks from the Overview page, Controls, Tests, and Test Results will also be hidden from view. You do not need to select each type - only the parent object type.
   b. When finished, click **Exclude**.
   c. At the confirmation prompt, click **OK** to effect the change.

Using Filters With Filtered List View Pages

By using a filter, you can narrow the scope of data that is returned in a Filtered List View for users who are assigned a specific profile.

Important: Before you can associate an object-specific filter to a Filtered List view page, you must have created a public filter for that object type by following the instructions in "Managing Filters for an Object Type" on page 157.

Associating Filters to Filtered List View Pages

When you associate a filter to a Filtered List View, the filter is displayed in the filter selection list on the Filtered List view page for that object type.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. From the **Object Types** table listing, click the name of the object type you want to modify (for example, SOXControlObjective).
4. Under the **Navigational Views** table of the selected object type, click the **Filtered List** link.
5. To add a filter to the Filtered List view page:
   a. On the **Associated Filters** tab, click **Associate**. The filters selection page is displayed.
   b. Select the box next to each filter you want to include.
   c. When finished, click **Include**.

Disassociating Filters From Filtered List View Pages

If you have a filter that is no longer appropriate for display in the filter selection list on a Filtered List view page for an object type, you can remove it from the list by following the steps below.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. From the **Object Types** table listing, click the name of the object type (for example, SOXControlObjective) that has the filter you want to remove.
4. From the **Associated Filters** table listing, select the box next to each filter you want to disassociate from this view.

5. When finished, click **Disassociate**.

Configuring Object Views

For each **Detail View** and **Activity View** for an object type within a profile, you can choose object fields and/or report fragment fields and set their order, insert section dividers, set fields to editable or read-only, and specify the number of columns each field will span (either one or two).

For **Activity Views**, you can also select up to three levels of object types, choose which paths to use to traverse the hierarchy for each level, select object-type filters to narrow the scope of returned search data, and determine the order of objects in a list or child hierarchy.

For information and examples about these views, see the following topics:

- **Detail Views** - see "About Detail Views" on page 199
- **Activity Views** - see "About Activity Views" on page 199

Before You Begin - Activity View Considerations

Before you create an Activity View, you need to determine the purpose of the view and identify the parent and child object types that will be included in the view. Planning your changes ahead of time helps to minimize the necessary work and prevents duplication of effort.

The following list will help you identify some of the questions you need to consider before you create a new Activity View:

- What task or activity does the user need to accomplish?
- What data does the user need displayed in this view to accomplish the task or activity?
- What are the object types that should be included in this view? Will levels be "skipped" in the object hierarchy?
- What field or fields does the user need to view or update?
- Are there constraints (such as a filter) that you need to put on the data in this view?
- If you plan to use a filter to remove extraneous objects that are not directly related to the current activity or to reduce the number of objects returned to a reasonable size, is the filter already configured for the selected object type? (For filter details, see "Managing Filters for an Object Type" on page 157.)

About the Layout of Activity Views

The layout of an Activity View page contains panes that are common to all views and panes that are unique to Activity Views. Figure 12 on page 209 shows the basic layout of an Activity View page.

The panes labeled "1" and "2" in Figure 12 on page 209 contain data common to all views, with pane "3" containing a combination of common and unique view elements.

The panes labeled "4" through "7" in Figure 12 on page 209 are unique to Activity Views. The pane labeled "4" contains the fields (configured in the Activity View Wizard) for the top-level object. Pane "5" displays the list of first-level child objects for the selected top-level object. Data displayed in the listing pane is not editable.

When an object in the listing pane is selected, that object and its children are displayed in hierarchical panes (panes "6" and "7" in Figure 12). Depending on the configuration, fields in the top-level object pane and in the hierarchical panes can be Read-only and/or editable.

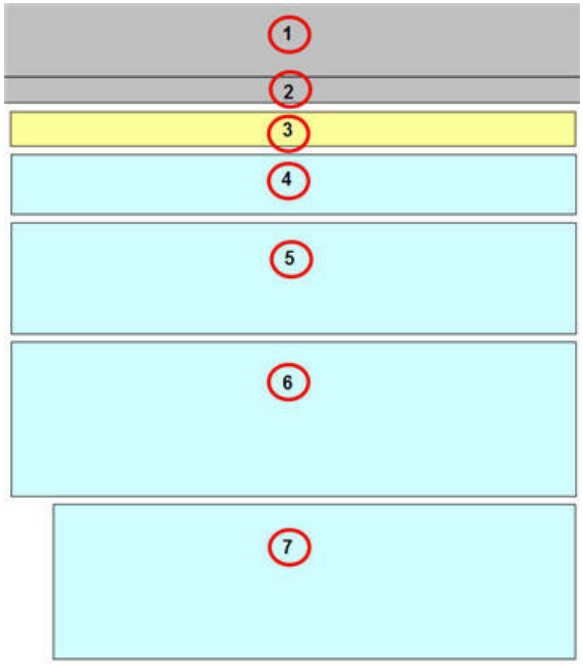


Figure 12. Layout of an Activity View Page

Key	Description
1	Header pane - contains common elements such as a logo, logon user name, logout link, and the Reporting Period selector.
2	Menu bar - a common element used as the main navigation tool for accessing objects.
3	Navigation pane - contains breadcrumb links (common element) and the Current View selector, which is displayed when multiple Object Views are available.
4	Top-level Object Field pane - unique to Activity Views - contains fields configured for the selected top-level object.
5	First-level Child Object Listing pane - unique to Activity Views - contains a list of first-level child objects configured for the top-level object. If multiple first-level child object types are configured, a selector box is displayed that allows users to switch between object types.
6	Child Hierarchy pane for the selected first-level child object - unique to Activity Views - contains fields configured for this object type.

Key	Description
7	Child Hierarchy pane for children of the selected child object - unique to Activity Views - contains fields configured for this object type.

About Creating Activity Views

When you create a new Activity View, you use the Activity View Wizard to guide you through the various tasks you need to perform to configure the view.

The following scenario describes how you might use the Activity View Wizard to create an Activity View called "Control Assessment by Risk Activity" for users who are "Control Assessors". Although the scenario does not include all the configuration features available in the Activity View Wizard, it does highlight many of the basic features.

Scenario

Let's say your organization created a profile called "Control Assessor" for users who have the responsibility to determine the effectiveness of controls.

To facilitate the work of a Control Assessor, you want to create a "Control Assessment by Risk Activity" view that would allow a Control Assessor to quickly analyze test results related to a particular control and then update the 'Operating Effectiveness' field of a Control object accordingly.

In addition, you want the users to be able to perform their work with minimal navigation and provide only data relevant to accomplishing the task. If multiple test results are displayed, the data should be sorted according to the 'Date Performed' field in ascending order.

To start, you would select the "Control Assessor" profile from the Profiles page and then select 'SOXRisk' from the list of Object Types as this is the parent object type. You would then navigate to the 'Object View' table and click the 'Add New' button to start the Activity View Wizard.

Table 37 highlights the tasks you would perform on each screen in the Activity View Wizard to create a basic Activity View called "Control Assessment by Risk Activity". The table also includes a reference for each screen in the Wizard where you can find more details about that task.

Table 37. Configuring a Sample "Control Assessment by Risk Activity" View

On this screen in the Activity View Wizard...	Do this...
1. Specify View Details (for details, see "Task 1: Specify View Details" on page 212)	In the **Name** field, type the name: *Control Assessment by Risk Activity.* (For layout refer to pane "3" in Figure 12 on page 209.)

Table 37. Configuring a Sample "Control Assessment by Risk Activity" View (continued)

On this screen in the Activity View Wizard...	**Do this...**
2. Select Object Types (for details, see "Task 2: Select Object Types" on page 213)	1. In the same row as 'Risk', click the **Choose Object Types** link and select 'Control'. (For layout refer to panes "4" for Risk, and "5" and "6" for Control in Figure 12 on page 209.) 2. In the same row as 'Control', click the **Choose Object Types** link and select 'Test Result'. (For layout refer to pane "7" in Figure 12 on page 209.) **Note:** Child object types can be at any level in the object hierarchy. In this example, we are "skipping" the 'Test' object type between 'Control' and 'Test Result'.
3. Specify Object Type Settings (for details, see "Task 3: Specify Object Type Settings" on page 213)	In the same row as 'Test Result', click the **Select Sort Criteria** link and do the following: 1. Select the 'Date Performed' field from the list. 2. Set the selected field to 'Ascending'. (For layout refer to pane "7" in Figure 12 on page 209.)
4. Specify Field Settings (for details, see "Task 4: Specify Field Settings" on page 214)	For each object type, click **Choose Fields** and select the following fields (if necessary, clear the 'Name' field box as the name of the object is automatically displayed in the pane title). When finished with selecting fields, set the display order of each field as shown and click **Update Order**. • **Risks** (all Read-only fields. For layout refer to pane "4" in Figure 12 on page 209.) – 1 Description – 2 Inherent Risk Rating – 3 Category – 4 Subcategory • **Control** (mostly Read-only fields. For layout refer to pane "6" in Figure 12 on page 209.) – 1 Description – 2 Domain – 3 Control Type – 4 Control Method – 5 Design Effectiveness – 6 Operating Effectiveness (writable) • **Test Result** (all Read-only fields. For layout refer to pane "7" in Figure 12 on page 209.) – 1 Description – 2 Performed By – 3 Reviewed By – 4 Reviewer Conclusion – 5 Date Performed – 6 Test Result – 7 Exceptions – 8 Exception Description

Table 37. Configuring a Sample "Control Assessment by Risk Activity" View (continued)

On this screen in the Activity View Wizard...	Do this...
5. Define Listing Columns (for details, see "Task 5: Define Listing Columns" on page 214)	Click **Choose Fields** and add the 'Description' field to the listing pane for child Control objects. Click **Finish** when done. (For layout refer to pane "5" in Figure 12 on page 209.)

Once the "Control Assessment by Risk Activity" view is saved, it becomes available as a selection in the **Current View** selection list at the top of a Risk object's detail page for that object type.

When a "Control Assessor" selects a particular risk for analysis and navigates to the detail page of that Risk object, that user can then click the **Current View** arrow and select the "Control Assessment by Risk Activity" view from the list of views.

When the "Control Assessment by Risk Activity" view is displayed on the page, the "Control Assessor" could then view the child controls and test results associated with that selected risk, discuss the test results (sorted by 'Date Performed' in ascending order), and then update the 'Operating Effectiveness' field of that Control object accordingly.

Adding an Activity View

To start the Activity View Wizard, perform the following steps.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. From the **Object Types** table listing, click the name of the object type to which you want to add an Activity View.
4. On the **Object Views** table, click **Add New** to open the Add Activity View Wizard.
5. Follow the instructions as described in the following tasks to complete activities in the Wizard.

Task 1: Specify View Details

The text you enter in the **Name** field for this Activity View is also the initial label text for this view. If you want different label text to be displayed as the 'name' of this Activity View to application users for selection in 'Current View' selection list, make sure to enter text in the appropriate language translation field.

Procedure

1. In the **Name** field, type a name for this Activity View.
2. Click the **Translate** link and type the label text you want to be displayed to users in the appropriate language field, and then click **Apply**.

   Note: If you do not enter translated label text for the **Name** field, the text you entered in Step 1 will be displayed to application users in the 'Current View' selection list.
3. When finished, click **Next** to continue.

Task 2: Select Object Types

Activity Views will display up to three levels of objects (the top-level object, list and detail panes for child objects, and objects under a selected child object). You can choose child object types at any level in the hierarchy for display in an Activity View.

Procedure

1. In the **Actions** column, click the **Choose Object Types** link in the row containing the selected object type (for example, RiskAssessment) to which you want to add child objects.
2. In the **Choose Object Types** box, select the box next to each child object type you want to display (for example, Risk) under that object type. When finished, click **Apply**.
3. If wanted, click the **Choose Object Types** link next to an associated object type (from Step 2), and select any object types you want to display (for example, Control) under that object type. When finished, click **Apply**.
4. When finished, click **Next** to continue.

Task 3: Specify Object Type Settings

A path is a specific branch of objects through the hierarchy. For associated objects that have multiple paths, you can choose which object paths you want to use to return data for that object type.

When a single path exists between one object level and the next, you do not have to select a path. Paths that loop back to the top-level object type are excluded from the selection list.

Procedure

1. For associated objects that have multiple paths, do the following to specify the paths through the object hierarchy by which associated data is retrieved:
   a. Click the **Choose Paths** link under the **Actions** column in the row containing the object type you selected in Task 1 (you may have to scroll down the page to see it).
   b. In the **Choose Paths** box, select or clear the box next to each object path that you want the application to use or ignore for retrieving associated object data.
   c. When finished, click **Apply**.

      The selected paths are listed under the **Paths** column.
2. To specify how the objects of a given type are sorted in a listing or child hierarchy pane, click the **Select Sort Criteria** link under the **Actions** column in the row of the object type that you want.
3. In the **Specify Sort Criteria** box:
   a. In the Available Fields pane, select each object field that you want to sort by.

      Note: A sort field does not have to be displayed on a page in order to sort a list or child hierarchy pane within the view.
   b. Click the double arrows to move object fields forward (>>) and backward (<<) between the **Available Fields** and the Selected Fields panes.
   c. In the Selected Fields pane, select a sort field and do any of the following:

Click this icon...	If you want to...
 (triangle up)	Sort objects according to this field in ascending order. This is the default setting.
 (triangle down)	Sort objects according to this field in descending order.
 (up arrow)	Move the field up in the list.
 (down arrow)	Move the field down in the list.

d. When finished, click **Apply**.

   The selected fields with their corresponding sort order are listed under the **Sort Criteria** column.

4. To specify a filter for an object type, click the **Choose Filter** link under the **Actions** column in the row of the object type that you want.
5. In the **Choose Filter** box:
   a. Select the filter you want to use.
   b. When finished, click **Apply**.

      The selected filter is listed under the **Filter** column.
6. When finished, click **Next** to continue.

Task 4: Specify Field Settings

You can choose the fields you want displayed in top-level and child hierarchy panes.

Fields can be object fields, computed fields, and/or report fragment fields.

Procedure

1. To specify the display fields for an object type, click **Choose Fields** under the object type.
   a. In the **Choose Fields** selection box, select the box next to each field you want to include.
   b. When finished, click **Apply**.
2. Optionally, insert a section. For details, see "Using Section Headings" on page 217.
3. Optionally, change the display order of the fields. For details, see "Setting the Display Order of Fields in a View" on page 202.
4. When finished, click **Next** to continue.

Task 5: Define Listing Columns

You can choose the fields you want displayed for table columns in a first-level child listing pane.

Procedure

1. To specify the table columns for the pane in which associated objects are listed:
   a. In the **Choose Fields** selection box, select the box next to each object field you want to include as a table column. By default, the **Name** field is selected.
   b. When finished, click **Apply**.
2. Optionally, change the display order of the fields. For details, see "Setting the Display Order of Fields in a View" on page 202.

3. When finished, click **Finish**.

Modifying an Activity View

When you modify an **Activity View**, you use the Activity View wizard to make the required changes. Each step in the wizard becomes an active link so you can go directly to that step and make the required changes.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. From the **Object Types** table listing, click the name of the object type (for example, RiskAssessment) you want to modify.
4. From the **Object Views** table listing, click the name of an Activity View you want to modify to open the Activity View wizard.
5. Click a link in the left pane of the wizard that corresponds with the type of change you want to make. Refer to "About Creating Activity Views" on page 210 for an overview of tasks.
6. When finished, click **Save**.

About Configuring Fields in Detail and Activity Views

For each **Detail** and **Activity** view that you configure for an object type within a profile, you can select which fields you want to include or exclude in that view.

Fields can be object fields, computed fields, and/or report fragment fields.

When you include fields in a Detail or particular Activity view, the additional fields are immediately visible to all users and are displayed in table rows on that view page.

For **Detail** views, only the object fields that you configure are used by the **Export** function (in `.xls` format) on a **Filtered List View** page (report fragment fields are ignored).

Each object type has a set of predefined object fields that consist of both shared and object-specific fields. The shared object fields (such as *Name*, *Description*, *Created By*, and so forth) are common to all object types and belong to the 'System Field' field group. With the exception of the **Name** field, which is required and always in position 1, you can choose which system and object-specific fields to include or exclude from an object view. In this way, you can tailor each view to accommodate changing business needs

Including Fields in Detail and Activity Views

Before you can include a field in a Detail or specific Activity view, the field must be visible in the object field list for selection.

Fields can be object fields, computed fields, and/or report fragment fields.

If the field is part of a field group, make sure you include the field group for the selected object type. For details, see "Configuring Fields for Object Types" on page 180.

Note: When using dependent fields in a Detail or specific Activity view, make sure to include both the controlling field and any required dependent fields. If the controlling field that requires a user to select or enter a value in a dependent field

is included in a view and the required dependent field is excluded, the user will not be able to complete the operation and the following error message will be displayed, "A field not available to you has been made required by a field dependency so you will be unable to continue with this operation."

When you include object fields in a Detail or Activity view for the selected object type, the object fields are displayed as table rows in that view.

Although you cannot modify the parameters of the table itself, you can set a field to span table columns.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. From the **Object Types** table listing, click the name of the object type you want to modify (for example, SOXControlObjective).
4. From the **Object Views** tab listing, select the view you want:

For this type of view...	Do this...
Detail View	Click the Detail link.
Activity View	1. Click the name of the Activity view you want. 2. In the left pane of the Activity View wizard, click the **Specify Field Settings** link.

5. To add fields to an object type:
   a. Click **Choose Fields** for the object type you want.
   b. In the **Choose Fields** selection box, select the box next to each field you want to include.
   c. When finished, click **Apply** or **Save**.
6. To modify the order in which the fields are displayed in the table rows on a Detail or Activity view, see "Setting the Display Order of Fields in a View" on page 202.
7. To format the field so it spans table columns, see "Spanning Table Columns" on page 219.

Excluding Fields from Detail and Activity Views

When you exclude fields from either a Detail or specific Activity view for the selected object type, the fields are removed from the table rows on that view page.

Fields can be object fields, computed fields, and/or report fragment fields.

With the exception of the required **Name** field, you can exclude any field from an object view. For example, if you exclude the 'Description' object field from a Filtered List View for an object type, the 'Description' table column and its associated data are dynamically removed from the Filtered List view page and the change is immediately visible to all users.

Note: If you exclude object fields that are referenced by JSP reports, the report may fail or return unexpected results.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. From the **Object Types** table listing, click the name of the object type you want to modify (for example, SOXControlObjective).
4. From the **Object Views** tab listing, select the view you want:

For this type of view...	Do this...
Detail View	Click the Detail link.
Activity View	1. Click the name of the Activity view you want. 2. In the left pane of the Activity View wizard, click the **Specify Field Settings** link.

5. To remove fields from an object type:
   a. Click **Choose Fields** for the object type you want.
   b. In the **Choose Fields** selection box, clear the box next to each field you want to remove from this view.
   c. When finished, click **Apply** or **Save** to effect the change.

Using Section Headings

Section headings are an optional formatting feature. You can use section headings to delineate a set of fields on a page. Once a section heading is created, it can be modified or deleted.

Inserting Section Headings

Before you create a section heading, you should identify where you want to insert it on a Detail or Activity view page. A section heading is displayed on the view page above whichever field you specify.

Fields can be object fields, computed fields, and/or report fragment fields.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. From the **Object Types** table listing, click the name of the object type you want to modify (for example, SOXControlObjective).
4. From the **Object Views** table listing:
   - For the **Detail** view - click the **Detail** link.
   - For an **Activity** view:
     a. Click the name of the Activity view you want.
     b. In the left pane of the Activity View wizard, click the **Specify Field Settings** link.
5. To insert a section heading in the selected view:
   a. Click **Insert Section** for the object type you want.
   b. In the **Section Information** box:

In this field...	Do this...
Name	Required. Type a name for this section heading.
Insert before field	Click the arrow and select a field from the list. The section heading will be displayed above the selected field.
language-specific (for example, Japanese)	Type a text string that will be used as the translated display text label for this section heading. By default, if no translation text is entered, the entry in the 'Name' field is displayed.

6. When finished, click **Apply** or **Save** to effect the change.

Modifying Section Headings

After you create a section heading, you can modify the label text used for translation.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. From the **Object Types** table listing, click the name of the object type you want to modify (for example, SOXControlObjective).
4. From the **Object Views** table listing:
   - For the **Detail** view - click the **Detail** link.
   - For an **Activity** view:
     a. Click the name of the Activity view you want.
     b. In the left pane of the Activity View wizard, click the **Specify Field Settings** link.
5. To modify a section heading in the selected view:
   a. Click **Insert Section** for the object type you want.
   b. On the object type tab, click the **Edit** link under the **Actions** column in the row containing the section that you want to modify.
   c. In the **Section Information** box, make the changes as wanted.
   d. When finished, click **Apply** or **Save** to effect the change.

Deleting Section Headings

You can remove section heading that are no longer wanted. Once a section is deleted, it is permanently removed from the system and cannot be restored.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. From the **Object Types** table listing, click the name of the object type you want to modify (for example, SOXControlObjective).
4. From the **Object Views** table listing:
   - For the **Detail** view - click the **Detail** link.
   - For an **Activity** view:
     a. Click the name of the Activity view you want.

b. In the left pane of the Activity View wizard, click the **Specify Field Settings** link.

5. To delete a section heading in the selected view:
   a. On the object type tab, click the **Delete** link under the **Actions** column in the row containing the section that you want to remove.
   b. If prompted, click **OK** to effect the change.
   c. For an **Activity** view, click **Save** to exit the wizard.

Setting Object Fields as Read-Only or Editable

You can configure object fields on an Object View page within a profile to be view only or editable to users assigned that profile by either selecting or clearing the **Read-Only** box for a field.

Note: Report fragment fields and certain system fields (such as "Last Modified By," "Created By," "Creation Date" and so forth) are set, by default, to Read-Only and cannot be changed.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. From the **Object Types** table listing, click the name of the object type you want to modify (for example, SOXControlObjective).
4. Select a 'Views' tab, and click the name of the view link you want to modify (for example, *Detail*) to open its detail page.
5. On the edit page for the selected object type, do the following in the row for each object field you want to modify:
   - To make a field non-editable - select the **Read-Only** box.
   - To make a field editable - clear the **Read-Only** box.
6. When finished, click **Save**.

Spanning Table Columns

In **Detail Views** and **Activity Views**, fields are typically displayed on the page in rows within a two-column table format. You can make a row containing a field span table columns by configuring the **Span Columns** setting.

Note:

- For object fields with a 'Text Area' display type, you can configure the text box size by setting the number of rows and columns. By default, the rows are set to 5, and the columns are set to 60.
- For report fragment fields with an 'Automatic' display type, you can configure the cell height of the report element. By default, this is set to 235 pixels.

The **Span Columns** setting is displayed for all field display types and the process of setting it is the same.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. From the **Object Types** table listing, click the name of the object type containing the object field you want to modify (for example, SOXControl).

4. On the **Object Fields** table for the selected object, click the name of the field to open its detail page (for example, *Who Performs Control?*).
5. On the **Display Type Information** table, click **Edit**.
6. On the edit page, click the Span Columns arrow and select a value from the list:

If the value is set to...	Then...
False	The row containing the field will be displayed within a table column and not span the columns of the table. See "Spanning Table Columns" on page 219. This is the default value.
True	The row containing the field will span the columns of the table.

7. When finished, click **Save**.

Configuring the Display Type for Reporting Fragment Fields

You can configure how report fragment fields are displayed to application users on Detail and Activity View pages. Report fragment fields are always read-only fields.

Report fragment fields can be displayed as follows:

- **Automatic** - this setting embeds the report element directly into the cell for the field and displays it as a view-only field on the page.

  If wanted, you can also configure the cell height of the field. By default, it is set to 235 pixels.

- **On Demand** - this setting displays a clickable icon  in the field that opens the report element in a pop-up window. For information on automatically sizing pop-up windows, see "Setting Limits for Automatically Sized Reporting Fragment Pop-up Windows" on page 309.

Note: Changing the display type setting will affect the display of this field in all profiles.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. From the **Object Types** table listing, click the name of the object type containing the report fragment field you want to modify (for example, SOXControl).
4. On the **Object Fields** table for the selected object type, click the name of a report fragment field to open its detail page.
5. On the **Object Field Information** table:
   a. Click **Edit**.
   b. On the edit page, click the **Display Type** arrow and select a value from the list.
   c. When finished, click **Save**.

6. For Automatic display types only. If the display type is On Demand, skip this step.
   Optionally, modify the cell height of the report fragment field:
   a. On the **Display Type Information** table, click **Edit**.
   b. On the edit page, modify the number of pixels in the **Cell Height** box.
   c. When finished, click **Save**.
7. To make the row with the report fragment field span table columns, see "Spanning Table Columns" on page 219.

Configuring Display Types for Simple String Fields

For object fields that have a Simple String data type, you can configure how string data displays to users on an object's details page. The display types for Simple String data fall into two basic categories: selector types for displaying users and/or groups, and text area display types for displaying text and URL information.

Note: Changing the display type setting will affect the display of this field in all profiles.

Selecting a Display Type for Simple String Fields

This is the procedure to select a display type for object fields that have a Simple String data type.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. From the **Object Types** table listing, click the name of the object type containing the object field you want to modify (for example, SOXControl).
4. On the **Object Fields** table for the selected object type, click the name of the object field to open its detail page.
5. On the **Object Field Information** table, click **Edit**.
6. On the edit page:
   a. To make the field required, select the **Required** box.
   b. To select a different display type, click the **Display Type** arrow and select a value from the list:
      - For user or group selector display types, see "Configuring User and Group Selector Display Types for Simple Strings" on page 224.
      - For a rich text display type, see "Configuring Rich Text Display Types for Simple Strings" on page 222.
      - For a box and URL display types, see "Configuring Text and URL Display Types for Simple Strings" on page 222.
      - For a plain text area display type, see "Configuring Text Area Display Types for Simple String Data Types" on page 223.
7. To have a row with a field span table columns, see "Spanning Table Columns" on page 219.
8. When finished, click **Save**.

Results

Note: To change a field to **Read-Only**, see "Setting Object Fields as Read-Only or Editable" on page 219.

Configuring Rich Text Display Types for Simple Strings

The Rich Text display type provides a text display area with a toolbar and commands for text formatting and word processing. The toolbar can be minimized or expanded. When this feature is used, you may not be able to enter 4000 rich text characters into the text display area because of the space used for formatting and multi-byte characters.

Note: When generating CommandCenter reports in PDF format, rich text fields do not render properly and the format is not preserved.

To modify these settings, click **Edit** on the **Display Type Information** tab.

You can configure the size of the display area with the following settings:

Table 38. Rich Text Display Settings

Setting	Description
Rows	The display length of the area, which includes the rich text editor interface and text input area. The default value is 250 rows. To change the value, type a number in the box.
Row Units (pixels or percent)	The unit of measure in pixels or percent for the Rows setting. The default value is "Percent". To change the value to "Pixels", select the **Pixels** button.
Columns	The percent or number of pixels allocated to the width of the display area, which includes the rich text editor interface and text input area. The default value is 100 percent. To change the value, type a number in the box. To change the unit of measure, use the **Column units** setting.
Column units	The unit of measure in pixels or percent for the Columns setting. The default value is "Percent". To change the value to "Pixels", select the **Pixels** button.

For instructions on how to configure a display type for a String data type object field, see "Configuring Display Types for Simple String Fields" on page 221.

Configuring Text and URL Display Types for Simple Strings

The Text and URL display types provide a box area in which users can enter a string value. For these display types, you can control the length of the display box and the number of characters users can enter for a string value.

Note: The URL display type validates that the internet address is a fully-qualified URL internet address (for example, http://www.mycompany.com or ftp://ftp.myftpsite.com) and will display an error message to the user if the format of the internet address is incorrect.

To modify these settings, click **Edit** on the **Display Type Information** tab.

For Text and URL display types, you can configure the following settings:

Table 39. Text and URL Display Settings

Setting	Description
Columns	The display length of the box area. The default value is 30. To change the value, type a number in the box.
Maximum Length	The maximum number of bytes allowed to be entered for a string value. The default value is 4000. To change the value, type a number in the box.

For instructions on how to configure a display type for a String data type object field, see "Configuring Display Types for Simple String Fields" on page 221.

Configuring Text Area Display Types for Simple String Data Types

The Text Area display type provides a box display area in which users can enter either plain or HTML-formatted text.

To modify these settings, click **Edit** on the **Display Type Information** tab.

You can configure the size of the display area with the following settings:

Table 40. Text Area Display Settings

Setting	Description
Rows	The display length of the box area. The default value is 5 rows. To change the value, type a number in the box.
Columns	The display width of the box area. The default value is 60. To change the value, type a number in the box.

For instructions on how to configure a display type for a simple string data type object field, see "Configuring Display Types for Simple String Fields" on page 221.

Configuring User and Group Selector Display Types for Simple Strings

You can configure a User, Group, User/Group Selector display type for a Simple String data type object field.

About User and Group Selectors

Object fields with a display type of 'User Selector' only accept user names as valid values. For example, 'Control Owner' is an object field for the Control object.

An object field that has a User, Group, User/Group Selector display type allows an application user to click either the field box or the user or group icon to display a pop-up dialog box from which they can select users or groups.

The following selector display types are available for Simple String data types:

Table 41. User and Group Display Settings

Selector Display Type	Description
User Drop-down	Provides an arrow  that users can click to display a drop-down list box of user names.
User Selector	Provides the following: • A user icon  that users can click to display a phonebook style pop-up dialog box of user names. For configuration details see, "Controlling User Selector Performance" on page 226 and "Modifying User and Group Selectors" on page 227. • A magnifying glass icon  that users can click to display a search pop-up dialog box to search for a user.
Group Selector	Provides the following: • A group icon  that users can click to display a pop-up dialog box of group names listed in a hierarchical tree structure. • A magnifying glass icon  that users can click to display a search pop-up dialog box to search for a group.
User/Group Selector	Provides a group icon  that users can click to display a pop-up dialog box of user names listed in a hierarchical tree structure under the group to which the user belongs.

Depending on the selector display type, you can configure some or all of the following settings.

To modify these settings, click **Edit** on the **Display Type Information** tab.

Note: These settings are also applied to the User and Group Search function.

Table 42. Additional Selector Display Type Settings

Setting	Description
Include Disabled	Allows or disallows disabled user accounts to be included in a selector listing. If the **Include Disabled** value is set to: • **True** - disabled user accounts are included in the selector listing. When this setting is selected, the **Minimum Access** setting is disabled. • **False** (default value) - disabled user accounts are excluded from the selector listing. When this setting is selected, the **Minimum Access** setting is enabled. **Note:** This setting generally applies to User (not Group) selectors.
Starting Group	Controls which group displays at the beginning of the selection hierarchy. To select a starting group, click the group icon and select a valid group name from the selector window. For example, if you are using role-based security, you could select the **Security Domains** group, for non role-based security, you could select the **Workflow, Reporting and Others** group.
Include Subgroups	Controls whether subgroups are included or excluded from the User selector listing. **Note:** This setting does not apply to the User/Group and Group selectors. If the **Include Subgroups** value is set to: • **True** (default value) - subgroups are included in the selector listing. • **False** - subgroups are excluded from the selector listing.
Minimum Access	This setting is enabled only if the **Include Disabled** value is set to **False**. This setting allows you to filter users based on access control list settings on an object's folder. For example, let's say you want to limit the number of users who can be assigned as a Process "Cycle Owner", which is an object field with a user selector display type for the Process object. Because you previously set up an access control list (ACL) for one or more groups or users to the Process folder, you can use the Minimum Access setting to filter the list of users. If you only wanted users with "Delete" permissions to be displayed on the user selector list, you can select the "Delete" Minimum Access setting to filter and display only those users with "Delete" ACL permissions.

Table 42. Additional Selector Display Type Settings (continued)

Setting	Description
• Read	If the **Read** box is: • Selected - only users with Read access are displayed on the user list. • Cleared - no filtering occurs. This is the default setting.
• Write	If the **Write** box is: • Selected - only users with Write access are displayed on the user list. • Cleared - no filtering occurs. This is the default setting.
• Delete	If the **Delete** box is: • Selected - only users with Delete access are displayed on the user list. • Cleared - no filtering occurs. This is the default setting.
• Associate	If the **Associate** box is: • Selected - only users with Associate access are displayed on the user list. • Cleared - no filtering occurs. This is the default setting.

Controlling User Selector Performance

If your deployment has a large number of users, the performance of the User Selector in opening and loading data may be sluggish. One way to improve the performance of the User Selector is to configure it so it only retrieves users that have permission on the object being edited.

The supplied profiles in the OpenPages application are configured such that the User Selector pop-up will retrieve all users in the system - including some application users who do not have security permissions on the selected object. This may result in the assignment of a user as 'owner' on an object when the user does not have read access on the object.

The following steps explain how to restrict the set of users retrieved by the User Selector to those users that have access permissions on the object being edited at the time.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. From the **Object Types** table listing, click the name of the object type containing the object field you want to modify (for example, SOXControl).
4. On the **Object Fields** table for the selected object, click the name of the object field with the User Selector display type to open its detail page (for example, 'Control Owner').
5. On the **Display Type Information** tab, click **Edit**.
6. On the edit page:

a. Under **Minimum Access**, select the **Read** box. This will restrict the users that are displayed in the User Selector to the set of users that have read permission on the object.
b. If wanted, select other permissions to further restrict the users that are available in the User Selector based on the users' permissions.

7. When finished, click **Save**.

Modifying User and Group Selectors

The pop-up dialog box for the User Selector displays user names in a phonebook style, and you can configure the number of users per category within the phonebook. The Group Selector and User/Group Selector use a hierarchical tree style to display group and user information in the dialog box.

If wanted, you could also configure the User, Group, or User/Group Selector display type to open a search box instead of a phonebook style box (see "Configuring a User or Group Selector to Use the Search Function" on page 283).

For all the selector display types, you can configure additional display information for users, such as the user's an e-mail address or first or last name.

Modifying the Phonebook: The User Selector displays user names in a phonebook style pop-up dialog box. User names within the phonebook are grouped into data buckets.

Each data bucket has the following characteristics:

- The names of the first and last users in a given bucket are used to show the scope of the bucket.
- The user names in a bucket can be expanded by clicking the plus sign, or collapsed by clicking the minus sign.
- The size of a bucket can be configured through the **Bucket Size** setting. The default size is 10 user names per bucket.
  For configuration details see, "Configuring the Bucket Size of the Phonebook" on page 282.

Modifying the Selector Dialog Box: You can show additional information (such as a user's email address, first name, and last name) in the pop-up dialog box used for selecting users and groups.

You can add one or more additional columns by configuring the **Display** setting. For configuration details see, "Configuring Display Columns in a Selector Dialog Box" on page 282.

By default, only the **Name** and **Description** columns are displayed in this selection box. You cannot change or remove the **Name** column - it is always the first column and contains the Username of a user or group.

If wanted, you can also change the format of the bucket heading for a locale. For configuration details see, "Modifying the Bucket Heading Format of the Phonebook" on page 241.

Configuring Display Types for Long String Fields

For object fields that have a long string data type, you can configure how long string data displays to users on an object's details page.

There are two sub types of long text fields: medium and large. The size of medium long text fields is fixed to 32KB. The size of the large long text fields is set by default to 256KB, but that can be increased by changing the **OpenPages | Platform | Repository | Resource | Large Text | Maximum Size** setting.

Be aware of the space used for non-printing characters (such as tabs and line breaks), and formatting and multi-byte characters (Rich Text display types). These may cause the data to exceed the size of the long string field, resulting in a message such as:

```
OP-03381: The specified value for "MyMediumLong" is too long. The 32966
characters entered (32966 bytes) exceeds the maximum size of 32768 bytes.
Reduce the number of characters and re-enter the text. Note that character
count includes non-printing characters, such as spaces, tabs, and line
breaks.
```

There four display types for medium long string data: On Demand, On Demand Rich Text, Text Area, and Rich Text.

There two display types for large long string data: On Demand, and On Demand Rich Text.

Both medium and large long string fields default to the On Demand display type.

Note: Changing the display type setting will affect the display of this field in all profiles.

For more information on long text fields, see "About Data Types" on page 111.

Selecting a Display Type for Long String Fields

This is the procedure to select a display type for object fields that have a Long String data type. You can configure how both medium and large long string data displays to users on an object's details page.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. From the **Object Types** table listing, click the name of the object type containing the object field you want to modify (for example, SOXControl).
4. On the **Object Fields** table for the selected object type, click the name of the object field to open its detail page.
5. On the **Object Field Information** table, click **Edit**.
6. On the edit page:
   a. To make the field required, select the **Required** box.
   b. To select a different display type, click the **Display Type** arrow and select a value from the list:
      - For On Demand and On Demand Rich Text, see "Configuring the On Demand Display Types for Long String Fields" on page 229. This applies to both medium and large long string fields.
      - For a Text display type, see "Configuring Text Display Types for Medium Long String Fields" on page 230. This applies only to medium long string fields.

- For a Rich Text display type, see “Configuring Rich Text Display Types for Medium Long String Fields” on page 231. This applies only to medium long string fields.

7. When finished, click **Save**.

Results

Note: To change a field to **Read-Only**, see “Setting Object Fields as Read-Only or Editable” on page 219.

Configuring the On Demand Display Types for Long String Fields

You can configure how long string fields are displayed On Demand and On Demand Rich Text to application users on Detail and Activity View pages.

Long string fields can be displayed as On Demand or On Demand Rich Text. Both settings display a clickable icon  in the field that opens the long string field in a pop-up window. On Demand displays text. On Demand Rich Text displays the data in rich text format.

The On Demand Rich Text display type provides a text display area with a toolbar and commands for text formatting and word processing. The toolbar can be minimized or expanded. When this feature is used, be aware of the space used for non-printing, formatting, and multi-byte characters. These may cause the data to exceed the size of the long string field, resulting in a message such as:

```
OP-03381: The specified value for "MyMediumLong" is too long. The 32966
characters entered (32966 bytes) exceeds the maximum size of 32768 bytes.
Reduce the number of characters and re-enter the text. Note that character
count includes non-printing characters, such as spaces, tabs, and line
breaks.
```

Note: When generating CommandCenter reports in PDF format, rich text fields do not render properly and the format is not preserved.

Note: Changing the display type setting will affect the display of this field in all profiles.

To modify these settings, click **Edit** on the **Display Type Information** tab.

For both display types, you can configure the following settings:

Table 43. On Demand and On Demand Rich Text Display Settings

Setting	Description
Span Columns	In **Detail Views** and **Activity Views**, fields are typically displayed on the page in rows within a two-column table format. You can make a row containing a field span table columns by configuring the Span Columns setting. The default is true. When true, the row containing the field will span the columns of the table. When false, the row containing the field will be displayed within a table column and not span the columns of the table.

Configuring Text Display Types for Medium Long String Fields

The Text display type provide a box area in which users can enter a medium long string value. For these display types, you can control the length of the display box and the number of characters users can enter for a string value.

Note: This only applies to medium long string fields.

To modify these settings, click **Edit** on the **Display Type Information** tab.

For the Text display type, you can configure the following settings:

Table 44. Text Display Settings

Setting	Description
Rows	The display length of the box area. The default value is 25 rows. To change the value, type a number in the box.
Columns	The display width of the box area. The default value is 60. To change the value, type a number in the box.
Span Columns	In **Detail Views** and **Activity Views**, fields are typically displayed on the page in rows within a two-column table format. You can make a row containing a field span table columns by configuring the Span Columns setting. The default is true. When true, the row containing the field will span the columns of the table. When false, the row containing the field will be displayed within a table column and not span the columns of the table.

For instructions on how to configure a display type for a String data type object field, see "Configuring Display Types for Long String Fields" on page 227.

Configuring Rich Text Display Types for Medium Long String Fields

The Rich Text display type provides a text display area with a toolbar and commands for text formatting and word processing. The toolbar can be minimized or expanded. When this feature is used, be aware of the space used for non-printing, formatting, and multi-byte characters. These may cause the data to exceed the size of the medium long string field, resulting in a message such as:

```
OP-03381: The specified value for "MyMediumLong" is too long. The 32966
characters entered (32966 bytes) exceeds the maximum size of 32768 bytes.
Reduce the number of characters and re-enter the text. Note that character
count includes non-printing characters, such as spaces, tabs, and line
breaks.
```

Note: When generating CommandCenter reports in PDF format, rich text fields do not render properly and the format is not preserved.

To modify these settings, click **Edit** on the **Display Type Information** tab.

You can configure the size of the display area with the following settings:

Table 45. Rich Text Display Settings

Setting	Description
Rows	The display length of the area, which includes the rich text editor interface and text input area. The default value is 250 rows. To change the value, type a number in the box.
Row Units (pixels or percent)	The unit of measure in pixels or percent for the Rows setting. The default value is "Percent". To change the value to "Pixels", select the **Pixels** button.
Columns	The percent or number of pixels allocated to the width of the display area, which includes the rich text editor interface and text input area. The default value is 100 percent. To change the value, type a number in the box. To change the unit of measure, use the **Column units** setting.
Column units	The unit of measure in pixels or percent for the Columns setting. The default value is "Percent". To change the value to "Pixels", select the **Pixels** button.

Table 45. Rich Text Display Settings (continued)

Setting	Description
Span Columns	In **Detail Views** and **Activity Views**, fields are typically displayed on the page in rows within a two-column table format. You can make a row containing a field span table columns by configuring the Span Columns setting. The default is true. When true, the row containing the field will span the columns of the table. When false, the row containing the field will be displayed within a table column and not span the columns of the table.

For instructions on how to configure a display type for a long string data type object field, see "Configuring Display Types for Long String Fields" on page 227.

Configuring Display Types for Enumerated Strings

For object fields that have an Enumerated String data type, you can configure how enumerated string data displays to users on an object's details page. The display types for Enumerated String data include lists, radio buttons, and check boxes.

Note: Changing the display type setting will affect the display of this field in all profiles.

Selecting a Display Type for Enumerated Strings

This is the procedure to select a display type for object fields that have an Enumerated String data type. Enumerated strings can be displayed as lists, radio buttons, or check boxes.

Procedure

1. Access the Profiles page (see "Accessing Profiles" on page 176).
2. From the list, click the name of a profile to open its detail page.
3. From the **Object Types** table listing, click the name of the object type containing the object field you want to modify (for example, SOXControl).
4. On the **Object Fields** table for the selected object type, click the name of the object field to open its detail page.
5. On the **Object Field Information** table, click **Edit**.
6. On the edit page:
   a. To make the field required, select the **Required** box.

      If a field is **not** required, to provide the ability to enter an empty value in the field:

      - For radio buttons, a **None** option is automatically added to the set of radio buttons.
      - For check boxes, the user would clear all check boxes.
      - For lists, an empty selection is added to the list of choices.

      When **None** is selected in a set of radio buttons, all check boxes are cleared, or the empty option in a list is selected, the value for the enumerated field will be blank.

Note: Field dependencies may mean a field is required even if **Required** is not selected. For details on field dependencies, see "Configuring Dependent Field Behavior" on page 165.

The **None** label can be changed and localized in the **Application Text | Labels | com.label.enum.selection.none** setting. For details on changing application text, see "About Application Text" on page 238.

b. To select a different display type, click the **Display Type** arrow and select a value from the list.

Select **List** to set the display as a list. Lists can be single selection or multiple value selection, depending on the **multi-value** setting for the field.

Select **Radio Button/Checkbox** to set the display type as radio buttons or check boxes. If the field is defined as **multi-value**, the display will use check boxes. If **multi-value** is not selected for the field, the display will use radio buttons.

For details on enumerated string data types, see "About Data Types" on page 111.

Chapter 11. Localizing Text

This chapter contains the following topics:

This chapter describes the administrative interface that you can use to manage localized text that displays to users for predefined object types, object fields that are supplied by OpenPages or created by you, and application objects.

Localization Overview

You can localize display text for object types and fields, and for a variety of application objects and custom return values.

About Locale Codes

The IBM OpenPages application provides translation support in several languages for predefined object text. Each supported language has a corresponding locale code that is listed under the object text. The locale code consists of a language code (for example, "fr" for French) and a country code (for example, "FR" for France).

The following table lists the supported languages with their corresponding locale code.

Table 46. Supported Languages and Locale Codes

Language	Locale Code
German	de_DE
U.S. English	en_US
U.K. English	en_GB
Spanish	es_ES
French	fr_FR
Italian	it_IT
Japanese	ja_JP
Brazilian Portuguese	pt_BR
Simplified Chinese	zh_CN
Traditional Chinese	zh_TW
Report Design Language **Note:** Users authoring reports in the CommandCenter tool must select this language prior to creating or modifying reports.	en_CA

The default language for object text that has not been translated is U.S. English.

You can globally set a default language in which the application user interface will be displayed to users and optionally enable auditing of translation label changes. For details see "Setting Localization Options" on page 276.

Configuring Client Systems to Display Asian Characters

For users who will be using the Japanese locale, client machines must have the Windows East Asian language pack installed. If this pack is not installed, IBM OpenPages application users will notice that the browser title bar and some pop-up messages will contain unreadable characters. To install the East Asian language pack on Windows client machines, follow these instructions.

Procedure

1. Click **Start** and select **Control Panel**.
2. Double-click **Regional and Language Options** to open its properties.
3. Click the **Languages** tab.
4. Select the **Install files for East Asian languages** option.
5. Click **OK** and follow the on-screen directions.

Localizing Object Text

About Object Text

Object text is the descriptive label name that displays in the application for object types and object fields. You can translate and modify object text for a specific locale. For a list of supported locales, see the topic, “About Locale Codes” on page 235.

You can modify the following object text for a locale:

- The singular and plural labels that display the name of an object type (for example, "Risk" and "Risks" for the Risk object type) or custom form (such as a survey) wherever that object type appears in the application. For details see, “Modifying Display Text for an Object Type” on page 237.
- A singular label that displays:
  - The name of an object field in an object view.
    For example, if you had an object field called "Impact" that displayed the label text "Impact", you could change the label text to display "Severity of impact" instead.
  - The value or values of an enumerated object string that are displayed on an object’s details page.

Note: Object text has a 4000 character maximum per label.

Object text is grouped primarily by object type with an additional group for unassigned field groups.

For example, the `SOXControl` group contains the label text for the Control object and its related field groups.

The `Unassigned Field Groups` group contains the label text for field groups that are either not assigned to an object type or are commonly used by all object types, such as System Fields, Currency Attributes, Publishing, and so forth.

Accessing the Object Text Page

Note: To access the **Object Text** menu item, you must have the **Object Text** application permission set on your account (for details, see “Configuring Application Permissions” on page 18).

Procedure

1. Log on to the IBM OpenPages application as a user with the **Object Text** application permission set.
2. From the menu bar, select **Administration** and click **Object Text**.

Results

From the Object Text page, you can:

- View a list of all the available object types and associated field groups with their corresponding locale text labels.
- Access the label detail page of an object type where you can modify its locale-specific object text label.
- Access the label detail page of an object field where you can modify its locale-specific object text label.
- Access the label detail page of a public filter where you can modify its display name on the various lists (such as pull-down menus or tables).

Modifying Display Text for an Object Type

You can modify the value for the singular and plural forms of the displayed label text for any object type or custom form object type (such as a survey). These labels appear in the IBM OpenPages application interface wherever the particular object type displays, such as on a menu (for object types) or in object views.

Procedure

1. Access the Object Text page (see "Accessing the Object Text Page" on page 236).
2. On the **Object Text** page, click the name of the object type you want to modify (for example, SOXRisk).
3. On the **Locale Information** tab, click the name of the locale code you want to modify (for example, en_US).
4. On the **Locale Code** detail page, make the required changes in the **Singular Label** box and **Plural Label** box to the display label text as needed.
5. When finished, click **Save**.
6. To modify other locale-specific labels for this object type, repeat Steps 3 through 5.

Modifying Display Text for Object Fields

You can modify the value of the displayed label text for any object field, including field guidance. These labels appear in the IBM OpenPages application interface wherever the particular object type displays in an object view, such as a detail or folder view page.

If the object field is an enumerated string data type, each string value is also displayed and can be modified as needed.

Procedure

1. Access the Object Text page (see "Accessing the Object Text Page" on page 236).
2. On the **Object Text** page:
   a. Click the plus sign next to the object type you want (this will expand its contents).
   b. Under the selected object type, click the plus sign next to the field group you want.

c. Under the selected field group, click the name of the object field that you want to modify. If this is an enumerated string, go to Step 8.

3. On the **Locale Information** tab, click the name of the locale code you want to modify (for example, en_US).
4. On the **Locale Code** detail page, make the required changes:
   a. In the **Label** box, change the display label text as needed.
   b. In the **Guidance** box, change the text as needed. This text is displayed when a user clicks the question-mark icon on an object's edit or add page.
   c. When finished, click **Save**.
5. To modify other locale-specific labels for this object field, repeat Steps 3 through 6.
6. To modify enumerated string values:
   a. On the Object Text page, click the plus sign next to the enumerated object field you want (this will expand its contents).
   b. Click the name of the value that you want to modify.
   c. Repeat Steps 4-5.

Modifying Display Text for Public Filters

You can modify the value of the displayed label text for public filters. In a Filtered List View, the label text for filters is typically displayed under "Public filters" in the filters list.

Procedure

1. Access the Object Text page (see "Accessing the Object Text Page" on page 236).
2. On the **Object Text** page:
   a. Click the plus sign next to the object type you want to expand its contents.
   b. Under the selected object type, click the plus sign next to the Filters  icon to expand its contents.
   c. Click the name of the filter that you want to modify.
3. On the **Locale Information** tab, click the name of the locale code you want to modify (for example, en_US).
4. On the **Locale Code** detail page, make the required changes:
   a. In the **Label** box, change the display label text as needed.
   b. In the **Guidance** box, change the text as needed. This text is displayed when a user clicks the question-mark icon on an object's edit or add page.
   c. When finished, click **Save**.
5. To modify other locale-specific labels for this filter, repeat Steps 3 and 4.

Localizing Application Text

About Application Text

Application text is the descriptive label name that displays for objects such as buttons, table headings and columns, and system object fields that are commonly used throughout the application. Application text is considered "static", which means that its label is unlikely to change over time. You can modify application text that is specific to a locale (see the topic, "About Locale Codes" on page 235 for a list of supported locales).

You can modify locale-specific application text for:

- A singular label that displays the name of an application object - see the following table for a list of object categories.
- The format for the display of names and numeric data. For details see, “Modifying User Display Formats” on page 241.

Note: Application text has a 4000 character maximum.

The following table shows the groupings for application text by folder category.

Table 47. Application Text Folder Categories

This folder...	Contains the label text for...
Application Messages	Messages that are displayed for dependent fields and picklists, and System Admin Mode.
Buttons	The buttons used within the application. For example, com.button.back contains the text for the "Back" button, button.copy contains the text for the "Copy" button.
Column Headings	The table column headings used in the various object views throughout the application and in JSP Notification Manager reports. For example, com.column.heading.start.date contains the text for the "Start Date" column, jspreports.notification.tests.column.parent contains the text for the "Parent" column in the JSP Notification report.
Custom	User-defined keys. For details, see “Using the Custom Folder” on page 245.
Exceptions	Messages that are displayed to users when an error condition occurs. For example, com.exception.object.profile.not.found contains the text for the error message displayed when a profile is not found, exception.file.delete contains the text for the error message displayed when a user does not have permission to delete a file.
Formats	The formatting of numeric and name display text. For details, see “Modifying User Display Formats” on page 241.
Labels	Objects that are generally not considered objects, such as administrative, task, and configuration objects. For example, com.label.acl.read contains the text for the "Read" property on the Access Control details page, com.label.email contains the text displayed next to the email input box on the User create and edit pages.
Menu Items	Links to all other menu items that are not listed on the menu bar. For example, com.menu.item.admin.object.profile contains the text for the ‘Profile’ link on the Administration menu, com.menu.item.admin.reporting.schema contains the text for the "Reporting Schema" link on the Administration menu.
Miscellaneous	A variety of objects that do not belong to other groups. Includes label text for such objects as guided action, page footer, reporting status, notification messages, and so forth.
Reporting Framework	Objects that are used by the Reporting Framework.

Table 47. Application Text Folder Categories (continued)

This folder...	Contains the label text for...
Table Headings	Messages that are displayed to users within a table as well as the tabs (tabular headings for a table). For example, com.table.empty.users contains the text that displays in the User listing table when no users are found, com.table.heading.object.field contains the text for the "Object Field Information" tab on the Object Field details page.
Titles	The initial portion of the breadcrumb trail.
Validation Messages	Messages that are displayed to users when invalid information has been entered in a field or to confirm a specific user action such as entering or exiting System Administration Mode or deleting any objects. For example, com.validation.logon.username.required contains the message text displayed when a user name is missing such as when it is created or when a user logs on, file.delete.confirmText contains the text in the confirmation prompt window that displays during a delete operation.
Workflow	Workflow related job names, task names, task descriptions, and arrow labels (originating from task nodes).

Accessing the Application Text Page

Note: To access the **Application Text** menu item, you must have the **Application Text** application permission set on your account (for details, see "Configuring Application Permissions" on page 18).

Procedure

1. Log on to the IBM OpenPages application as a user with the **Application Text** application permission set.
2. From the menu bar, select **Administration** and click **Application Text**.

Results

From the Application Text page, you can:

- View a list of the various object types with their corresponding object fields.
- Access the detail page of an object field where you can modify its locale-specific object text label.

About Modifying Display Text in the Application User Interface

You can modify the value of the displayed label or text for any application object (such as buttons, labels, report names and descriptions, messages) in the IBM OpenPages application user interface. Changes to the displayed text appear wherever the particular object is displayed in the application.

Note: The process for modifying display text is the same for all application objects, including reports.

Note:

- The 'Miscellaneous' folder typically contains a listing of report name and description keys for localizing the display text of reports that were automatically

published by the system. For information about automatically publishing CommandCenter reports, see "Adding CommandCenter Reports" on page 86.

- For reports that were manually published from the IBM OpenPages server and require localized display text on the application user interface for multiple languages, keys will need to be added to the 'Custom' folder (see "Using the Custom Folder" on page 245).

1. Access the Application Text page (see "Accessing the Application Text Page" on page 240).
2. On the **Application Text** page:
   a. Navigate to the folder that contains the label of the object field you want to modify (for example, 'Buttons' or 'Miscellaneous'), and click the plus sign to expand the folder contents.
   b. Click the name of the object field or key you want to modify.
3. On the **Locale Information** tab, click the name of the locale code you want to modify (for example, en_US or ja_JP).
4. On the **Locale Code** details page, make the required changes in the **Label** box to the display label text as needed.
5. When finished, click **Save**.
6. To modify other locale-specific labels for this object field, repeat Steps 3-5.

Modifying User Display Formats

You can globally change the display format for certain object fields. The most commonly used formats are described here. For information about other format settings, contact your IBM representative.

The format string uses Java code. Generally, the **{0}** in the format string is a variable that is replaced by the name of the target object.

Modifying the Bucket Heading Format of the Phonebook

You can modify the format of the bucket heading in the phonebook style pop-up box of the User selector for a locale.

Note: If wanted, you can also modify the bucket size of the phonebook. For more information, see "Configuring the Bucket Size of the Phonebook" on page 282.

Procedure

1. Access the Application Text page (see "Accessing the Application Text Page" on page 240).
2. On the **Application Text** page:
   a. Navigate to the **Formats** folder, and click the plus sign to expand the folder contents.
   b. Click the **com.user.bucket.name.format** link to open its detail page.
3. On the **Locale Information** tab, click the name of the locale code you want to modify (for example, en_US).
4. On the detail page, modify the format in the **Singular Label** box. The default format is {0} - {1}.
5. When finished, click **Save**.
6. To modify the bucket heading for another locale, repeat Steps 3 - 5.

Example

To display a bucket heading with the name of the first person in the bucket followed by a dash and then the name of the last person in that bucket, you would enter the following codes in the Singular Label field: {0} - {1}.

Modifying the User Name Format

You can control how user names are displayed for a locale. By default, only the user name displays.

When you change the display name format, the change occurs throughout the application wherever the person's name displays. For example, if you modified the name format so that the last name of the person was followed by the person's first name, that modified name format displays in the top menu bar, user selector and search result boxes.

Note: If an invalid format string is defined, only the user's logon name will be displayed.

Procedure

1. Access the Application Text page (see "Accessing the Application Text Page" on page 240).
2. On the **Application Text** page:
   a. Navigate to the **Formats** folder, and click the plus sign to expand the folder contents.
   b. Click the **com.display.name.format** link to open its detail page.
3. On the **Locale Information** tab, click the name of the locale code you want to modify (for example, en_US).
4. On the detail page, modify the format in the **Singular Label** box as follows:

To display this name format...	Type this code...	Comments
User name	%NM;	By default, displays the logon name of a User. If other values are entered, the logon name appears within brackets.
First Name	%FN;	Displays information from the "First name" object field on a User Information page.
Last Name	%LN;	Displays information from the "Last name" object field on a User Information page.
Email	%EM;	Displays the email address of a user from the "Email" object field on a User Information page.

5. When finished, click **Save**.
6. To modify the bucket heading for another locale, repeat Steps 3 - 5.

Example

To display the first and last name of users, you would enter the following codes in the Singular Label box: **%FN; %LN;**.

The user name displays within brackets when the first and last names are used.

Modifying Navigational Link Formats

You can modify the link format of items that are listed on menus for each locale.

Under the various menu headings on the menu bar, Overview menu item links are typically listed before the other object view links. With the exception of Overview object links and the Business Entities link (which is a List view), all other object types have Filtered List View and/or Folder object views.

Modifying Overview Menu Links

You can globally modify the format of Overview navigational links on menus.

By default, the format for overview links is:

```
{0} Overview
```

where {0} represents the singular label of the object.

This format displays, for example, menu item links such as 'Risk Assessment Overview' or 'Business Entity Overview'.

Example:

If you wanted to change the Overview link format from the singular object name followed by the text 'Overview' (as in Risk Assessment Overview or Business Entity Overview) to 'Overview' followed by the object name (as in Overview Risk Assessment or Overview Business Entity) you would enter the value in the Singular Label box as:

```
Overview {0}
```

Procedure

1. Access the Application Text page (see "Accessing the Application Text Page" on page 240).
2. On the **Application Text** page:
   a. Navigate to the **Formats** folder, and click the plus sign to expand the folder contents.
   b. Click the **menu.item.documentation.object.overview** link to open its detail page.
3. On the **Locale Information** tab, click the name of the locale code you want to modify (for example, en_US).
4. On the detail page, modify the text in the **Singular Label** box.
   The singular label of the object type is represented by **{0}** in the format string.
5. When finished, click **Save**.
6. To modify the link Overview format for another locale, repeat Steps 3 - 5.

Modifying Navigational View Links

You can globally modify the format of Folder View or Filtered List View navigational links on menus.

By default, the format for these links is:

```
{0}
```

where {0} represents the plural label of the object.

This format displays, for example, menu item links such as ‘Risks’ or ‘Business Entities’.

Example:

If you wanted to change the Folder View or Filtered List View link format from the object type name (such as ‘Risks’ or ‘Controls’) which is represented by {0}, to display the object type name followed by the text "View" (such as ‘Risks View’ or ‘Controls View’), you would enter the value in the Singular Label box as `{0} View`.

Procedure

1. Access the Application Text page (see “Accessing the Application Text Page” on page 240).
2. On the **Application Text** page:
   a. Navigate to the **Formats** folder, and click the plus sign to expand the folder contents.
   b. Click the **menu.item.documentation.object.folder.view** link to open its details page.
3. On the **Locale Information** tab, click the name of the locale code you want to modify (for example, en_US).
4. On the details page, add or edit text in the **Singular Label** box.

   Note: The plural label of the object type (such as, Risks, Controls, Processes) is represented by **{0}** in the format string.
5. When finished, click **Save**.
6. To modify the link Folder View or Filtered List View format for another locale, repeat Steps 3 - 5.

Modifying List View Links

You can globally modify the format of the Business Entity List view navigational link on the Organization menu.

Procedure

1. Access the Application Text page (see “Accessing the Application Text Page” on page 240).
2. On the **Application Text** page:
   a. Navigate to the **Formats** folder, and click the plus sign to expand the folder contents.
   b. Click the **menu.item.documentation.object.list.view** link to open its details page.
3. On the **Locale Information** tab, click the name of the locale code you want to modify (for example, en_US).
4. On the details page, add or edit text in the **Singular Label** box.

   Note: The plural label of the object type (such as, Business Entities) is represented by **{0}** in the format string.
5. When finished, click **Save**.
6. To modify the link List View format for another locale, repeat Steps 3 - 5.

Using the Custom Folder

About the Custom Folder

The **Custom** folder is a container for user-defined keys (such as values returned by computed fields, e-mail text for Notification Reports, and values used by Survey reports). The keys also provide a means for displaying localized text in the IBM OpenPages application user interface for reports (such as reports that are manually published from the IBM OpenPages server).

Typically, this folder is populated through the ObjectManager tool. Optionally, you can add new keys to the **Custom** folder from the Application Text page.

To modify localized display text for a key in the **Custom** folder, see "About Modifying Display Text in the Application User Interface" on page 240.

Adding New Keys

Note: For CommandCenter report pages (or JSP report instances) that were manually created using the publishing facility on the IBM OpenPages server, you can use the values in the 'Report Name Key' and 'Report Description Key' fields on the report page to manually create custom application text keys to localize the name and description of a report after it is created.

To add new keys to the Custom folder for localization, follow these steps.

Procedure

1. Access the Application Text page (see "Accessing the Application Text Page" on page 240).
2. On the **Application Text** page:
   a. Navigate to the **Custom** folder.
   b. Click the **Add New** link to open its detail page.
3. On the add detail page:
   a. In the **Name** box, type the name of the key.
      For example, a report called 'My Loss Events' could have `report.name.my.loss.events` for a report name key or `report.description.my.loss.events` for a report description key.
   b. Optionally, type a description of the key.
   c. In the **Default Label** box, type the text that will be displayed, by default, if no translated text is provided.
   d. When finished, click **Create**.
4. Click the name of the field created in the previous step, to open its detail page.
5. To change the label text for a locale, on the Locale Information pane:
   a. Click the link for the locale code you want.
   b. In the **Label** box, type the translated text you want displayed for that locale.
   c. When finished, click **Save**.
   d. Repeat Steps a-c for other locales.

Modifying Custom Keys

To modify custom keys, follow these steps.

Procedure

1. Access the Application Text page (see "Accessing the Application Text Page" on page 240.
2. On the **Application Text** page:
   a. Navigate to the **Custom** folder.
   b. Click the name of a key to open its detail page.
3. On the **Locale Information** pane:
   a. Click the link for the locale code you want.
   b. In the **Label** box, type the translated text you want displayed for that locale.
   c. When finished, click **Save**.
   d. Repeat Steps a-c for other locales.

Chapter 12. Resetting Objects

This chapter contains the following topics:

Overview of Reporting Periods

A reporting period is a "snapshot" of the current state of the repository, usually created when the documentation phase of a quarter or year is complete and ready for attestation. Administrators with the Reporting Periods application permission can create, modify, and delete reporting periods.

Past reporting periods can then be viewed and reported on from any time in the future without rolling back the changes made to the repository after the reporting period was created.

Once a reporting period is created, the existing report is carried forward to the current reporting period and can be modified in a normal fashion without altering the state of the earlier reporting period’s data.

Note: Only one reporting period at a time can be "Active".

About Active Reporting Periods and Operational Limitations

Active reporting periods are essentially in the process of being closed (or "finalized"). An active reporting period can be reapplied at any business entity level to synchronize the business entity and its children with the Current Reporting Period.

An active reporting period affects application behavior as follows.

- Filtering behavior:
  - Only filters that use system fields (such as, ‘Name’ or ‘Description’) will work.
  - All objects on Filtered List View, Activity View, and Home pages are generally displayed, unless a system-field filter is applied to a particular view.
- Reporting behavior: Reports cannot run against an active reporting period. You can only run reports against the current reporting period and any finalized past reporting periods.
- The following operations CANNOT be performed during an active reporting period:
  - Move operations
  - Rename operations

– Delete operations

About Finalized Reporting Periods

Once an active reporting is finalized, the contents of that reporting period cannot be altered. Any changes to the objects or files will only be reflected in the current reporting period.

This allows administrators to create the next reporting period ahead of time and then apply it incrementally to different areas of their documentation project when each area is ready to be finalized.

How Reporting Periods and the Reporting Schema Interact

By default, the reporting schema is only populated with the data from the current reporting period. To populate the reporting schema with data from previous reporting periods you must enable the **Populate Past Periods** setting and recreate the reporting schema (see, "Populating Past Reporting Periods" on page 61).

How Reporting Periods and ACLs Interact

When viewing objects, your existing ACLs control which objects you can view in the current reporting period and in past reporting periods. If your access permissions change in the current reporting period, you will be able to view the newly accessible items in past reporting periods, and you will not be able to view items to which you have lost permissions, even if in past reporting periods you had access to them.

Regardless of your access permissions, you are never allowed to add, edit or remove objects and/or files from past reporting periods.

How Reporting Periods and Audit Trails Interact

When viewing an audit trail for an object, only the changes made during the currently selected reporting period are shown. You can view the audit trail for past reporting periods, but only the change activities for that reporting period will be shown.

You cannot view audit trails for multiple reporting periods on the same page.

Using System Administration Mode with Reporting Periods and Schemas

When you create, recreate, or finalize reporting periods, follow these guidelines:

- If you create an active Reporting Period before creating a real-time Reporting Schema, you need to be in System Administration Mode (see Chapter 4, "Using System Admin Mode," on page 57) to either finalize or drop the active Reporting Period.
- If the Reporting Period is created after you have created the real-time Reporting Schema, you do not need to be in System Administration Mode to finalize or drop the Reporting Period if the Reporting Schema is disabled.
- If the real-time Reporting Schema is enabled, you must be in System Administration Mode to create, drop, or finalize a Reporting Period.

Reporting Period Permissions and Settings

To manage reporting periods, the user performing the reporting period operation must belong to a group with the following application permissions.

Reporting Period Permissions

There are two sub-permissions for reporting periods:

- **Finalize** - allows members of the group to finalize reporting periods on Business Entities. Users will only be able to finalize reporting periods on Business Entities to which they have viewing permissions.
- **Reapply** - allows members of the group to update the active reporting period to represent the current state of a Business Entity.

Configuring the Deletion Period

It is possible to configure the amount of time after a reporting period is created in which the reporting period can be deleted. This property is set in the *Delete Interval* setting and defaults to 7 days after the reporting period is created. For details see, "Modifying the Deletion Interval for a Reporting Period" on page 273.

Creating a New Reporting Period

To create a new reporting period, you must have the Reporting Periods application permission. If an active reporting period already exists, you cannot create a new reporting period.

Procedure

1. From the menu bar, select **Administration** and click **Reporting Periods**. The Reporting Periods page is displayed.
2. Click the **Add Active...** button at the top of the page. A new page is displayed.
3. Enter the necessary information into the correct fields and click **Create** to create the new reporting period. You are returned to the Reporting Periods page and the new reporting period is listed in the table with a status of "Active".
4. Click **Refresh** to update the current value of the Status field.

Results

After adding a new reporting period, the reporting period will be added to the Reporting Period selection list at the top of each overview and object page.

Note: If you have any standalone objects in your system (objects that were not created in the context of a business entity hierarchy) they will be immediately finalized when the reporting period is created.

Creating a New Finalized Reporting Period

You may know that you will not need to edit a reporting period further, and do not need to reapply portions of the object hierarchy before finalization. In this case, you can use the **Add Finalized** button to create a new reporting period and immediately finalize it. After the reporting period is created you will not be able to modify it without deleting the entire reporting period.

Procedure

1. From the menu bar, select **Administration** and click **Reporting Periods**.
2. Click the **Add Finalized** button at the top of the page. The Create a Reporting Period page is displayed.
3. Enter the label and description for the new reporting period and click **Create**.

Working with the Active Reporting Period

When an active reporting period is created, it is applied to all of the objects (resources) in the IBM OpenPages repository. While a reporting period is active, there are two actions you can take - reapplying the reporting period, or finalizing the reporting period. The reporting period can be reapplied or finalized on a business entity by business entity case.

When you reapply a reporting period, it updates the "checkpoint" created by the reporting period to include the current state of the business entity (and its children).

When you finalize a reporting period, it freezes the reporting period and prevents any more updates through reapplying the reporting period.

Reapplying the Active Reporting Period to a Business Entity

Reapplying a reporting period updates the reporting period version of the entity (and its associated hierarchy of objects) to match the current "live" version. Reapplication of the reporting period can be done at any level of the business entity hierarchy, and will only affect the children of the currently viewed business entity.

Note: To perform any Reporting Period operation, the system must be in System Administration Mode (see Chapter 4, “Using System Admin Mode,” on page 57).

Procedure

1. Navigate to the business entity you want to be the root of the reapplied reporting period.
2. At the top of the page, select the active reporting period from the list and click the **View** button. The **Re-Apply** and **Finalize** buttons appear.
3. On the locks page, if you want to remove all locks on the selected business entity after the reapply operation, select the ‘Remove all Locks’ option.
4. Click the **Re-Apply** button to update the business entity and all of its children to their current "live" version.

Results

For example, if you have a business entity with the field "Entity in Scope?" set to "Yes" and you create an active reporting period, when you view that business entity in that reporting period you will see "Yes" as the value.

If you then change the value of Entity In Scope to "No" in the Current Reporting Period (the live data), and you want to update the entity in the active reporting period, you can reapply the active reporting period and the value of Entity In Scope will be updated to "No".

Note: There is no way to reverse a reapplication of a reporting period or to only pick up some of the modifications made to the children of the business entity, so be careful when reapplying a reporting period.

Finalizing a Reporting Period

Once you are certain that no more changes need to be made to a business entity and its descendants, you can finalize the reporting period for that business entity.

Once you have finalized an entire reporting period, it ceases to be active. Only then can you create a new active reporting period. If even one business entity remains un-finalized, the reporting period remains active.

Procedure

1. From the menu bar, select **Administration** and click **Reporting Periods**.
2. Click the name of the active reporting period to display the detail page.
3. Click the **Finalize** button to finalize the entire reporting period. You are returned to the Reporting Periods page. The status of the reporting period changes to Finalizing.
4. Click **Refresh** to update the current value of the Status field.

   Note: You cannot undo a finalize operation without removing the entire reporting period. Depending on the size of your repository, it may take a significant amount of time to finish the finalizing operation.

   To finalize a reporting period on a business entity:

   a. Navigate to the business entity you want to be the root of the finalized reporting period.
   b. At the top of the page, select the active reporting period from the list and click the >> button. The **Reapply** and **Finalize** button appear.
   c. Click the **Finalize** button to prevent any further changes to the business entity and all of its child objects.

Deleting a Reporting Period

After you have created a reporting period, occasionally you may have to delete it to reflect last-minute changes to your financial close, or due to a mistake in the name (for example, wrong quarter, wrong year, and so forth).

The IBM OpenPages application supports deletion of reporting periods for a configurable amount of time after the reporting period is created.

Note: The default period for deletion of a reporting period is seven days after creating an active reporting period.

The following table lists the various conditions under which a reporting period can be deleted:

If the deletion period has...	Then the active reporting period...
expired	cannot be deleted.
not expired	can be deleted.

When a reporting period is deleted, no files are removed from the database.

Procedure

1. From the menu bar, select **Administration** and click **Reporting Periods**.
2. On the Reporting Periods page, select the check box next to the name of the reporting periods you want to delete.
3. Click the **Delete** button at the top of the page.
4. At the confirmation prompt, click **OK** to delete the selected reporting period. You are returned to the Reporting Periods page and the deleted reporting period is removed from the table.

5. Click **Refresh** to update the current value of the Status field while the deletion is occurring.

Results

Note: If you cannot delete a reporting period (you click the check box and the **Delete** button does not activate), the deletion period for that reporting period has expired. However, if wanted, you can retroactively change the setting.

Overview of Object Resets

Object Resets are a way to automatically modify objects that exist in the IBM OpenPages repository. Resets can be started by users with the proper permissions from the Object Reset menu item in the Administration section of the menu bar.

The most common use of the Object Reset functionality is to "reset" all of your objects at the beginning of a new Reporting Period. For example, each quarter you have controls and tests that need to be reviewed and performed. The results of those tasks are recorded by updating the properties and attachments of the appropriate objects. Once all of these quarterly tasks have been completed, and the quarter is finished, you archive all of the results into a Reporting Period and prepare for the new quarter. However, the existing objects still display the test results and changed properties of the previous quarter.

Rather than go in and modify the objects by hand, you can use the Object Reset capability to take your existing objects and modify their properties based on the rules in your ruleset.

While Resets work well with the Reporting Period capability of the IBM OpenPages application, Resets do not require the existence of a Reporting Period to be utilized.

Using Object Reset on System Fields

When modifying fields or using fields within <criteria> tags, you may not use "system" fields. System fields are the fields common to all object types, such as name, description, or creator. Field modifications and ruleset criteria must use custom fields (non-system fields). If the field you want does not appear in a field group for the appropriate Object Type, you cannot use it in your ruleset.

Using Object Reset on Currency Fields

If you use an Object Reset rule to update the value of the Local Currency Code of a currency field, the Exchange Rate and Base Amount are not updated to match the new Local Currency Code value.

While the Base Amount is calculated using the Local Currency Code and the Exchange Rate, it will not change because the Exchange Rate has not been modified and the number of displayed fraction digits for the currency has not been changed.

In order to see a change in the Base Amount, you must include a rule to update the Exchange Rate or modify the number of displayed fraction digits.

Preparing Your Data

Before a Reset is performed, you will need to perform a few tasks to help ensure that the Reset procedure goes smoothly. It is always recommended that you back up your IBM OpenPages data before running a Reset. In addition, if you plan on archiving your changes to a Reporting Period, you will need to set the Reporting Period up before running the Reset.

Backing Up Your IBM OpenPages Data

It is highly recommended that you back up your pre-existing IBM OpenPages data prior to running a Reset. In this way, an un-modified copy of your data is maintained, in case your Reset ruleset does not perform as intended. For details on backing up your data, see "About the Backup and Restore Utilities" on page 329.

Creating a Reporting Period (optional)

If you are planning to reset your data as part of the beginning of a new Reporting Period, you will have to archive the existing data to a Reporting Period. Detailed instructions for creating a new Reporting Period can be found in "Overview of Reporting Periods" on page 247.

Creating a Ruleset

Object Resets are rule-based operations on the objects in your IBM OpenPages repository. The rules that govern how a Reset will affect your data are contained in a Ruleset. A Ruleset is a set of rules contained in an XML loader file that is created outside of the IBM OpenPages application. Multiple Rulesets can be included in a single XML file. The ruleset loader file is loaded into the system through the ObjectManager loader tool. Once the Ruleset is imported, it can be selected during the Specify Options step of the Object Reset guided action.

Object Resets can modify objects in three ways: modifying the value of a property, deleting an object, and disassociating two objects.

When creating a Ruleset, you must know the bundles, properties, and property values you are modifying and match them exactly. If you do not specify a valid property or property value, the property will not be modified.

Note: Before creating a final Ruleset to use for your Reset session, it can be extremely helpful to create simple Rulesets that contain a single rule from your final Ruleset. Running these single Rulesets against a known data set can verify the accuracy of each rule before attempting a massive modification of your data.

Creating the Ruleset File

To create the ruleset file, open a new text file in a text editor. Save the file with the following naming convention:

```
<file-identifier>-op-config.xml
```

Once the file is saved, you may edit it to create the XML file.

Sample Ruleset

Here is a sample Ruleset:

```
 <?xml version="1.0" encoding="UTF-8"?>

<openpagesConfiguration xmlFormatVersion="1.20">
```

```
    <ruleSets>
        <ruleSet name="Quarterly Reset"
                 description="Rule set to be executed at the beginning of each
and every quarter"
                 type="Object Reset">

            <rule name="Rule 1"
                  description="Property Update rule setting a property"
                  type="Property Update">
                <propertyUpdateRule contentType="SOXControl">
                    <bundle name="SOXControl">
                        <property name="Design Effectiveness"
                                  useDefaultValue="false">
                            <propertyValue name="Not Rated"/>
                        </property>
                    </bundle>
                </propertyUpdateRule>
            </rule>

            <rule name="Rule 2"
                  description="Property Update rule setting a collection of
properties (including a multi-valued one)."
                  type="Property Update">
                <propertyUpdateRule contentType="SOXRisk">
                    <bundle name="SOXRisk">
                        <property name="Assertions"
                                  useDefaultValue="false">
                            <propertyValue name="Existence"/>
                            <propertyValue name="Rights and Obligations"/>

   </property>
                        <property name="Impact"
                                  useDefaultValue="false">
                            <propertyValue name="Unknown"/>
                        </property>
                    </bundle>
                </propertyUpdateRule>
            </rule>

            <rule name="Rule 3"
                  description="Object Delete rule"
                  type="Object Delete">
                <objectDeleteRule contentType="SOXTestResult"/>
            </rule>

            <rule name="Rule 4"
                  description="Object Delete rule with criteria"
                  type="Object Delete">
                <objectDeleteRule contentType="SOXIssue"/>
                <criteria logicalOperator="or">
                    <criterion bundle="SOXIssue"
                               property="Status"
                               operator="=">
                        <propertyValue name="Closed"/>
                    </criterion>
                </criteria>
            </rule>

            <rule name="Rule 5"
                  description="Object Disassociate rule"
                  type="Object Disassociate">
                <objectDisassociateRule parentContentType="SOXRisk"
                                        childContentType="SOXDocument"/>
            </rule>

        </ruleSet>
```

```
<!-sample Reset Ruleset for a currency property->
<ruleSet name="Your_Ruleset_Name"
          description="Reset a currency property"
                 type="Object Reset">
            <rule name="Reset a currency property"
       description=""
       type="Property Update">
     <propertyUpdateRule contentType="SOXAccount">
      <bundle name="OPSS-Account_Annualized Value">
        <property name="Annualized Value_LA"
               useDefaultValue="false">
          <propertyValue name="1.0"/>
              </property>
     </bundle>
           <bundle name="OPSS-Account_Annualized Value">
        <property name="Annualized Value_LC"
               useDefaultValue="false">
          <propertyValue name="AED"/>
              </property>
     </bundle>
           <bundle name="OPSS-Account_Annualized Value">
        <property name="Annualized Value_ER"
               useDefaultValue="false">
          <propertyValue name="1.0"/>
              </property>
     </bundle>
     </propertyUpdateRule>
            </rule>
        </ruleSet>
    </ruleSets>
</openpagesConfiguration>
```

The Ruleset Tag Library

The following XML tags can be used to build a ruleset:

<openpagesConfiguration>

Description: Progenitor tag for the loader file contents. All other tags are contained within the <openpagesConfiguration> tag.

Parent Tags: None.

Child Tags: <ruleSets>

Syntax:

```
<openpagesConfiguration xmlFormatVersion="1.15">
</openpagesConfiguration>
```

Attributes:

Attribute	Description
xmlFormatVersion	Version of the OpenPages XML DTD.

<ruleSets>

Description: Container tag for one or more ruleSet tags.

Parent Tags: <openpagesConfiguration>

Child Tags: <ruleSet>.

Syntax:

```
<ruleSets>
</ruleSets>
```

Attributes: None.

<ruleSet>

Description: A ruleset is a collection of rules that will be executed when the ruleset is selected during a Reset session. Each ruleset is displayed in the IBM OpenPages user interface as a separate entry in the list of Rulesets.

Parent Tags: <ruleSets>

Child Tags: <rule>

Syntax:

```
<ruleSet name="Name"
      description="Description"
      type="Object Reset"
</ruleSet>
```

Attributes:

Attribute	Description
name	An identifying name for the ruleset. Will be displayed in the IBM OpenPages user interface. The maximum length for the ruleset name attribute is 255 bytes (not characters).
description	A description of the function of the ruleset. The maximum length for the ruleset name attribute is 2000 bytes (not characters).
type	The type of ruleset. Currently, there is only one type - "Object Reset".

<rule>

Description: Each <rule> tag contains a single rule that will be applied to the IBM OpenPages data when the ruleset is selected and a Reset session is initiated.

Parent Tags: <ruleSet>

Child Tags: <propertyUpdateRule>, <objectDeleteRule>, <objectDisassociateRule>, <criteria>

Syntax:

```
<rule name="Name"
      description="Description"
      type="[Property Update|Object Delete|Object Disassociate]"
</rule>
```

Attributes:

Attribute	Description
name	The name of the rule. The maximum length for the rule name attribute is 255 bytes (not characters).
description	A description of the function of the rule. The maximum length for the rule name attribute is 2000 bytes (not characters).
type	The type of rule. There are three types of rules: Property Update, Object Delete, and Object Disassociate.

<propertyUpdateRule>

Description: The <propertyUpdateRule> tag defines a rule that modifies the value of an existing property on a certain object type. Unless modified by the use of the <criteria> tag within the same <rule> tag, all objects of the specified object type within the scope of the Reset will be updated.

Parent Tags: <rule>

Child Tags: <bundle>

Syntax:

```
<propertyUpdateRule contentType="">
</propertyUpdateRule>
```

Attributes:

Attribute	Description
contentType	Specifies the object type that the rule will be applied to. Must match a valid IBM OpenPages object type.

<bundle>

Description: The <bundle> tag specifies which bundle contains the property to be modified.

Parent Tags: <propertyUpdateRule>

Child Tags: <property>

Syntax:

```
<bundle name=""
</bundle>
```

Attributes:

Attribute	Description
name	The name of the bundle whose property will be modified.

<property>

Description: The <property> tag is used inside a <bundle> tag to specify the property that will be updated.

Parent Tags: <bundle>

Child Tags: <propertyValue>

Syntax:

```
<property name="">
          useDefaultValue="[true|false]"
  [<propertyValue>
   <propertyValue>]</property>
```

Attributes:

Attribute	Description
name	The name of the property to be updated
useDefaultValue	Specifies whether the property should be updated to reflect the default value of the property (if one exists). If no default value exists, the property is not updated.

<objectDeleteRule>

Description: The <objectDeleteRule> tag is used to specify an object type for deletion. Unless modified by the use of the <criteria> tag within the same <rule> tag, all objects of the specified object type within the scope of the Reset will be deleted.

Parent Tags: <rule>

Child Tags: None.

Syntax:

```
<objectDeleteRule contentType=""/>
```

Attributes:

Attribute	Description
contentType	Specifies the object type to be deleted. All objects of this type within the scope of the Reset are deleted.

<objectDisassociateRule>

Description: The <objectDisassociateRule> tag is used to disassociate an object type from another object type. If you use the <criteria> tag with this rule type, the criteria must be based on the child's property values. You cannot base a rule on properties or property values belonging to the parent object type.

Parent Tags: <rule>

Child Tags: None.

Syntax:

```
<objectDisassociateRule parentContentType=""
                        childContentType=""/>
```

Attributes:

Attribute	Description
parentContentType	Identifies the parent object type that the child object type is associated with.
childContentType	Identifies the child object type to be disassociated. Any objects of the child object type associated with objects of the parent object type within the scope of the Reset will be disassociated from the parent object.

<criteria>

Description: The <criteria> tag is used to refine the behavior of a rule by specifying the standards that need to be met in order to invoke the rule. The criteria tag can contain one or more <criterion> tags that will be judged when deciding whether to apply the rule to a specific object. It should be noted that criteria can only be applied in a "positive" manner - that is, if the criteria are met, the rule will be used. You cannot specify a rule where if the criteria are met, the rule is NOT applied.

Parent Tags: <rule>

Child Tags: <criterion>

Syntax:

```
<criteria logicalOperator="[and|or]">
```

Attributes:

Attribute	Description
logicalOperator	Specifies whether all of the criterion ("and") will be used to determine whether the rule will be applied to the object, or if only one of the criterion ("or") needs to be satisfied.

<criterion>

Note: It is strongly recommended that you use a maximum of three criterion within a single <criteria> tag. Adding additional criterion will increase the processing time required to complete the Reset.

Description: The <criterion> tag allows the user to specify a property and value(s) that must match the evaluation specifications set in the <criterion> tag.

Parent Tags: <criteria>

Child Tags: <propertyValue>

Syntax:

```
<criterion bundle=""
           property=""
           operator="[=|<>|<=|<|>|>=|like]"
  <propertyValue=""/>
 [<propertyValue=""/>]</criterion>
```

Attributes:

Attribute	Description
bundle	The property bundle containing the property to be evaluated.
property	The property name of the property to be evaluated
operator	Specifies the manner in which the value of the property will be evaluated. Valid operators are equal (=), not equal (<>), greater than (>), less than (<), greater or equal to (>=), less than or equal to (<=), and "like". Only the equal, not equal, and "like" operators can be used with string variables. **Note:** The "like" parameter allows the use of wild cards in the <propertyValue> tag. These wild cards consist of the "%" and "_" symbols, which are passed to a SQL database query against the Oracle database. The percent mark (%) symbol is used to represent any number of characters in a location, while the underscore (_) character is used to represent any single character in a location. The usage is consistent with the use of wild cards in a SQL **where** clause. See your SQL documentation for additional information, if needed.

<propertyValue>

Description: The <propertyValue> tag performs two functions, depending on its location.

If the <propertyValue> tag is contained inside a:

- <property> tag, it specifies the new value (or values) for the updated property.
- <criterion> tag, it specifies the relevant property to be considered when applying the criteria.

If you are modifying an enumerated string (drop-down list) property that is multi-selectable, you can place multiple <propertyValue> tags inside the <property> tag. When the rule is processed, all of the <propertyValue> tags will be evaluated, and the property will be modified to select all of them.

Parent Tags: <property>, <criterion>

Child Tags: None.

Syntax:

```
<propertyValue name=""/>
```

Attributes:

Attribute	Description
name	Specifies the value of the property. See the description of the <propertyValue> tag for details. The maximum length for the property value's name attribute is 2000 bytes (not characters).

Loading the Ruleset

After you have finished creating the ruleset loader file, you will need to use the ObjectManager tool to load the ruleset into the IBM OpenPages system.

Procedure

1. Open a command or shell window on the IBM OpenPages server.
2. Navigate to the <OP_Home> directory.

Where: <OP_Home> represents the installation location of the IBM OpenPages GRC Platform application. By default, this is:	
Windows	C:\OpenPages
AIX	/opt/OpenPages

3. Run the following command on a single line:

   ```
   ObjectManager load config OpenPagesAdministrator  <password>
   <path-to-ruleset-xml-file> <file-identifier>
   ```

   where

   <password> is the password to the OPAdminstrator user account.

   <path-to-ruleset-XML-file> is the full path to the ruleset file you created.

   <file-identifier> is the portion of the ruleset file name preceding "-op-config.xml". For example, if you created a ruleset file called "ruleset-op-config.xml", the <file-identifier> in the ObjectManager command is "ruleset".
4. The ruleset is now loaded. If you have created multiple ruleset files, repeat this procedure for each of them.
5. If you encounter errors, read the log file to determine the cause of the error and fix it, then re-run the command in Step 2.

Updating a Ruleset

If you load a ruleset with the same name as an already-loaded ruleset, the ruleset will be overwritten with the new rules. To return to an earlier version of the ruleset, you would have to re-load the original ruleset loader file. Rulesets are not "version-controlled".

Performing the Object Reset

After you have loaded the ruleset you will be using for the Object Reset, you must log into the system and begin the Reset.

Preparing for the Reset

The user running the Reset must have the Object Reset application permission and the proper access to modify the data. If the user does not have the Object Reset permission, they will not be able to see the Object Reset menu item under the Administration heading.

Configuring the Ruleset Parameters

Before executing the Reset, there are some configuration parameters that should be set. In general, these settings will only need to be set once before your first time initiating a Reset, but you may want to change them for different entity trees or ruleset behavior.

The following Object Reset settings can be accessed from the **Settings** link on the Administration menu (located in the *OpenPages\Applications\Common\Object Reset* folder):

- *Logging Level* - this setting controls how much information is displayed. For configuration details, see "Changing the Logging Level" on page 300.
- *Check ACL* - this setting controls whether the Reset occurs against all or only some of the objects contained within the scope of the Reset session. For configuration details, see "Obeying ACL Restrictions" on page 301.
- *Ignore Locks* - this setting controls whether existing locks on objects are honored when running the Reset. For configuration details, see "Obeying Locking Restrictions" on page 301.
- *Continue on Error* - this setting controls whether the Reset session will log errors and continue to run or halt processing. For configuration details, see "Continuing on Error" on page 301.

Using the Object Reset Page

The Object Reset page contains a table that shows all of the previous Reset sessions that have been started. The table contains columns with the following information:

- the name of the Reset session
- the description of the Reset session
- the date and time the Reset began
- the date and time the Reset completed
- the current status of the Reset

The table also has an **Start New Reset** button that can be selected to start a new Reset session. For more information on starting a new Reset session, see "Starting the Object Reset."

Starting the Object Reset

Procedure

1. Log on to the IBM OpenPages system as a user with the Object Reset application permission.

   Note: If you have chosen to obey ACL restrictions, the user must have the permissions to modify the objects within the scope of the Reset. If the user does not have sufficient permissions, warning messages will be generated in the log, and the objects will not be modified.
2. Click the **Object Resets** menu item under the **Administration** heading on the menu bar. The Object Reset page is displayed.

3. Click the **Start New Reset** button at the top of the table to create a new Reset. The Specify Options page is displayed.
4. Enter a name and description for the new Reset.
5. Select a Ruleset from the list of available Rulesets. The chosen Ruleset will be used for the new Reset.
6. Click **Next** to display the Reset Scope page.
7. Choose the Business Entities to which the Reset will be applied by selecting the check boxes next to the entity names. Once you have selected the Business Entities, click the **Start Reset** button to begin the Reset.
8. A confirmation warning dialog is displayed. If, after reading the warning, you want to begin the Reset, click **Ok**. The Reset begins, and the Object Reset page is displayed.

Viewing the Reset Status

The new Reset session is added to the list of Reset sessions on the Object Reset page. You can track the progress of the Reset by monitoring the Status column of the table. The possible values for the Status field are Initiated, In Progress, Completed, or Failed.

The "Failed" status will only be shown if the system is set to stop the Reset if errors are encountered. If the system is set to continue on errors, then when the Reset is completed, the "Completed" status will be shown. Any errors that occurred during the Reset will be captured in the Reset Session Log.

Viewing the Reset Session Details

Every time you start a Reset, an entry is added to the Reset Session table. By clicking on the name of the reset, the Reset Session detail page is displayed for that Reset Session.

The detail page contains the following information:

Name - The name of the Reset Session.

Description - The description of the Reset Session (set during the creation procedure)

Ruleset Name - The name of the Ruleset that was applied during this session.

Created - The time and date the Reset Session was created.

Start Date - The time and date the Reset was begun.

End Date - The time and date the Reset was completed.

Status - The current status of the Reset. The Status can be one of the following values:

- Initiated - The Reset has been initialized, and is preparing to modify your data.
- In Progress - The Reset is currently modifying the selected data.
- Completed - The Reset finished successfully. Depending on whether the Reset was set to continue on errors, some errors may be reported in the Session Log.
- Failed - The Reset did not finish, because errors were encountered. Check the Session Log for details on what errors occurred.

Created By - The user that initiated the Reset Session.

Scope - The Business Entities that were modified by the Reset.

Logging Level - The level of detail that will be displayed in the Session Log. Can be one of the following values:

- Low - display error messages only
- Medium - display any error messages and any warning messages.
- High - display any errors, warnings, and any informational or diagnostic messages.

Continue on Error - Whether the Reset Session will log errors and continue to run, or whether the error will be logged and the session will halt. Value will either be "true" or "false".

Check ACLs - Whether the Reset occurs against all objects contained within the scope of the Reset session, or whether the Reset occurs against only those objects that the user who initiated the Reset has access to. It can have a value of "true" or "false".

Ignore Locks - Whether existing locks on objects are honored when running the Reset. A value of "true' means that locks were ignored when running the Reset, and a value of "false" means that locked objects were not modified by the Reset.

Viewing the Reset Session Log

In addition to the detail page, a detailed view of the Reset Session is recorded in the Reset Session Log. The level of detail depends on the configuration setting. For details on setting the logging level, see the section "Configuring the Ruleset Parameters" on page 262.

To view the Reset Session Log, click the **View Log** button on the Reset Session detail page.

The Reset Session Log contains three sections - the Error Messages section, the Warning Messages section, and the Informational Messages section.

Error Messages

The Error Messages section contains the details of any errors encountered by the Reset.

Warning Messages

The Warning Messages section contains any warning messages generated by the Reset.

Informational Messages

The Informational Messages section captures the running details of the Reset - the number of successful operations, details on the preparation steps that occur during the Initializing phase, and a summary of the number of errors encountered during the Reset.

Refreshing the Reporting Database After the Reset

After you have performed an Object Reset, it is highly recommended that you refresh the Reporting database so that users who run third-party reports will immediately see the changes.

If your users are using the real-time reporting schema, you do not need to perform a reporting schema refresh. The IBM OpenPages reports will automatically see the changes. If you are still using the datamart reporting schema, you will need to manually update the reporting schema

For detailed information on performing a reporting database refresh, see "Administering the Reporting Schema" on page 59.

Exporting Rulesets to an XML File

You can export all of the Object Reset rulesets to an XML file using ObjectManager. In order to do this, you must have file access to the IBM OpenPages application server.

This will export ALL defined rulesets. Exporting rulesets does not remove them from the IBM OpenPages application - they will still be available for use after they are exported.

1. Back up the `ObjectManager.properties` file.

   Note: The ObjectManager.properties file is located in the root installation folder of your IBM OpenPages installation. By default, this is `c:\OpenPages`.
2. Open the `ObjectManager.properties` file in a text editor.
3. Locate the following block of settings in the file:

```
configuration.manager.dump.modules=true
configuration.manager.dump.file.types=true
configuration.manager.dump.bundle.types=true
configuration.manager.dump.file.upload.content.types=true
configuration.manager.dump.jsp.based.content.types=true
configuration.manager.dump.content.type.relationship.sets=true
configuration.manager.dump.app.permissions=true
configuration.manager.dump.actors=true
configuration.manager.dump.actor.group.memberships=true
configuration.manager.dump.actor.object.profile.associations=true
configuration.manager.dump.non.form.based.resources=true
configuration.manager.dump.form.based.content.types=true
configuration.manager.dump.form.based.resources=true
configuration.manager.dump.channels=true
configuration.manager.dump.resource.sets=true
configuration.manager.dump.associated.resources=false
configuration.manager.dump.rule.sets=true
configuration.manager.dump.rule.set.execute.sessions=true
configuration.manager.dump.registry=true
configuration.manager.dump.object.profiles=true
configuration.manager.dump.locales=true
configuration.manager.dump.application.string.key.categories=true
configuration.manager.dump.application.string.keys=true
configuration.manager.dump.application.strings=true
configuration.manager.dump.error.strings=true
configuration.manager.dump.object.strings=true
configuration.manager.dump.job.types=true
configuration.manager.dump.currency.exchange.rates=true
configuration.manager.dump.currencies=true
configuration.manager.dump.query.definitions=true
```

4. Modify each line to have a `false` value, except the line that reads:

```
configuration.manager.dump.rule.sets=true
```

5. Make sure that the following setting has a value of `false`:

   ```
   configuration.manager.migrate.configuration.objects
   ```

6. Once you have finished your modifications, save the file and exit the editor.
7. Open a Command Prompt window.
8. Navigate to the `<OP_Home>` directory.

   Where:

   `<OP_Home>` is the installation location of the OpenPages application. By default, this is `c:\OpenPages`.

9. Run the following command on a single line:

   ```
   ObjectManager dump config OpenPagesAdministrator  <password>
   <path-to-xml-file> <file-identifier>
   ```

   where

   <password> is the password to the OPAdminstrator user account.

   <path-to-XML-file> is the full path to the ruleset file you created.

   <file-identifier> is the portion of the ruleset file name preceding "-op-config.xml". When the XML file is created, the file name will append "-op-config.xml" to the end of the filename. For example, if you specified a <file-identifier> called "ruleset", the generated XML file would be named "ruleset-op-config.xml".

10. A new XML file is generated in the specified location that contains only the latest version of the rulesets that exist in the application at the time of the export.

Note: Be sure to "reset" the ObjectManager.properties file to its original contents - otherwise, your scheduled backups using ObjectManager will only export the rulesets.

Chapter 13. Configuring Settings

This chapter contains information about the various settings you can configure for the IBM OpenPages application.

About the Settings Page

The Settings page in the application contains a structured collection of name-value pairs used to store non-machine specific configuration data that spans across load-balanced systems. Settings are organized in a folder hierarchy by category with each name-value pair having a unique full path name.

Note: The add and copy buttons on the Setting list view page are for OpenPages Services and Support use only**.**

The top-level folder categories are:

- Applications - contains settings related to application and object specific behaviors.
- Common - contains settings that are common to both the application and platform.
- Platform - contains settings related to the system such as workflow, reporting, and the repository.
- User Preferences - contains settings related to users, such as alert behavior.

You can make changes to the value of a configuration "setting" (a name-value pair) without having to restart system services.

This section highlights the most commonly used configuration settings. For information about changing the value of settings that are not listed in this section, contact your IBM representative for details.

Accessing the Settings Page

Note: To access the **Settings** menu item, you must have the **Settings** application permission set on your account (for details, see "Configuring Application Permissions" on page 18).

Procedure

1. Log on to the IBM OpenPages application with an account that has the **Settings** application permission set.
2. From the navigation bar, select **Administration** and click **Settings**.

   From the **Settings** list view page, you can:
   - View summary information about settings
   - Access the detail page of a setting

Applications Folder Settings

The settings listed in this section represent a selected list of individual settings that are under the OpenPages Applications folder:

Modifying the Overview View Cache Capacity

To enhance performance on an Overview view page, you can change the maximum number of nodes that can be displayed to users in an Overview view by changing the value of the **Overview Cache Capacity** setting.

By default, the Overview Cache Capacity value is set to display 10000 nodes. If the number of nodes displayed exceeds the above setting, the additional nodes will not be displayed. Each cached object requires 1600 bytes of memory.

Procedure

1. Access the Settings page (see "Accessing the Settings Page").
2. Expand the **OpenPages | Applications | GRCM | Caches** folder hierarchy.
3. Click the **Overview Cache Capacity** setting to open its detail page.

4. In the **Value** box, type a new numeric value.
5. When finished, click **Save**.

Results

The new setting will take effect after you log out and log back in.

Configuring the Browser Cache

You can affect the behavior of the browser's **Back** and **Forward** buttons by changing the value of the **Disable Browser Cache** setting. By default, the browser's cache setting is enabled (the value is set to *false*).

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages** | **Applications** | **Common** | **Configuration** folder hierarchy.
3. Click the **Disable Browser Cache** setting to open its detail page.
4. In the **Value** box, if the value is set to:
   - **true** – the browser's cache is disabled; so using the **Back** button will sometimes require a refresh command for the page to display.
   - **false** - the browser's cache is enabled and no refresh action is required; however, the data on the page may be whatever was cached in the browser. This is the default setting value.
5. When finished, click **Save**.

Displaying the Accessibility Link

If you want to display a client-specific page with information about accessibility for disabled users, you can configure the display of the **Accessibility** link in the header pane of the IBM OpenPages application.

When a user clicks the Accessibility link, the designated page is displayed. By default, the Accessibility link is not displayed in the header pane of the application.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages** | **Applications** | **Common** | **Accessibility** folder hierarchy.
3. Click the **URL** setting to open its detail page.
4. In the **Value** box, type a URL (it is blank by default).
5. When finished, click **Save**.

Example

Let's say you created a page in HTML format that contained information about your company's accessibility policy for disabled users and wanted this policy to be available to all users through the application. Let's also say that the saved file is named "accessibility.htm" and was copied to the "custom_files" folder, which you created, under the /sosa folder location on the server, "machine1".

The URL path that you would enter in the Value box might look similar to this:

```
http://machine1:7009/openpages/custom_files/accessibility.htm
```

Displaying or Hiding Field Guidance

You can show or hide field-specific guidance on the Add or Edit page of an object through the **Show Field Guidance** setting. By default, the **Field Guidance** setting is set to display in the application. When a user clicks a question mark icon next to a specific field on an object's Add or Edit page, the field guidance text is displayed.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Set the value in the **Show Hidden Settings** setting to `true` (for details, see "Showing Hidden Settings" on page 273).
3. Expand the **OpenPages** | **Applications** | **Common** | **Configuration** folder hierarchy.
4. Click the **Show Field Guidance** setting to open its detail page.
5. In the **Value** box, if the value is set to:
   - **true** - the question mark icon and field guidance text will be displayed to users. This is the default setting value.
   - **false** - the question mark icon and field guidance text is hidden from users.
6. When finished, click **Save**.
7. `Reset the value` in the **Show Hidden Settings** setting `to false.`

Setting a Default Object View

If an object view for an object type is configured to display both a Folder View and Filter List View (displayed as tabs on the page), you can configure which tab is displayed first to users on the page through the **Default Object View** setting.

Note: For information about configuring Folder and Filter List views for an object type, see "About Folder View and Filtered List Views" on page 196.

By default, the **Default Object View** setting is configured to display the Filtered List View tab first.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages** | **Applications** | **GRCM** folder hierarchy.
3. Click the **Default Object View** setting to open its detail page.
4. In the **Value** box, if the value is set to:
   - **filter** – the Filter List View tab is displayed first to users. This is the default setting value.
   - **folder** - the Folder View tab is displayed first to users.
5. When finished, click **Save**.

Configuring File Check-out

The file check-out feature locks files to prevent other users from uploading and overwriting changes, or from moving, renaming, or deleting the file while a file is checked out. When the file is checked in, the lock is removed.

You can configure the display of the **Check Out** and **Check In** buttons by changing the value of the **Enable File Checkout** setting. By default, the setting is enabled (the value is set to *true*).

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | Applications | GRCM** folder hierarchy.
3. Click the **Enable File Checkout** setting to open its detail page.
4. In the **Value** box, if the value is set to:
   - **true** – the file check-out and check-in feature is enabled and the corresponding buttons are displayed on the detail page of a file. This is the default setting value.
   - **false** - the file check-out and check-in feature is disabled and the corresponding buttons are hidden.
5. When finished, click **Save**.

Creating and Deleting Custom Settings

When enabling new content types and creating your own reports, you may need to create your own custom setting within the OpenPages Settings menu.

By default, you cannot create or delete settings in the IBM OpenPages application, so you will need to enable the feature, and then create the new setting as described in the following instructions.

Enabling the Creation and Deletion of New Settings

Use the **Allow Create and Delete Settings** entry to enable or disable the **Add Setting** button on the Settings page. This button allows you to add and delete settings.

By default, the **Add Setting** button is disabled (the value is set to `false`).

Important: Do not delete any of the predefined settings shipped with IBM OpenPages . These settings are required and will cause unexpected behavior in the application if they are removed.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | Applications | Common | Configuration** folder.
3. Click the **Allow Create and Delete Settings** setting to display the Edit page.
4. In the **Value** box, change the value to `true` (the default value is `false`).
5. Click **Save**. The **Add Setting** button at the top of the page is enabled.

Creating a New Setting:

After enabling the **Allow Create and Delete Settings** setting, you can create custom settings entries in new or existing folders.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Verify that the **Allow Create and Delete Settings** entry is set to `true` (see "Enabling the Creation and Deletion of New Settings").
3. Navigate to the folder where you want to create the new setting and select the check box next to the folder.
4. Click the **Add Setting** button.
5. On the Settings detail page, do the following:

In this box...	Do this...
Setting Name	This field is required. Type a name for this setting.
Description	Type a description of the setting.
Value	Type a value for this setting

6. Select **Encrypted** if you want the value of the setting to be encrypted.
7. When finished, click **Create** to add the new setting to the current folder.

Deleting a Setting:

After enabling the **Allow Create and Delete Settings** setting, you can delete settings in new or existing folders.

Important: Do not delete any of the predefined settings shipped with IBM OpenPages . These settings are required and will cause unexpected behavior in the application if they are removed.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Navigate to the folder that contains the setting to be deleted and select the check box next to the desired setting. The **Delete** button should become active.
3. Click the **Delete** button. A confirmation dialog is displayed.
4. Click **OK** to delete the chosen setting.

Results

Note: If you select a folder, all settings within that folder will be deleted as well.

Configuring the Sort Order of Object List Views By Modification Date

Note: The information in this topic applies to IBM OpenPages GRC Platform 6.0.1.2 or greater.

You can use the **Sort by Modification Date** setting to globally configure the sorting behavior of objects in list views so that objects are listed by their modification date. By default, objects in a list view are listed by name.

Example

Let's say an object type has multiple associated objects. By default, associated objects are listed by name in a list pane on a Detail View page. However, users want to see associated objects listed by their last modified date. To globally change the sort order of objects in list panes so that objects are listed by the date they were last modified, you would set the value of the **Sort by Modification Date** setting to `true`.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages** | **Applications** | **GRCM** | **List View** folder hierarchy.
3. Click the **Sort by Modification Date** setting to open its detail page.

4. In the **Value** box, if the value is set to:
   - **true** - objects in a list view will be sorted by their last modification date.
   - **false** - objects in a list view will be sorted by name. This is the default setting value.
5. When finished, click **Save**.

Modifying the Deletion Interval for a Reporting Period

You can configure the number of days in which a reporting period can be deleted after it is created. By default, the interval is set to 7 days (after day 7, the reporting period can no longer be deleted).

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages** | **Applications** | **GRCM** | **Reporting Periods** folder hierarchy.
3. Click the **Delete Interval** setting to open its detail page.
4. In the **Value** box, edit the number of days you want for the new deletion interval.
5. When finished, click **Save**.

Showing Hidden Settings

Some settings within the OpenPages product are hidden to protect these settings from accidentally being modified. To display hidden settings so you can modify a particular setting, you will need to change the value in the **Show Hidden Settings** setting. By default, this value is set to `false` (hide).

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Set the value of the **Show Hidden Settings** setting to `true` (this will display all hidden settings) as follows:
   a. Expand the **OpenPages** | **Applications** | **Common** | **Configuration** folder hierarchy.
   b. Click the **Show Hidden Settings** setting to open its detail page.
   c. In the **Value** field on the setting detail page, change the value to `true` (the default value is `false`).
   d. Click **Save**.
3. Set the value of the **Allow Create and Delete Settings** setting to `true` as follows:
   a. Expand the **OpenPages** | **Applications** | **Common** | **Configuration** folder hierarchy.
   b. Click the **Allow Create and Delete Settings** setting to open its detail page.
   c. In the **Value** box, change the value to `true` (the default value is `false`).
4. Modify any hidden settings as necessary.
5. When finished, reset the value in the **Show Hidden Settings** setting to `false`.

Common Folder Settings

The settings listed in this section represent a selected list of individual settings that are under the OpenPages Common folder:

- "Excluding Characters From User Names"
- "Setting the System Security Model"
- "Disabling Access Control on Role Groups" on page 275
- "Optimizing File Uploads" on page 275

Excluding Characters From User Names

When you create user names, you can exclude the use of any alphanumeric and special characters, including spaces, through the **Illegal Characters** setting. For example, if you were to add an asterisk (*) as a value to this setting, the application would validate the user name for that character before it was created. If it detected an asterisk in the user name, such as Test*User, it would display an error message.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | Common | Security | User Name** folder hierarchy.
3. Click the **Illegal Characters** setting to open its detail page.
4. In the **Value** box, type any characters (including spaces and punctuations) that you want to be considered as invalid when creating a user name. For example, to include the asterisk (*) and ampersand (&) as invalid characters when creating a user name, you would enter *& in the Value box.
5. When finished, click **Save**.

Setting the System Security Model

During installation, by default, the security context point at which you can assign Role Templates to users on objects in the hierarchy is set at the Business Entity (`SOXBusEntity`) level. If wanted, you can extend the security context to other objects in the hierarchy to achieve a finer level of control by changing the **Model** setting.

Important:

This is a system-wide setting. Switching the security model after data is loaded (or migrated) into the system is not recommended and requires assistance from OpenPages Professional Services.

The syntax for the **Model** setting is: `SOXBusEntity/object_type-name`

Example

To create a security point for assigning Role Templates at a Process level, you would enter:

```
SOXBusEntity/SOXProcess
```

Permissions in the Role template could then be assigned at either the Business Entity or Process level, and would include any objects that were created beneath that security context point in the same location.

The maximum number of security context points you can have in the **Model** setting is 3. For example, `SOXBusEntity/SOXProcess/RiskAssessment`

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | Common | Security** folder hierarchy.
3. Click the **Model** setting to open its detail page.
4. In the **Value** box, enter the object type names you want to use as security points.
   For example, `SOXBusEntity/SOXProcess`
5. When finished, click **Save**.

Disabling Access Control on Role Groups

When a Role Template is disabled, you can use the **Disable Role Group** setting to globally control the security access of users and groups who were previously assigned that role.

By default, the value of the setting is 'false', which means that users and groups retain their access control and application permissions when a previously assigned role template is disabled.

A disabled role template is removed from the role assignment selection list and cannot be used for further role assignments.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | Common | Security | Role Templates** folder hierarchy.
3. Click the **Disable Role Group** setting to open its detail page.
4. In the **Value** box, type one of the following values:

If the value is set to...	Then...
true	Users and groups who were previously assigned that role, will lose their access control and application permissions.
false	Users and groups who were previously assigned that role, will retain their access control and application permissions. This value is set by default

5. Click **Save**.

Optimizing File Uploads

To enhance the performance of large files for upload to the OpenPages application, you can enable the **Optimized File Upload** setting.

When enabled, this feature:

- Compresses the selected file on the user's machine before uploading it to the IBM OpenPages repository.
- Displays additional 'Optimized File Upload' text and a **Browse and Save** button to users for attaching files.

Note: The file upload applet requires the Java Runtime Environment version 6 on the client browser.

By default, this value is disabled.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | Applications |Common** folder hierarchy.
3. Click the **Optimized File Upload** setting to open its detail page.
4. In the **Value** box, type one of the following values:

If the value is set to...	Then...
true	The Optimized File Upload **Browse and Save** button is displayed to users in addition to the standard file upload button.
false	Only the standard file upload button is displayed to users. This value is set by default.

5. When finished, click **Save**.

Platform Folder Settings

The settings listed in this section represent a selected list of individual settings that are under the OpenPages Platform folder:

- "Setting Localization Options"
- "Configuring Primary Associations" on page 277

Setting Localization Options

You can configure settings in the Globalization folder to audit translation label changes and set a default language for the IBM OpenPages application. The Globalization folder contains the following configuration settings:

About this task

Table 48.

Setting	Description
Auditing Enabled	Enable auditing of changes made to translated object and application label text. If the value is set to: • **true** - auditing is enabled. • **false** - auditing is disabled. By default, the value is **true**.

Table 48. (continued)

Setting	Description
Default Locale	Set the language in which the application user interface will be displayed to users by default. **Note:** Users can override the default locale setting by choosing another language through the **My OpenPages** , **My Settings** menu item on the navigation bar. The following is a list of the supported locale code values with their corresponding language: • **de_DE** (German) • **en_GB** (U.K. English) • **en_US** (U.S. English) • **es_ES** (Spanish) • **fr_FR** (French) • **it_IT** (Italian) • **ja_JP** (Japanese) • **pt_BR** (Brazilian Portuguese) • **zh_CN** (Simplified Chinese) • **zh_TW** (Traditional Chinese) The default installation locale value is **en_US**. To set, for example, the default language of the application interface so it displays information in German, you would type **de_DE** in the Value box.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages** | **Platform** | **Globalization** folder hierarchy.
3. Click a setting to open its detail page.
4. In the **Value** box, type a value.
5. When finished, click **Save**.

Configuring Primary Associations

When a child object has multiple parent objects, the **Association Heuristic** setting controls how the system reassigns a new primary parent to a child object that is disassociated from its primary parent object. You can change how primary parent objects are reassigned to disassociated child objects.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages** | **Platform** | **Repository** | **Resource** folder hierarchy.
3. Click the **Association Heuristic** setting to open its detail page.
4. In the **Value** box, type one of the following values:

If the value is set to...
Then...

Chronological
The reassignment of a primary parent is based upon the earliest creation date and time of an association.

This value is set by default.

Folder Context
The reassignment of a primary parent is based upon the folder path within the context of the business entity.

For example, let's say that control, C1, has multiple risk parents: R1, R2, R3, and R4 (primary parent) and the object associations were created in the following chronological order:

Parent Folder Path
C1 Child Folder Path

/BE1/SBE2/R2
/BE1/SBE1/C1

/BE1/SBE1/R1
/BE1/SBE1/C1

/BE1/SBE3/R3
/BE1/SBE1/C1

/BE1/SBE4/R4
(primary parent)
/BE1/SBE1/C1

If you disassociate the primary parent, R4, from C1, although R2 is chronologically the earliest association to C1, R1 will be reassigned as the primary parent. This is because R1 and C1's folder paths match (/BE1/SBE1).

Note: If no folder path matches the child object, then chronological order is used.

5. When finished, click **Save**.

User Preferences Folder Settings

The settings listed in this section represent a selected list of individual settings that are under the OpenPages User Preferences folder.

Setting Alert Notification Behavior

You can set which alert notifications are displayed, by default, to application users. The various alert notification settings that you can select are under the **Alerts** folder. Application users, if wanted, can change these default settings through their My Settings page.

Example

Let's say you configured dependent fields or dependent picklists for an object type and you want to alert users that different values for particular fields are available depending on their selection. Under the **Alerts** folder, you can set the values in the **Picklist Options Changed** and **Picklist Values Removed** settings to 'true', so each time a user changes a value in one of these fields, an alert notifying the user that values have changed is displayed.

By default, no alert settings under the **Alerts** folder are selected.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | User Preferences | Alerts** folder hierarchy.
3. Select the name of a setting you want under the **Alerts** folder to open its detail page.
4. In the **Value** box, type one of the following values:

If the value is set to...	Then...
true	An alert is displayed to application users.
false	No alert is displayed to application users. This value is set by default.

5. When finished, click **Save**.
6. To select another setting, repeat Steps 3 - 5.

Configuring Security Settings

The settings listed in this section represent a selected list of individual settings that are under the OpenPages Platform | Security folder:

- "Redirecting the IBM OpenPages Log Off Link"
- "Configuring Security for User Log On"
- "Setting the Cross-site Scripting Filter" on page 280
- "Configuring the Safe Tags Setting" on page 281

Redirecting the IBM OpenPages Log Off Link

By default, clicking the **Log Off** link in the header pane logs the user out of the IBM OpenPages application and displays the Log On page.

If you are using single sign-on (SSO), you can change the destination page by modifying the value of the **Logout URL** setting.

Note: If you are not using single sign-on, you cannot redirect the logout link. You will always return to the Log On page.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | Platform | Security** folder hierarchy.
3. Click the **Logout URL** setting to open its detail page.
4. In the **Value** box, type a fully qualified URL.
5. Click **Save**.

Configuring Security for User Log On

You can configure all or some of the following settings to prevent users from logging into the IBM OpenPages application.

Locking a user account prevents the user from logging into the IBM OpenPages application. The user is still an active user in the system, however, and can be selected through the user selector.

Users can be locked automatically if they exceed a set number of unsuccessful login attempts.

The **User Locking** folder contains the following settings that control the locking behavior of the IBM OpenPages GRC Platform application.

Setting	Description
Enabled	Sets whether the User Locking settings are active. When set to `true`, users will be locked after they unsuccessfully log in more than the allowed amount. Defaults to `false`.
Maximum Allowed Attempts	Sets the maximum number of times a user can unsuccessfully log in to the application before their account is locked. Defaults to '3'.
Timeout	Sets the amount of time (in minutes) that the user account will be locked after failing to log in. Defaults to 300 minutes.
Unsuccessful Login Window	Sets the amount of time (in minutes) that has to pass in order to reset the number of unsuccessful login attempts. Defaults to 120 minutes.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages** | **Platform** | **Security** | **User Locking** folder hierarchy.
3. Click a setting to open its detail page.
4. In the **Value** box, type a value.
5. When finished, click **Save**.

Setting the Cross-site Scripting Filter

Cross-site scripting (XSS) is a type of computer security vulnerability that allows malicious attackers to inject client-side script into web pages viewed by other users. You can use the **Cross-site Scripting Filter** setting to check all HTTP `GET` requests sent to the IBM OpenPages application server.

By default, the **Cross-site Scripting Filter** setting is enabled.

If you want to allow certain HTML elements or attributes to pass through this filter, see "Configuring the Safe Tags Setting" on page 281.

Note: When you change the value of this setting, you must restart all application servers in your cluster.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Set the value in the **Show Hidden Settings** setting to `true` (for details, see "Showing Hidden Settings" on page 273).
3. Expand the **OpenPages** | **Platform** | **Security** folder hierarchy.
4. Click the **Cross-site Scripting Filter** setting to open its detail page.
5. In the **Value** box, type one of the following values:

If the value is set to...	Then...
true	Cross-site filtering is enabled. This value is set by default.
false	Cross-site filtering is disabled

6. Click **Save**.
7. Restart all application servers in your cluster to effect the change. For details, see "Starting and Stopping OpenPages Application Servers" on page 465.

Configuring the Safe Tags Setting

When the **Cross-site Scripting Filter** setting is enabled (see "Setting the Cross-site Scripting Filter" on page 280), certain HTML elements will be blocked by that filter. You can use the **Safe Tags** setting to globally allow certain HTML elements to pass through the filter.

By default, the HTML `style` element is the only element allowed through the XSS filter. To allow additional HTML elements or attributes to pass through the filter, use the following instructions.

Example

Let's say your company uses embedded forms to capture information provided by users. The embedded form contains the HTML `form` element, which is passed in an HTTP request. By default, the **Cross-site Scripting Filter** setting is enabled so the `form` element will be blocked. To allow user input in an embedded form to be passed in an HTTP request, you would add the HTML `form` element to the **Safe Tags** value list as follows:

```
style, form
```

After you change the value of this setting, you must restart all application servers in your cluster to effect the change.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Set the value in the **Show Hidden Settings** setting to `true` (for details, see "Showing Hidden Settings" on page 273).
3. Expand the **OpenPages** | **Platform** | **Security** folder hierarchy.
4. Click the **Safe Tags** setting to open its detail page.
5. In the **Value** box, type the name of an HTML element or attribute.

   Note: Multiple values must be separated by a comma.
6. Click **Save**.
7. Restart all application servers in your cluster to effect the change. For details, see "Starting and Stopping OpenPages Application Servers" on page 465.

Selector Display Type Settings

This section contains the following topics for configuring actor selectors:

Configuring the Bucket Size of the Phonebook

You can use the **Bucket Size** setting to control the number of user names that are displayed in a bucket or category within the User Selector phonebook style pop-up dialog box. By default, this value is set to **10**. For information about the phonebook, see the topic "Modifying the Phonebook" on page 227.

The number of buckets that are displayed in the phonebook is determined by the size of the bucket and the number of users. For example, if there are 100 users and the bucket size is set to 20, the phonebook would display 5 buckets of 20 users per bucket.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | Applications | Common | User Selector** folder hierarchy.
3. Click the **Bucket Size** setting to open its detail page.
4. In the **Value** box, type a numeric value for the number of users you want displayed per bucket. By default, the value is set to 10.

   Note: If the value of the bucket size is set to zero or a negative number (such as -5), all users will be displayed in a single bucket.
5. When finished, click **Save**.
6. To configure the columns that are displayed in a selector dialog box, see "Configuring Display Columns in a Selector Dialog Box."

Configuring Display Columns in a Selector Dialog Box

For all selector display types, you can use the **Fields** setting to configure additional display information for users and groups. For information about selector dialog boxes, see the topic "Modifying the Selector Dialog Box" on page 227.

Note:

- The **Name** column is always displayed as the first column of the table and cannot be removed or changed. The **Name** column in a User Selector represents the user account name (Username). In a **Group** selector, it is the name of the group.
- If no values are present in the **Fields** setting, the **Name** and **Description** column headings are displayed by default.
- The values in the setting are globally displayed in the appropriate selector dialog box. For example, if you set the first name of a user to be displayed, the user's first name would appear in the User and User/Group dialog boxes but not the Group dialog box because the Group dialog box lists only groups (no users).

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | Applications | Common | Actor Selector** folder hierarchy.
3. Click the **Fields** setting to open its detail page.
4. In the **Value** box, type one or more of the following codes in the order in which you want the columns to display in a User, Group, or User/Group Selector dialog box:

To display this column heading...	Type this code...	Comments
Description	%DN;	Displays any description information from the "Description" object field on a User or Group Information page. This column heading is displayed by default in the User, Group, and User/Group Selector dialog boxes.
First Name	%FN;	Displays information from the "First name" object field on a User Information page. This column heading is displayed only in the User and User/Group Selector dialog boxes.
Last Name	%LN;	Displays information from the "Last name" object field on a User Information page. This column heading is displayed only in the User and User/Group Selector dialog boxes.
Email	%EM;	Displays the email address of a user from the "Email" object field on a User Information page. This column heading is displayed in the User, Group, and User/Group Selector dialog boxes.

5. When finished, click **Save**.

Example

To display the Email address of users followed by a description of the user, you would enter the following codes in the **Value** box: `%EM;%DN;`.

The result of these settings in the User Selector is that the **Name** column is followed by the **Email** and **Description** columns.

Configuring a User or Group Selector to Use the Search Function

If you have a large number of users and/or groups, you can improve performance by using the **Use Actor Search Only** setting to globally configure the User, Group, or User/Group Selector display type to open a search box instead of a phonebook style box.

By default, this value is set to always display buckets or categories of users and groups in a phonebook style box.

Procedure

1. Access the Settings page (see “Accessing the Settings Page” on page 268).
2. Expand the **OpenPages** | **Applications** | **GRCM** | **Detail Page** folder hierarchy.
3. Click the **Use Actor Search Only** setting to open its detail page.
4. In the **Value** box, type one of the following values:

If the value is set to...	Then...
true	A search box will open when a user clicks either the selector field box or a user or group icon.
false	A phonebook style box will open when a user clicks either the selector field box or a user or group icon This value is set by default.

5. When finished, click **Save**.

Configuring Menus

This section contains the following topics for configuring menus:

Modifying the Order of Menus on the Navigation Bar

The navigation bar on the IBM OpenPages application contains various menus that represent categories for grouping views and object types. You can use the **Items** setting to modify the order in which the main menus are displayed on the navigation bar.

Which categories for object types are available as menus on the navigation bar depends on your particular business solution.

By default, 'My OpenPages' is typically displayed as the first menu item on the navigation bar, and 'Administration' as the last menu item.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages** | **Applications** | **GRCM** | **NavigationMenu** folder hierarchy.
3. Click the **Items** setting to open its detail page.
4. In the **Value** box, modify the order of the menus as you want these to appear on the navigation bar.

   Note:
   - The list must be comma delimited.
   - The order in which the menus are defined in the list determines the order in which the menus are displayed on the navigation bar in the application user interface.

     Example

     In this example, the menus on the navigation bar will be displayed as follows: 'My OpenPages' followed by 'Reports', 'Organization', 'Remediation', and then 'Administration'.

     ```
     MyOpenPages,Reports,Organization,Remediation,Administration
     ```
   - The list must not have any leading or trailing spaces.
5. When finished, click **Save**.

Modifying Submenus

The navigation bar on the IBM OpenPages application contains various menus that represent categories for grouping views, object types, and system pages.

There are two types of menu items that you can add to a menu: object types and system pages.

Note:

- The list of submenu items must be comma delimited.
- Optionally use the `__separator__` (two underscores) keyword to organize submenu items into groups.

  The following example shows how to create two groupings of object types in a list.

  ```
  RiskAssessment,SOXRisk,__separator__,SOXControl,SOXTest,SOXTestResult
  ```

  The result is a list of submenu items that are grouped as follows:

  ```
  Risk Assessment

  Risk

  ____________

  Control

  Test

  Test Result
  ```
- The order in which the submenu items are defined in the list determines the order in which the submenu items are displayed in the selected menu on the application user interface.
- The list must not have any leading or trailing spaces.

Modifying Object Type Submenus

You can use the **ObjectTypes** setting to globally add or modify the various object type submenus that are displayed in the list for a specific menu.

Which object types are available as submenus depends on your particular business solution.

Example

Let's say you have a new custom 'Baseline' object type that must be added to the 'Assessments' menu, and then made available to users who are assigned the 'Analyst' profile. In this example, the 'Assessments' menu already contains the following object types in the submenu listing: Risk Assessment, Risk, Control, Test, and Test Result.

You want the new 'Baseline' object type to come after the Risk Assessments submenu item in the drop-down list. You also want the Risk Assessment and Baseline object types to be displayed in a separate group from the other object types in the list. Using the **ObjectTypes** setting, you would add the submenu item for the new 'Baseline' object type to the 'Assessments' menu as follows:

```
RiskAssessment,Baseline,__separator__,SOXRisk,SOXControl,SOXTest,SOXTestResult
```

To make the new object type available to users with the 'Analyst' profile, you would then modify the profile to include the new object type and then add the new object type to various navigational views.

Because this change is global, any other profiles that contain the 'Baseline' object type would also see this submenu item displayed under the 'Assessments' menu.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages** | **Applications** | **GRCM** | **NavigationMenu** folder hierarchy.
3. Navigate to the folder that contains the submenu items you want to modify (for example, 'Assessments') and then expand the folder to see its settings.
4. Click the **ObjectTypes** setting to open its detail page.
5. In the **Value** box, type the name of the object type where you want it to appear in the list.
6. When finished, click **Save**.
7. To view your changes in the browser, log out and then log back in to the application.
8. If wanted, add the new object type to a profile and views. For more information, see "Configuring Object Types in Profiles" on page 179, and "About Object Type Views" on page 194.

Modifying System Page Submenus

System page menus are menus that generally contain various functions but can also include object types. Some examples of system page menus are **My IBM OpenPages** and **Administration**.

You can use the **Subitems** setting to globally add or modify the various submenu items that are displayed in the list for a specific menu.

Which functions and object types are available as submenus depends on your particular business solution.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages** | **Applications** | **GRCM** | **NavigationMenu** folder hierarchy.
3. Navigate to the folder that contains the submenu items you want to modify (for example, 'Administration') and then expand the folder to see its settings.
4. Click the **Subitems** setting to open its detail page.
5. In the **Value** box, type the name of the item where you want it to appear in the list.
6. When finished, click **Save**.
7. To view your changes in the browser, log out and then log back in to the application.

Auto-Naming Settings

For most object types, you can auto-generate the names of newly created objects. This ability allows users to enforce internal naming policies and ensure unique object names.

The auto-generation of object names is controlled by a series of settings that can be accessed from the Settings menu item under the Administration menu on the navigation bar. It is possible to turn autonaming on or off for each object type individually. For example, you may want all business entities and processes named by users, but all risks, controls, and test plans named automatically by the IBM OpenPages application.

Note: Autonaming is not supported for the following object types: SOXDocument and SOXSignature.

This section contains the following topics for configuring auto-naming:

- "Configuring Auto-naming for an Object Type"
- "Configuring the Format of Object Names" on page 288

Configuring Auto-naming for an Object Type

You can configure auto-naming for an object type when an object is copied or created.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | Applications | GRCM | Auto Naming** folder hierarchy.
3. Navigate to the object type that you want to modify and then expand the folder to see its auto-naming settings.
   For each object type, you can modify the following settings:

Setting Name	Description
Auto-Named folder	
Copied Object	Determines whether or not copied instances of the selected object type are automatically named. If the value is set to: • **true** - auto-naming is enabled for copied instances. **Note:** Only the object that is directly selected for copy will be auto-named. Any child objects associated with the selected object will not be renamed, even if the 'Copied Object' setting is set to 'true' for these associated child objects. • **false** - auto-naming is disabled for copied instances. The default value is **false**.
New Object	Determines whether new instances of the object are automatically named. If the value is set to: • **true** - auto-naming is enabled for new instances. • **false** - auto-naming is disabled for new instances. The default value is **false**.

Setting Name	Description
Can be Edited	Determines whether the generated name can be edited during the creation process. If the value is set to: • **true** - the generated name can be edited. • **false** - the generated name cannot be edited. The default value depends on the object type.
Default Parent Name	If the created object has no parent, the value for this parameter will be used to replace the "%P;" variable in the generated name.
Format	Determines the format of the generated name. Additional details can be found in "Configuring the Format of Object Names."

4. Click a setting to open its detail page.
5. In the **Value** box, type a value.
6. Click **Save**.

Configuring the Format of Object Names

The **Format** setting allows you to incorporate some contextual information about the object, as well as an identifier in the object name.

You can use the variables described in Table 49 to format the auto-generated name.

Note:

- In addition to the variables, you can include any valid text in the autoname.
- The name of an object:
  - Must be 252 bytes or less.
  - Cannot contain forward slashes (/), backslashes (\), or the ellipsis character (...).

Table 49. Auto-naming Variables

Variable	Meaning
%P;	Will be replaced with the name of the parent of the new object. If the created object has no parent, the value of the default setting will be used.
%U;	Will be replaced with the creator's user name.
%Nn;	A unique sequentially generated numeric identifier. Where: n" specifies the amount of padding the number has. For example, %N3 might result in 001, 002, 003, while %N5 might result in 00001, 00002, 00003, and so forth.

Table 49. Auto-naming Variables (continued)

Variable	Meaning
%Rn;	A unique randomly generated alphanumeric identifier. Where: n" specifies the amount of padding the number has. For example, %R3 might result in T6d, while %N5 might result in T6d3fF, and so forth.

About Auto-generating Long Names

Be wary of nesting objects with auto-generated names too deep, as the generated names can "stack" with repeated use of the %P; variable.

For example, if you auto-generate the names of Processes, Control Objectives, Risks, Controls, and Tests using the %P; variable for all of them, the following will happen.

The Process Name will be Entity_Name - Process 001 (given the format string %P; - Process &N3;)

Using the same format through the rest of the object hierarchy, the name of the associated Control Objective is "Entity_Name - Process 001 - Control Objective 001" (the parent name plus the rest of the format string).

The Risk name would then be "Entity_Name - Process 001 - Control Objective 001 - Risk 001".

The Control name would then be "Entity_Name - Process 001 - Control Objective 001 - Risk 001 - Control 001".

And finally, the Test name is "Entity_Name - Process 001 - Control Objective 001 - Risk 001 - Control 001 - Test 001". (85 characters)

With repeated use of the %P; variable, the names can get extremely long. With longer naming conventions or the use of a multi-byte language, you could exceed the maximum length of an object name (252 bytes).

Naming Examples

Here are some examples of the various ways the variables can be used:

If we use a parent Process of "Hiring Practices" and a creator of "JSmith", and have the following settings:

Auto-Named value is set to **true**
Can be Edited value is set to **false**
Format value is set to **%P;_RIS_%N7;**
Default Parent Name has no value set

The auto-generated name is "Hiring Practices_RIS_0000001" and could not be edited.

Example 1:

For the auto-naming format parameter

Format is set to:%P;-Risk-%N5;

the generated Risk name is "Hiring Practices-Risk-00001".

Example 2:

Given a different auto-naming format parameter, such as
`Format is set to: Risk %N3; for %P; (%U;)`

would result in the generated name "Risk 001 for Hiring Practices (JSmith)"

Example 3:

Not all of the variables need to be used in an auto-generated name. For example,
`Format is set to: Risk %N4;`

results in "Risk 0001"

Example 4:

If the risk HAD no parent process, the value of **Default Parent Name** is used. In this case, the value
`Format is set to: %P;_RIS_%N7;`

results in "_RIS_0000001"

Signature and Lock Settings

This section contains the following topics for configuring signatures and locks:

Overview of Signatures and Locks

The IBM OpenPages application allows users to create "signatures" on objects. By itself, a signature is a merely a virtual "note" that signifies the user's agreement that the object meets with their approval. It has no enforcement powers, and does not prevent the item from being modified after approval has been given.

There are two ways in which signatures can be applied to an object: manually through the **Add** button, or automatically through a workflow task. Your IBM OpenPages system must be configured to support either method, and they are not exclusive - you can implement both ways, if desired.

A workflow signature is a signature that is created on an object as a direct result of a workflow being completed. If all other methods of creating a signature are disabled, the presence of a signature verifies that the necessary workflow was completed (and when). A manual signature is added through the object's detail page.

A signature lock is a lock placed on an object and its descendants that prevents the objects from being modified. The lock is activated by placing a signature on an

object; whether manually or automatically makes no difference. Once the signature is placed, the lock becomes active. The signed object and all of its associated child objects below it in the object hierarchy cannot be modified until the signature is revoked or an administrator removes the lock.

Only one active lock can be placed on an object. Multiple locks can be inherited from parent objects as those objects are locked.

The following sections explain how to implement signatures and locking behavior.

Configuring Signatures

There are two types of signatures you can enable or disable: automatic and manual signatures.

About Automatic Signatures

Automatic signatures are applied to an object as a result of a workflow task.

If a user is assigned a task to create a signature, completing the task results in a signature dialog box. Once the user fills out the dialog, the new signature is created on the object. For instructions on setting up automatic workflow signatures, see "Enabling Signatures for Jobs" in the *IBM OpenPages Workflow Authors Guide* .

About Manual Signatures

Manual signatures are added on the detail page of an obj. The Signatures table has Add and Revoke buttons at the top of the table. Users without the ability to add signatures to an object will not see the buttons. In order to add a signature to an object, the user must have Read privileges to the object.

When you configure the ability to manually add a signature to an object, you are actually granting a specific group of users permission to add a signature to an object type (such as Processes or Accounts). The group will be able to add a signature to any object of the proper type to which they have Read access.

To enable a user or group to add a signature or disable a user or group from adding a signature directly to an object, you need to configure the Permission setting for the desired object type. For details, see “Configuring Manual Signatures.”

Configuring Manual Signatures

When you explicitly add a group to an object type setting for signatures, the following occurs:

- Manual sign off is enabled for objects of that type.
- Users who belong to the specified group will have add and revoke signature links displayed on the Signatures Actions menu for the configured object type.

Note: Only groups that are explicitly named in the setting for a selected object type can manually sign off on objects of that type. Sub-groups of a named group do not inherit the sign-off permission.

Procedure

1. Access the Settings page (see “Accessing the Settings Page” on page 268).
2. Expand the **OpenPages | Applications | GRCM | Signature | Permission** folder hierarchy.

3. Click the name of the setting that corresponds to the object type to which you want to enable or disable a signature.
4. In the **Value** box on the setting detail page, do the following:
   - To enable one or more groups to manually add a signature to the selected object type, type a name of the group you want to add.

     Note: If you are entering multiple user groups, use a comma to separate group names, and do not use a space after the comma.

     For example, to add the groups Auditors and Managers to the sign-off list for Process object types, the value in the SOXProcess setting would look like this: **Auditors,Managers**
   - To disable one or more user groups from manually adding a signature to the selected object type, delete the group name.
5. When finished, click **Save**.
6. Repeat Steps 3-5 for each object type for which you want to enable or disable a manual signature for a group.

Configuring Signature Locks

The **Mode** setting controls whether a lock is created when a signature is added. When the Autolock value is set, adding a signature to an object will also create a lock on the object that prevents further changes from being made to the object and any object associated with it. Revoking a signature will remove the associated lock.

Note: When the locking feature is enabled, users can only create signatures on items to which they have Write privileges.

Configuring the Mode Setting

This **Mode** setting controls how signature locks are applied to objects. By default, this value is set to 'None' and objects are not automatically locked when a signature is added.

Note: If you want to enable cascading signatures (for details see, "Configuring Cascading Signatures" on page 293), the value must be set to **Cascade**.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | Applications | GRCM | Signature** folder hierarchy.
3. Click the **Mode** setting to open its detail page.
4. In the **Value** box, type one of the following values:

If the value is set to...	Then...
None	No lock is applied to the object when a signature is added. This is the value set by default.
Autolock	The object is locked when a signature is added. Only users with Write permission for an object can create a signature.
Cascade	Cascading signatures as specified in the **Cascade** setting are enabled for child objects (for details see, "Configuring Cascading Signatures" on page 293).

5. When finished, click **Save**.

Configuring Cascading Signatures

When a parent object has a signature added to it, you can automatically apply signatures to all of the associated objects underneath the signed object down the entire object tree. For example, signing a process would apply that signature to any sub-processes, accounts, risks, controls, and tests associated with the process. This feature is turned off by default, but can be enabled through the **Cascade** setting.

Note: To enable cascading signatures, the **Mode** setting must have the "Cascade" value set (for details see, “Configuring the Mode Setting” on page 292).

Procedure

1. Access the Settings page (see “Accessing the Settings Page” on page 268).
2. Expand the **OpenPages | Applications | GRCM | Signature | Cascade** folder hierarchy.
3. Click the name of the setting that corresponds to the parent object type to which you want to add or remove a cascading signature.
4. In the **Value** box on the setting detail page, do the following:
   - To add a cascading signature to child objects, type the name of the child object type.

     Note: If you are entering multiple child objects, use a comma to separate the names, and do not use a space after the comma.

     For example, to add a cascading signature to the Process object type for child sub-processes, accounts, and risks, the value in the SOXProcess setting would be: **SOXSubprocess,SOXAccount,SOXRisk**
   - To remove a cascading signature from child objects, delete the name of the child object type.
5. When finished, click **Save**.
6. Repeat Steps 3-5 for each object type you want to modify.

About Locking and Unlocking Objects

Locks can be applied to objects without the use of signatures.

If the **Lock** application permission is granted to a group, the group can create a lock on any object to which they have Write privileges (as long as they also have write privileges to all of the object’s associated objects down the hierarchy).

The **Unlock** application permission allows a user to unlock any locked object, as long as the user has Write permission to the object and all associated objects in the hierarchy.

Note: Unlocking an object using the **Unlock** button does NOT revoke the signature.

For information about object tree locking, see “Configuring Object Tree Locking” on page 295.

For information about globally unlocking business entities, see “Globally Unlocking Business Entities” on page 299.

Locking Access Privileges

By default, "Read" permission is required in order to be able to lock an object. This setting can now be configured through a new property in the *aurora.properties* file named "allow.locking.read.access". This property is set to 'false' by default.

When set to 'true', users with Read access to an object will be able to lock the object by adding a signature. The default value of 'false' requires that users have at least "Write" access to an object before they are allowed to lock it.

Configuring the Lock Button

You can configure the display of the **Lock** button for various object types through the **Display Lock Button** setting. This setting applies to manual and automatic signature locking. For details, see "Configuring the Lock Button for Object Types."

For users in a group to see the **Lock** button on the application user interface, the **Lock** application must be set on the user group. For details, see "Configuring the Lock Button for Display to Users."

Configuring the Lock Button for Object Types:

You can view or edit the list of object types for which the **Lock** button will be displayed.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Navigate to the **OpenPages | Application | GCRM | Locks** folder.
3. Click the **Display Lock Button** setting. The current list of object types that can be locked appears in the **Value** box.
4. In the **Value** box:
   a. To add an object type, type the name of the object type separated by a comma.
      For example: SOXBusEntity, SOXAccount, SOXSubaccount, SOXProcess, SOXSubprocess, SOXControlObjective, SOXRisk, SOXControl, SOXTest, SOXTestResult, SOXSignature, SOXIssue, SOXTask, SOXDocument, SOXExternalDocument.
   b. To remove an object type, delete the name of the object type from the list.
5. When finished, click **Save**.

Configuring the Lock Button for Display to Users:

For users in a group to see the **Lock** button on the application user interface, you must set the **Lock** application on the user group.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Select the group you want to open its detail page.
3. On the Group Information page, navigate to the **Permissions** tab.
4. Click **Edit**, and select the **Lock** application permission under Files.
5. When finished, click **Save**.

Configuring Object Tree Locking

About Object Tree Locking

Typically, users lock entire object hierarchies by either adding a signature (if Autolock is enabled) or clicking the **Lock** button on the detail page of an object.

You can, as an administrator, configure specified child object types to automatically lock whenever the parent object is locked using the **Lock Child Types** setting. If values in the **Lock Child Types** setting are specified, then the platform checks each object type for criteria settings. If criteria is not specified, then that particular child object will be locked as it is. For details, see "Locking Child Objects When a Parent Object is Locked."

If **Criteria** settings are specified for a child object type, then the child object will be locked only if the specified criteria is met. If no criteria is specified, then that particular child object will be locked as it is. For details, see "Specifying Optional Criteria for Locking Child Objects" on page 296.

For example, suppose you want to lock a business entity. The IBM OpenPages application would do the following to lock objects under a business entity (SOXBusEntity):

Procedure

1. The IBM OpenPages application would read the setting value for the *SOXBusEntity* key under the Locked Objects/Lock Child Types folder.
2. If a value is specified for *SOXBusEntity*, then for each of the object types listed in the value, the platform would check whether any criteria is specified for them under the Lock Child Types/Criteria folder.
3. If a criteria is not specified, then that particular child object will be locked as it is.
4. If a criteria is specified for a child object type, then that child object will be locked only if the specified criteria is met.
5. If the value obtained is step 2 is null or empty (value not specified for the SOXBusEntity setting), then only that particular business entity will be locked. None of its child objects would be locked.
6. If the SOXBusEntity (the key itself) setting does not exist, then the default Lock/Lock Object Types settings will come into effect. All the object types specified in it will be locked.

Results

If you were, for example, to specify the value for SOXBusEntity as *SOXProcess, SOXAccount*, then only the Process and Account child objects under that business entity would be locked.

The child objects of that process and account will not inherit any locks. If you want to lock their child objects too, then you would have to specify those object types in the value of the SOXBusEntity setting.

Locking Child Objects When a Parent Object is Locked

You can use the object type settings under the **Lock Child Types** folder to configure locks on child objects when a parent object is locked. If multiple child

object types are specified, then for each of the object types listed in the value, the platform checks whether any criteria for each listed object type is specified under Lock Child Types/Criteria setting.

For example, let's say you wanted to lock child Risk objects whenever a business entity is locked. You would enter SOXRisk in the setting Value box for SOXBusEntity. When a business entity is locked, users would not be able to add, associate, copy, and disassociate risks to the locked business entity. The child objects of that risk will not inherit any locks. If you want to lock its child objects too, then you would have to specify those object types in the value of the SOXBusEntity setting.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Navigate to the **OpenPages | Applications | GRCM | Locked Objects | Lock Child Types** folder.

   Make note of the exact object name (as listed under **Allowed Associations** folder) that you want to define.
3. Under the **Lock Child Types** folder, click a setting link that corresponds to the child object type for which you want to configure locks (for example *SOXRisk*).
4. In the **Value** box of the selected setting, enter the exact name of one or more child object types that should be locked when the parent object is locked.

   Note: If there are multiple child object types, you must add a comma to separate each object name. For example: SOXControl,SOXIssue,SOXDocument,SOXExternalDocument,SOXSignature
5. When finished, click **Save**.

Specifying Optional Criteria for Locking Child Objects

You can optionally define a single criterion (rule) for locking selected child objects during tree locking. You can define these rules in the **Criteria** setting. When applied, the system locks only those objects that satisfy the selection criteria.

For example, when a Business Entity is locked all child objects of a Business Entity, such as Accounts, are locked also. If you do not want to lock an Account object with a particular property value, you can set a criterion value in the **Criteria** setting for only the value you want locked. For instance, you can lock only Accounts that have an Account Type value of "Balance Sheet". All Accounts that have different values (such as "Income Statement", "Disclosure", or "Unknown") remain unlocked.

Note: There are no default criteria listed in the out-of-the-box IBM OpenPages schema.

Specifying optional criteria is a two-step process:

Procedure

1. Setting permissions to add new registry settings (see "Setting Permissions to Add New Settings")
2. Adding a criterion (see "Adding Criteria" on page 297)

Setting Permissions to Add New Settings:

To set your user permissions so you can add new settings, you need to set the value of the **Allow Create and Delete** setting to **true**.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Navigate to the **OpenPages | Applications | Common | Configuration** folder.
3. Click the **Allow Create and Delete** setting to open its detail page.
4. In the **Value** box, change the value to **true** to allow you to add new registry settings. (the default value is set to **false**).
5. When finished, click **Save**.

Adding Criteria:

Typically when a parent object is locked, all the child objects are locked also. However, you can configure certain child objects to remain unlocked even when the parent object is locked using criteria. Criteria are based on the property values of child objects.

For example, let's assume that a financial control Business Entity is being locked and you want its child accounts to be locked only if the value of the *Account Type* field is "Balance Sheet".

The instructions that follow use the example of how you could lock an Account object type with a particular property value of "Balance Sheet". All Accounts that have different values (such as "Income Statement", "Disclosure", or "Unknown") remain unlocked.

Note: To add new settings, the value of the **Allow Create and Delete** setting must be set to **true**. For details, see "Setting Permissions to Add New Settings" on page 296.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Navigate to the **OpenPages | Applications | GRCM | Locked Objects | Lock Child Types** folder.
3. Select the **Criteria** box and click the **Add Folder** button.

   Note: You must use this format to specify criteria:
   <child object type>/<parent object type>/Field Name
   <child object type>/<parent object type>/Operator
   <child object type>/<parent object type>/Value

   In this example, the *SOXAccount* (child object type) is located in the Criteria folder and *SOXBusEntity* (parent object type) is located in the SOXAccount folder, as indicated in Steps 4 - 6.
4. In the **Add Folder** box, enter a folder name for the child object type, and click **OK**. This example uses *SOXAccount* for the child object type folder name.
5. Under the newly created child object type folder (for example, *SOXAccount*), click **Add Folder** to add a parent object type folder.
6. In the **Add Folder** box, enter a folder name for the parent object type, and click **OK**. This example uses *SOXBusEntity* for the parent object type folder name.

7. Select the newly created parent object type folder (for example: *SOXBusEntity*), and then click the **Add Setting** button to specify criterion conditions for the child object type under the selected folder.

   Note: In this example, the folder is the *SOXBusEntity* folder. You will be adding three criteria conditions: a "Field Name", "Operator", and "Value" to this folder. Once the criteria are added, SOXAccount is locked only if its Account Type value is Balance Sheet.
8. In the **Settings** box:
   a. In **Setting Name**, type a name for the setting.
      For example: *Field Name*
   b. In **Value**, define a value for the *Field Name* setting in the format:
      <Field Group Name>.<Field Definition Name>
      For example: `OPSS-Account.Account Type`
      where:
      <Field Group Name> is `OPSS-Account`
      <Field Definition Name> is *Account Type*
9. Repeat Steps 7 and 8 to add an "Operator" criteria.
   To specify an Operator, define the **Setting Name** as *Operator* and the **Value** as =.

   Note: The allowed values for the Operator are **=**, **>**, **<**, **!=**, and **IN** (IN is used for the Enum-type property). Use commas to separate values in this property.
10. Repeat Steps 7 and 8 to add a "Value" criteria.
    To specify a Value, define the **Setting Name** as *Value* and the **Value** as *Balance Sheet*.
11. When you are finished with each criterion condition, click **Save**.

Results

Behind the scenes, the IBM OpenPages system reads the **Lock Child Types** setting for the parent *SOXBusEntity* as well as the child object type (*SOXAccount*) specified in its value. Then, the IBM OpenPages application checks for any defined criteria for each object type listed under the Lock Child Types for this object. If a criterion is specified and the condition is met, the IBM OpenPages system locks the child object type.

Enabling Buttons on Locked Associated Objects

You can enable associations of child objects, such as Risks or Controls, to their locked parent objects. You can define these child objects in the **Allowed Associations** setting. Specifically, the **Add New**, **Associate**, **Copy From**, and **Disassociate** buttons or menu items remain available to users on specific Associated object tabs of the parent object, as well as in the detail pages of the child objects.

For example, you can enable the SOXProcess and LossEvent child objects for SOXBusEntity so users can associate processes and loss events to a locked business entity. When enabled, the business entity detail page displays the Associate buttons (Add New, Associate, Copy From, and Disassociate) *only* on the Processes and Loss Events tabs. Note that the Associate buttons also display on the SOXProcess and LossEvent detail pages.

Configuring the Registry to Enable Associations of Child Objects

You can make objects available to users for association when a parent object is locked.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Navigate to the **OpenPages | Applications | GRCM | Locked Objects | Allowed Associations** folder.
3. Make note of the exact object name (as listed under Allowed Associations) that you want to define (for example *SOXRisk*).
4. Under **Allowed Associations**, click the name of a parent object type (such as SOXBusEntity).
5. In the **Value** box, enter the exact name of one or more child object types.

   Note: If you have multiple object types, you must add a comma to separate each object type name.
6. When finished, click **Save**.

Results

When a business entity is locked, users will be able to add, associate, copy, and disassociate risks to the locked business entity.

Note: The **Add New**, **Associate**, **Copy From**, and **Disassociate** buttons are disabled for all other object types in the system that are not defined in the **Allowed Associations** setting.

Globally Unlocking Business Entities

Administrators can enable a global unlock operation for business entities or sub-entities by enabling the **Remove All Tree Locks** application permission for designated groups of users. The Unlock All operation removes all direct and inherited locks on a business entity, including all of its children.

Note: When you enable the **Remove All Tree Locks** application permission for a group, the **Unlock All** button is displayed only on a business entity or sub-entity detail page.

Typically, you would use the Unlock All operation if

- The remove locks option was not selected after a finalized reporting period.
- Different business sub-entities of a multi-national organization have different reporting-period closure dates during the year. One sub-entity may need to remain locked while other entities are unlocked.

  For example:

  BE-US is a business entity representing the corporate office of a multi-national firm. BE-IND and BE-UK are two sub-entities within the BE-US entity. December is the financial closure period for BE-UK while March is the closure period for BE-IND.

  When BE-US is signed off in December, BE-IND and BE-UK remain locked along with their associated objects. Since December is the reporting-period closure date for BE-UK also, its reporting period is finalized. If the Unlock All operation is applied to BE-UK exclusively, users can keep working in the BE-UK object hierarchy while BE-IND and its hierarchy remain locked.

Setting a Global Unlock Permission

When loading buttons for a business entity or sub-entity detail page, the IBM OpenPages application checks whether the logged-in user has the **Remove All Tree Locks** application permission. If permissions are satisfied, the **Unlock All** button displays on the business entity or sub-entity detail page.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Create or select a group and navigate to its **Permissions** tab.
3. On the **Permissions** tab, click **Edit**.
4. Under **Files**, select **Remove All Tree Locks**.
5. When finished, click **Save**.

Object Reset Settings

Before performing an Object Reset, you can set the logging level, whether or not the Reset session should continue or halt if errors are encountered, if ACLs should be checked and locks ignored. In general, these settings will only need to be set once before your first time initiating an Object Reset, but you may wish to change them for different entity trees or ruleset behavior.

This section contains the following topics for configuring object resets:

Changing the Logging Level

The **Logging Level** setting controls how much information is displayed on the user interface. The Session Log captures detailed information regardless of the user interface display setting. You can change the logging information that is displayed on the user interface for a reporting period.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages** | **Applications** | **Common** | **Object Reset** folder hierarchy.
3. Click the **Logging Level** setting to open its detail page.
4. In the **Value** box, type one of the following values:

If the value is set to...	Then...
Low	Only error messages are displayed.
Medium	Both error and warning messages are displayed.
High	Errors, warnings, and any informational or diagnostic messages are displayed. This value is set by default.

5. When finished, click **Save**.

Continuing on Error

The **Continue on Error** setting determines whether the Object Reset session will log errors and continue to run, or whether the errors will be logged and the session halted. You can change whether the Object Reset session runs or halts processing when an error is encountered.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages** | **Applications** | **Common** | **Object Reset** folder hierarchy.
3. Click the **Continue on Error** setting to open its detail page.
4. In the **Value** box, type one of the following values:

If the value is set to...	Then...
true	Errors are logged and processing continues. This value is set by default.
false	Errors are logged and processing is halted.

5. When finished, click **Save**.

Obeying ACL Restrictions

The **Check ACL** setting controls whether the Object Reset occurs against all objects contained within the scope of the Reset session, or whether the Object Reset occurs against only those objects to which the user who initiated the Reset has access. You can change the scope of the Object Reset session.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages** | **Applications** | **Common** | **Object Reset** folder hierarchy.
3. Click the **Check ACL** setting to open its detail page.
4. In the **Value** box, type one of the following values:

If the value is set to...	Then...
true	Includes all objects within the scope of the Reset session. This value is set by default.
false	Includes only those objects within the Reset session to which the user has access.

5. When finished, click **Save**.

Obeying Locking Restrictions

The **Ignore Locks** setting controls whether existing locks on objects are honored or ignored when running an Object Reset. You can change whether or not locks are ignored during an Object Reset session.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).

2. Expand the **OpenPages | Applications | Common | Object Reset** folder hierarchy.
3. Click the **Ignore Locks** setting to open its detail page.
4. In the **Value** box, type one of the following values:

If the value is set to...	Then...
true	Locks on objects will be ignored when running the Reset session.
false	Locked objects will not be modified by the Reset session. This value is set by default.

5. When finished, click **Save**.

Copy Settings

This section contains the following topics for configuring copy operations:

Setting Copy Operations

You can optionally configure settings in the Copy Options folder to resolve duplicate names during copy operations and show additional copy options to users during a "Copy From" operation.

Note:

- During a copy operation for self-contained objects, if a naming conflict exists between the source and the target object, the copy operation will fail and the naming conflict resolution choices made by a user are ignored (see "About Self-Contained Object Types" on page 305).
- Self-contained object types and security context point object types do not respect the "copyof" naming option, if selected. By definition self-contained and security context point objects types automatically have their own folder, so no "Copy Of" prefix is required.
- In a 'Copy From' operation, the target folder path is based on the closest self-contained parent object.

The Copy Options folder contains the following configuration settings:

Table 50. Copy Operations Configuration Settings

Setting	Description
Conflict Policy	Set the default behavior of the copy operation when it encounters a duplicate object name during a copy operation. If the value is set to: • **overwrite** - a new version of the object in the target directory is created with all of the information of the copied object. All prior versions of the object in the target directory are maintained. • **copyof** - during the copy operation, any objects with the same name as an existing object in the target location will be renamed to "Copy of <objectname>". • **existing** - if a copied object has the same name as an object in the target location, that file will not be copied. All other objects (without duplicate names) will still be copied to the target location. **Note:** If you choose this option, you should examine the results of copy operations to determine whether any associations between objects have changed as a result of the copy. For example, if an associated risk is not copied to the new location because an existing risk has the same name, the copied parent process of the risk will be associated with the pre-existing risk in the target location. The default value is **overwrite**.
Show Copy Options Page	Allow users to select how duplicate names will be handled for the current copy. This setting displays the following options to users during a copy operation: • *Create a new version of the existing object in the destination directory.* This is the default selection. This option corresponds to the "overwrite" value in the Conflict Policy setting. • *Create new object whose name is prefixed with "Copy Of".* This option corresponds to the "copyof" value in the Conflict Policy setting. • *Do not copy resources with naming conflicts.* This option corresponds to the "existing" value in the Conflict Policy setting. If the value is set to: • **true** - the additional copy options are displayed to users. • **false** - no additional copy options are displayed to users. The default value is **false**.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | Applications | Common | Configuration | Copy Options** folder hierarchy.
3. Click a setting to open its detail page.
4. In the **Value** box, type a value.
5. When finished, click **Save**.

Cross-Context Sharing

You can use the **Cross context sharing** setting to affect whether any non-primary links to objects outside the context (scope) of a copy operation are included or ignored during a copy operation.

When cross-context sharing is enabled, copy operations will maintain non-primary links to objects outside the context of the copy. When it is disabled, non-primary links to objects outside the context of the copy are ignored.

Example

Let's say that in Figure 13, Control C1 was originally created under Risk R1, and R1 has a primary association to C1. Risks R2 and R3 have non-primary associations to C1. If a user copies Process P2 from BE2 to BE3, the link to C1 will be maintained if the **Cross context sharing** setting is enabled (set to 'true'). If the setting is disabled (set to 'false'), the copied tree will end at R3 as the non-primary association to C1 is outside the context of the copy operation. If the user copies P1 from BE1 to BE3, the current state of the **Cross context sharing** setting is irrelevant as the non-primary association from R2 to C1 falls within the context of the copy operation.

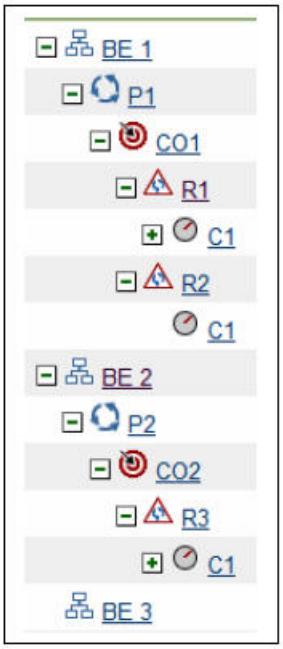


Figure 13. Sample Hierarchy

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Set the value in the **Show Hidden Settings** setting to `true` (for details, see "Showing Hidden Settings" on page 273).
3. Expand the **OpenPages** | **Platform** | **Repository** | **Resource** | **Copy** folder hierarchy.
4. Click the **Cross context sharing** setting to open its detail page.
5. In the **Value** box, type one of the following values:

If the value is set to...	Then...
true	Cross-context sharing is enabled and the copy operation will maintain any non-primary links to objects that are outside the scope (context) of the copy.

If the value is set to...	Then...
false	Cross-context sharing is disabled and the copy operation will ignore any non-primary links to objects that are outside the scope (context) of the copy. This value is set by default.

6. When finished, click **Save**.
7. `Reset the value` in the **Show Hidden Settings** setting `to false.`

Self-Contained Object Type Settings

This section contains the following topics for configuring self-contained object types:

- "About Self-Contained Object Types"
- "Configuring Settings for Self Contained Object Types" on page 306

About Self-Contained Object Types

A self-contained object type is an object type that has its own folder and is either part of the role-based security model (as defined in the **Model** setting "Setting the System Security Model" on page 274) or defined using the **Self Contained Object Types** setting "Configuring Settings for Self Contained Object Types" on page 306.

Note:

- Roles can only be assigned to objects that are defined as security context points through the **Model** setting.
- Defining an object type through the **Self Contained Object Types** setting does not automatically change the folders of existing instances of that type. If instances of the object type you want to define as self-contained already exist, you must contact your IBM representative for assistance in executing a special PL/SQL script that will go back and create folders for existing instances. This script is maintained by IBM OpenPages Customer Services & Support and does not ship as part of the product. Conversely, if an object type is later removed from the self-contained list, no automatic re-foldering occurs. All existing instances retain their dedicated folders.

By default, Business Entities are self-contained objects. For example, if the role-based security model setting is defined as SOXBusEntity/SOXProcess, both Business Entity and Process objects are treated as self-contained objects.

Self-contained object types behave differently than non-self-contained object types for copy, move, and rename operations. The characteristics that distinguish self-contained objects from non-self-contained objects follow.

Self-contained objects:

- Are always created under a parent folder that matches the object name (the same behavior as Business Entities). For example, a process 'P1' under the 'North America' business entity will have the path /North America/P1/P1.txt
- When copied, all the objects under its hierarchy will also be copied to the target.
- When moved, all the objects under its hierarchy will also be moved to the target.
- Can only be moved to an allowed parent object.
- Cannot be moved to a folder.

- Cannot have their parent folder edited, moved, or renamed.
- Can be renamed by users who have Read+Write access control (ACLs) permission.
- During a copy operation, if a naming conflict exists between the source and the target object, the copy operation will fail and the naming conflict resolution choices made by a user are ignored.

Configuring Settings for Self Contained Object Types

When you define an object type using the **Self Contained Object Types** setting, the behavior of that object type changes for copy, move, and rename operations (for more details, see "About Self-Contained Object Types" on page 305).

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | Common** folder hierarchy.
3. Click the **Self Contained Object Types** setting to open its detail page.
4. In the **Value** box, type a comma-separated list of object type names. For example, if you wanted Process and Risk Assessment object types, you would type: `SOXProcess,RiskAssessment`.
5. When finished, click **Save**.

Configuring Object View Settings

This section contains the following topics for configuring object views:

- "Home Page Settings"
- "Filtered List View Settings" on page 308
- "Listing Pane Setting" on page 309

Home Page Settings

For all profiles, you can globally configure the following Home page settings.

Ordering the Display of Pre-defined Tables

You can use the **Items** setting to globally change the order of how pre-defined tables are displayed on a Home page. The order of the items determines the order of the corresponding HTML tables.

The format and default order of items are:
`myTasks,myJobs,myCheckedOutFiles,myReports`

Where:

This item value...	Corresponds to this pre-defined table...
`myTasks`	My Tasks
`myJobs`	My Jobs
`myCheckedOutFiles`	My Checked-Out Files
`myReports`	My Reports

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).

2. Expand the **OpenPages | Applications | GRCM | Home Page** folder hierarchy.
3. Click the **Items** setting to open its detail page.
4. In the **Value** box, re-order the items as wanted.
5. When finished, click **Save**.

Defining the Number of Embedded Reports

You can use the **Maximum Embedded Reports** setting to globally change the maximum number of embedded reports that can be configured for a Home page.

By default, the value is set to display a maximum of 2 embedded reports.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | Applications | GRCM | Home Page** folder hierarchy.
3. Click the **Maximum Embedded Reports** setting to open its detail page.
4. In the **Value** box, type a number greater than zero.

   Note: Setting this value too high will negatively impact performance.
5. When finished, click **Save**.

Setting the Number of Objects Listed in a Table

You can use the **Maximum Objects** setting to globally control the maximum number of objects that can be listed for each table (excluding My Reports) on a Home page.

By default, the value is set to display a maximum of 5 listed objects per table.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | Applications | GRCM | Home Page** folder hierarchy.
3. Click the **Maximum Objects** setting to open its detail page.
4. In the **Value** box, type a number greater than zero.
5. When finished, click **Save**.

Setting the Number of Report Listings

You can use the **Maximum Reports Listing** setting to globally control the maximum number of reports that can be listed in the **My Reports** table on a Home page.

By default, the value is set to display a maximum of 5 listed reports.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | Applications | GRCM | Home Page** folder hierarchy.
3. Click the **Maximum Reports Listing** setting to open its detail page.
4. In the **Value** box, type a number greater than zero.
5. When finished, click **Save**.

Filtered List View Settings

You can globally configure the following Filtered List View page settings.

Note: If you are using the FastMap tool, in addition to configuring export settings on a Filtered List View page, you can also configure FastMap import settings to optimize performance. See "Optimizing FastMap Performance" on page 591.

Setting the Number of Objects for Export to Excel

You can use the **Maximum Export Size** setting to control the maximum number of objects that can be retrieved and exported to Microsoft Excel (in `.xls` format) from a Filtered List View page.

By default, the value is set to retrieve and export a maximum of 1000 objects.

If the number of objects being exported exceeds the defined number, then the user will be prompted to refine their filter.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages** | **Applications** | **GRCM** | **Filtered List** folder hierarchy.
3. Click the **Maximum Export Size** setting to open its detail page.
4. In the **Value** box, type a number greater than zero.
5. When finished, click **Save**.

Setting the Number of Concurrent Export Requests

You can use the **Concurrent Exports** setting to control the maximum number of Export to Excel (in `.xls` format) requests that will be handled at the same time.

By default, the value is set to 10.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages** | **Applications** | **GRCM** | **Filtered List** folder hierarchy.
3. Click the **Concurrent Exports** setting to open its detail page.
4. In the **Value** box, type a number greater than zero.
5. When finished, click **Save**.

Setting the Number of Objects Listed Per Page

You can use the **Page Size** setting to control the maximum number of objects that can be listed per page on a Filtered List View page.

By default, the value is set to display a maximum of 20 objects per page.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages** | **Applications** | **GRCM** | **Filtered List** folder hierarchy.
3. Click the **Page Size** setting to open its detail page.
4. In the **Value** box, type a number greater than zero.
5. When finished, click **Save**.

Listing Pane Setting

You can globally configure the following listing pane setting.

Setting the Number of Objects Listed

You can use the **Page Size** setting to control the maximum number of associated objects that can be listed in a child object listing pane on Detail View and Activity View pages.

By default, the value is set to 5. If the number of child objects that are returned exceed the set value, a 'Prev' and 'Next' link is displayed.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages** | **Applications** | **GRCM** | **List View** folder hierarchy.
3. Click the **Page Size** setting to open its detail page.
4. In the **Value** box, type a number greater than zero.
5. When finished, click **Save**.

Reporting Fragment Settings

For all profiles, you can globally configure the following settings for report fragment fields.

Setting Limits for Automatically Sized Reporting Fragment Pop-up Windows

Using the settings in this section, you can control the size of the pop-up window for report fragment fields in certain object views.

A report fragment pop-up window can be sized:

- Manually — by specifying the size of the pop-up on the field definition page of a report fragment field.
- Automatically — if no size is specified on the field definition page of a report fragment field, the pop-up window will be automatically sized using the settings in Table 51 on page 310.

Report fragment fields with a display type of 'On Demand' always display CommandCenter report components in a pop-up window.

For report fragment fields with a display type of 'Automatic', the display behavior varies depending on the object view:

- For Detail and/or Activity View pages — CommandCenter report components are always embedded directly into the cell of the report fragment field.
- For view pages that have a tabular format, such as List View, Folder View, and Filtered List View pages, and on the Classic tab on the Home page — CommandCenter report components are displayed in pop-up windows.

The sizing rules for report fragment field pop-up windows apply to both 'On Demand' and 'Automatic' display types used in List and/or Folder Views.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).

2. Expand the **OpenPages | Applications | Common | Report Fragments** folder hierarchy.
3. Click one of the following settings to open its detail page:

Table 51. Settings for Reporting Fragment Pop-up Windows

Setting	Description	Initial Value
Maximum Height	Sets the default maximum height allowable for a report fragment pop-up window.	375
Maximum Width	Sets the default maximum width allowable for a report fragment pop-up window.	575
Minimum Height	Sets the default minimum height allowable for a report fragment pop-up window.	250
Minimum Width	Sets the default minimum width allowable for a report fragment pop-up window.	350

4. In the **Value** box for the selected setting, change the existing value to a new number (must be greater than zero).
5. To change another setting value, repeat Steps 3 and 4.
6. When finished, click **Save**.

Reporting Framework V6 Generation Settings

This section contains settings for controlling reporting framework generation:

- "Enabling Reporting for Custom Forms"
- "Configuring Namespaces in the Reporting Framework" on page 311
- "Configuring Triangle Object Relationships" on page 315

Enabling Reporting for Custom Forms

In order to run CommandCenter reports against a custom object type (such as a custom form or survey), you must include the object type in the **Object Prefix** setting with a unique two-letter identifier. The framework generator will use the two-letter identifier as a prefix when creating columns in the real-time reporting schema tables.

As a best practice, we recommend you use `Z<n>` as a prefix for custom forms to avoid conflicts with future IBM OpenPages object types.

Where: `Z` represents the first letter of the prefix, and `<n>` represents an uppercase letter, such as 'A', 'B', 'C', and so forth (for example, `ZA`, `ZB`, `ZC`).

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | Platform | Reporting Framework V6 | Configuration** folder hierarchy.
3. Click the **Object Prefix** setting to open its detail page.
4. Add the new object type and prefix to the end of the current setting with a comma.
   Example
   In the following example, the new object type (in bold) is called 'CustomSurvey' and the prefix is 'ZA'.
   ```
   ...PROJECTACTIONITEM=PA,SOXSIGNATURE=SI,CUSTOMSURVEY=ZA
   ```

Note: The prefix must be entered as two upper-case letters, and must be unique - no other content type in the list can have the same prefix.

5. When finished, click **Save**.
6. Update the reporting framework model. For details, see "Updating the Reporting Framework" on page 64.

Results

Note: The following information applies only to systems that have been upgraded from versions of OpenPages 5.x or earlier and are using the Legacy Reporting Framework.

If you add a new custom form (such as a survey) and want reporting capability in both the Reporting Framework V6 and Legacy Reporting Framework, then you must also add the new prefix to the **Object Prefix** setting in the **OpenPages | Platform | Reporting | Framework | Generatio**n folder hierarchy for the Legacy Reporting Framework.

Configuring Namespaces in the Reporting Framework

If the supplied (out-of-the-box) namespaces in the generated IBM OpenPages Reporting Framework V6 do not meet your reporting requirements, you can define new namespaces that contain the required objects with the necessary relationships.

Note: For systems that have been upgraded from versions of OpenPages 5.x or earlier, see Appendix C, "Legacy Reporting Framework Generation Settings," on page 615 for information on configuring namespaces in the Legacy Reporting Framework.

About Namespaces

A namespace uniquely identifies a collection of query subjects and other objects (such as calculations) for satisfying reporting requirements. The IBM OpenPages CommandCenter reporting framework model contains one default namespace and, depending on your environment, non-default namespaces.

Table 52 on page 312 lists the entries that define a namespace in the IBM OpenPages Reporting Framework V6. Only the **Object Model** entry is required, all other entries are optional.

Important: Entries in a namespace must exactly match the names under the 'Entry Name' column in Table 52 on page 312.

Table 52. Entries that Define a Namespace

Entry Name	Required?	Comment
Is Default	No	This setting defines whether or not a namespace will be used as the default namespace in the IBM OpenPages data model. If the value is set to: • `true` - the namespace is set as the default namespace for use by generation logic, and is created first. **Note:** The data model can have only one default namespace. By default, the value of the `DEFAULT` namespace that is supplied by IBM OpenPages (out-of-the-box) is set to `true`. • `false` - the namespace is set as a non-default namespace.
Is Enabled	No	This setting defines whether or not a namespace is generated in the IBM OpenPages Reporting Framework V6 data model. If the value is set to: • `true` - the namespace will be generated when the framework model is updated. This is the default value. • `false` - the namespace will not be generated and any previously existing namespace will be removed.
Object Model	Yes	This setting contains your data object model (object relationships) . The IBM OpenPages Reporting Framework V6 generator uses the value pairs in this entry to define the parent-child relationships in the generated framework model.
Entity Recursive Object Levels	No	If one or more sets of recursive object levels are defined in the IBM OpenPages application, this setting provides the ability to specify which recursive object level set you want available in a given namespace. Multiple recursive object level sets must be separated by a comma. **Example** `ROL-1,ROL-2,ROL-3` For information on defining recursive object levels, see "Configuring Recursive Object Levels" on page 73.

The IBM OpenPages CommandCenter Reporting Framework V6 generator uses the definition of a namespace to create corresponding namespaces in the framework model.

If a relationship defined in a namespace matches a relationship that is defined in the object model, then the Reporting Framework V6 automatically creates a direct relationship between these objects.

About Naming Namespaces

Names of namespaces can be translated in application text. The following list contains best practices to keep in mind when naming namespaces.

- Keep namespace names short for readability (long names will wrap to another line).
- For consistency and compatibility with the reporting framework, use only the following characters when naming namespaces:
  - Uppercase letters
  - Numbers
  - Underscores (_)

  Examples : `MY_NAMESPACE` and `NAMESPACE101`

Configuring a New Namespace

The process for configuring a new namespace in the IBM OpenPages Reporting Framework V6 involves the following tasks:

"Add a New Namespace."

"Populate the Namespace with Entries."

Note:

- Only the `Object Model` entry is required.
- If you want reporting capability for object types that are in a triangle relationship and have configured the **Supported Triangle Relationships** setting, the paths between these object types must be reflected in the **Object Model** entry of a namespace. The namespace can be either new or existing. For details on configuring the **Supported Triangle Relationships** setting, see "Configuring Triangle Object Relationships" on page 315.

Add a New Namespace:

Use the following steps to add a new namespace to the IBM OpenPages Reporting Framework V6.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Set the value in the **Show Hidden Settings** setting to `true` (for details, see "Showing Hidden Settings" on page 273).
3. Expand the **OpenPages | Platform | Reporting Framework V6 | Models | OPENPAGES_FRAMEWORK_V6 | Namespaces** folder hierarchy.
4. Select the box next to the **Namespaces** folder, and then click the **Add Folder** button.
5. In the **Add Folder** box, type a name for the new namespace. For example, `MYCOMPANY_NAMESPACE`.

   The newly created namespace is represented by a folder icon under the **Namespaces** folder.

Populate the Namespace with Entries:

You can populate a namespace with the proper namespace entries by doing one of the following:

- "Creating Each Entry Separately" on page 314
- "Copying Entries from an Existing Namespace" on page 314

Note: The `Object Model` entry is required. Other entries from Table 52 on page 312 can be added to the namespace as wanted.

Once the reporting framework is updated with the new namespace, that namespace will be available in CommandCenter for reports.

Creating Each Entry Separately:

This method requires that you create and type the name of each entry you want.

Procedure

1. Verify that the **Allow Create and Delete Settings** setting is enabled (see "Enabling the Creation and Deletion of New Settings" on page 271).
2. Select the box next to the namespace you created in "Add a New Namespace" on page 313.
3. Click the **Add Setting** button.
4. On the **Settings** detail page, do the following
   a. In the **Setting Name** box, type `Object Model` (text must be exactly as shown).
   b. In the **Description** box, optionally type a description.
   c. In the **Value** box, type the values you want.

      The `Object Model` entry uses value pairs to reflect parent-child object relationships. The syntax is:

      ```
      <parent object>|<child object>,<parent object>|<child object>
      ```

      Example

      ```
      SOXBusEntity|SOXBusEntity,SOXRisk|SOXControl
      ```

   d. When finished, click **Save**.
5. If wanted, create additional namespace entries (see Table 52 on page 312 for a list) in the new namespace. Repeat Steps 2 - 4 substituting the name of the entry and values you want.
6. When finished, update the reporting framework model. For details, see "Updating the Reporting Framework" on page 64.

Copying Entries from an Existing Namespace:

This method involves using the copy operation to copy an entry from an existing namespace into the new namespace and then modifying the values of the copied entry as wanted.

Procedure

1. Navigate to an existing namespace and expand the selected namespace folder.
2. Copy the `Object Model` entry from the existing namespace into the new namespace created in task "Add a New Namespace" on page 313 as follows:
   a. In the existing namespace, select the box next to the `Object Model` entry.
   b. Click the **Copy To** button.
   c. In the copy window, select the name of the new namespace.
   d. Click **OK** to copy the entry from the existing namespace into the new namespace.
3. Modify the copied values in the `Object Model` entry as follows:
   a. Under the new namespace, click the `Object Model` entry to open its detail page.

b. In the **Value** box, modify the value pairs that reflect the parent-child object relationships you want.

   The syntax for adding parent-child object relationships is:

   ```
   <parent object>|<child object>,<parent object>|<child object>
   ```

   Example

   ```
   SOXBusEntity|SOXBusEntity,SOXRisk|SOXControl
   ```

c. When finished, click **Save**.

4. If wanted, copy additional namespace entries (see Table 52 on page 312 for a list) into the new namespace. Repeat Steps 2 and 3 substituting the name of the entry and values you want.
5. When finished, update the reporting framework model. For details, see "Updating the Reporting Framework" on page 64.

Editing Values in an Existing Namespace

If wanted, you can modify the values contained in an existing namespace so that the namespace satisfies your reporting requirements.

Important: We do not recommend changing the relationships of any IBM OpenPages supplied namespaces.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | Platform | Reporting Framework V6 | Models | OPENPAGES_FRAMEWORK_V6 | Namespaces** folder hierarchy.
3. Navigate to and expand the namespace folder you want to modify.
4. To change the value of an entry, do the following:
   a. Under the selected namespace, click the entry name to open its detail page.
   b. In the **Value** box of the selected entry, modify the values as wanted.
   c. When finished, click **Save**.
5. When finished, regenerate the framework model. For details, see "Updating the Reporting Framework" on page 64.

Configuring Triangle Object Relationships

To enhance report authoring capability, you can use the **Supported Triangle Relationships** setting to configure object types with triangle relationships in the Reporting Framework V6 relational data model.

About Triangle Object Relationships

A triangle object relationship exists when one child has two parents that are related to each other. Within the triangle, the "top" (parent 1) and "bottom" (child) object types are non-recursive, with the "middle" (parent 2) object type being recursive (such as Sub-Process).

A triangle relationship that includes two recursive object types is not supported.

Example

A report author has a requirement to create a Risk report that allows business users to access risks associated with various processes and sub-processes within their company.

To provide the report author with easier reporting capability in the framework model, you could configure a triangle relationship between the non-recursive child Risk object and its two related parents: a non-recursive parent Process object and a recursive parent Sub-Process object type, as shown in Figure 14.

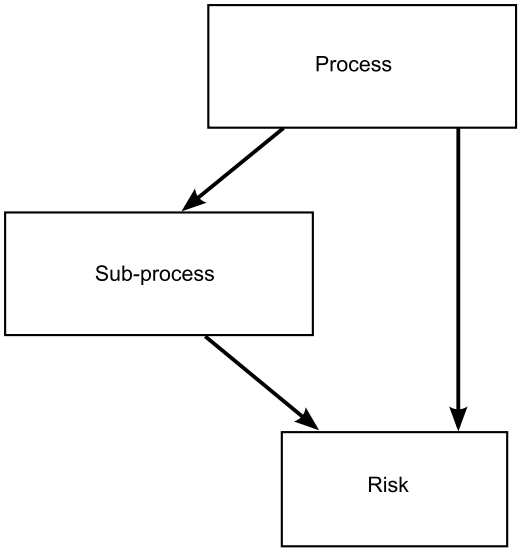


Figure 14. Triangle Object Type Relationships

Without the configured triangle, the report author would have to use advanced techniques that may not perform as well to accomplish this task.

Process Overview

Whenever you configure triangle object relationships in the reporting framework, you must perform the following tasks:

"Configure Triangle Object Relationships in a Namespace"

"Configure the Supported Triangle Relationships Setting" on page 317

"Update the Reporting Schema to Include the Configured Triangle Relationship" on page 317

"Update the Reporting Framework" on page 318

Configure Triangle Object Relationships in a Namespace

Note: If you have already configured triangle object relationships in a namespace, then skip this task.

The path between the objects forming a triangle relationship must be reflected in a namespace within the reporting framework.

For example, a namespace might have the following object type hierarchy configured for Business Entity, Process, Sub-Process, and Risk object types as follows:

```
SOXBusEntity|SOXProcess,SOXProcess|SOXSubprocess,SOXSubprocess|SOXRisk
```

To reflect the triangle relationship shown in Example 1 in Figure 14 on page 316, that namespace would have to be modified to also include the path between Process and Risk objects as follows:

```
SOXBusEntity|SOXProcess,SOXProcess|SOXSubprocess,SOXProcess|SOXRisk,
SOXSubprocess|SOXRisk
```

You can add triangle object relationships to a namespace.

For instructions on:

- Modifying an existing namespace, see "Editing Values in an Existing Namespace" on page 315.
- Adding a new namespace, see "Configuring a New Namespace" on page 313.

Configure the Supported Triangle Relationships Setting

Important: The spelling and case of the object type name must exactly match its system name. For example, you would type `SOXBusEntity` for the Business Entity object type. Using the wrong case for letters or using the label text will result in an error message.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | Platform | Reporting Framework V6 | Configuration** folder hierarchy.
3. Click the **Supported Triangle Relationships** setting to open its detail page.
4. In the **Value** box, use the following syntax to configure the three objects in a triangle relationship:

   ```
   Parent1|Parent2|Child
   ```

   Example

   ```
   SOXProcess|SOXSubprocess|SOXRisk
   ```

   Note: To enter multiple sets of triangle relationships, separate each triangle set with a comma.

   Example

   ```
   SOXProcess|SOXSubprocess|SOXRisk,Mandate|Submandate|Requirement
   ```
5. When finished, click **Save**.

Update the Reporting Schema to Include the Configured Triangle Relationship

There are two ways to update the reporting schema. You can either:

- Run the SQL script described in this procedure. This method incrementally updates the reporting schema with the triangle relationship configuration.
- Use the IBM OpenPages application user interface described in "Creating or Re-creating the Reporting Schema" on page 60. This method updates the entire reporting schema.

Note: We recommend running the following SQL script to incrementally update the reporting schema as it is much faster than using the application user interface method.

Procedure

1. Log on to a machine with SQL*Plus and access to the database server.
2. Run the following script:

```
begin
            OP_CONTEXT_MGR.ENTER_SINGLE_USER_MODE;
            OP_RPS_TRIANGLE_MGR.ADD_TRIANGLE_SUPPORT;
            commit;
            OP_CONTEXT_MGR.EXIT_SINGLE_USER_MODE;
end;
/
```

3. When finished, log out of SQL*Plus.

Update the Reporting Framework

When finished, regenerate the IBM OpenPages Reporting Framework V6 data model. For details, see "Updating the Reporting Framework" on page 64.

Reporting Framework Configuration Settings

This section contains settings for controlling reporting framework configuration:

- "Configuring Fact Types"
- "Configuring Legacy Reporting Framework Settings in Upgraded Systems" on page 319

Configuring Fact Types

A fact is typically a numeric field that can be aggregated. For each fact that is selected for inclusion in the dimensional model (see "Configuring Facts and Dimensions" on page 66 for details), you can use the **Fact Types** setting to globally control the types of aggregations that can be created for each configured fact field.

Table 53 lists the valid fact types that can be used for aggregation. When the reporting framework is generated, all the aggregation types specified in the **Fact Types** setting will be created for each fact selected for inclusion in the dimensional model. The aggregated facts are then grouped into a single measure dimension under each object type in the model where they were defined.

By default, the following fact types are configured: `SUM,AVG`.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | Platform | Reporting Framework V6 | Configuration** folder hierarchy.
3. Click the **Fact Types** setting to open its detail page.
4. In the **Value** box, type one or more of the following values.

   Note: If multiple values are specified, you must separate each value with a comma (for example: `SUM,MIN,MAX,AVG`).

Table 53. Valid Fact Type Values

This Fact Type...	Performs this summary function on a set of objects...
SUM	Totals the value of objects in the set.
MIN	Returns the smallest existing value of an object in the set.

Table 53. Valid Fact Type Values (continued)

This Fact Type...	Performs this summary function on a set of objects...
MAX	Returns the largest existing value of an object in the set.
AVG	Adds all values in the set and then divides by the count of existing values.
MED	Returns the median value of objects in the set.
STD	Returns the standard deviation of objects in the set.

5. When finished, click **Save**.

Configuring Legacy Reporting Framework Settings in Upgraded Systems

Note: The following settings are only available for systems that have been upgraded from IBM OpenPages 5.x or earlier.

Upgraded systems can generate two reporting frameworks:

- `OPENPAGES_REPORTS` - this is the legacy reporting framework and is available for backward compatibility for CommandCenter reports that have not been migrated to the new reporting framework
- `OPENPAGES_REPORTS_V6` - this is the new reporting framework, which has a new architecture with faster execution of CommandCenter reports

Enabling the Legacy Framework

You can control whether or not to generate the legacy reporting framework through the **Enable Legacy Framework** setting.

By default, the legacy framework is enabled for all upgrades.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | Platform | Reporting Framework V6 | Configuration | Legacy** folder hierarchy.
3. Click the **Enable Legacy Framework** setting to open its detail page.
4. In the **Value** box, type one of the following:
   - `true` - to enable the Legacy Reporting Framework
   - `false` - to disable the Legacy Reporting Framework
5. When finished, click **Save**.

Enabling Computed Fields in Reporting Framework V6

When the **Legacy Framework** setting is enabled, computed fields are, by default, executed against it. Object types that are listed in the **Object Types Using New Framework For Computed Fields** setting will use the new Reporting Framework V6 for computed field calculations.

By default, this setting is blank.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).

2. Expand the **OpenPages | Platform | Reporting Framework V6 | Configuration | Legacy** folder hierarchy.
3. Click the **Object Types Using New Framework For Computed Fields** setting to open its detail page.
4. In the **Value** box, type the name each object type containing computed fields.

   Note: If there are multiple object types, separate each object type with a comma.

   Example : `SOXBusEntity,SOXProcess,SOXIssue`
5. When finished, click **Save**. The change is effective immediately.

Reporting Schema Settings

Adding New Indexes

You can add a new index to any RT_ table in the database through the **Create Index on Fields** setting.

Prior to configuring this setting, we strongly recomment that you:

- Review this task with both your database administrator and your IBM representative.
- Test this change by manually creating the index in Oracle prior to making the permenant change in the IBM OpenPages GRC Platform application.

Note:

- You can only create a string up to 4096 characters.
- You should only configure this setting after careful analysis of your data query patterns. Adding too many indexes to a table can harm performance.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | Platform | Reporting Schema** folder hierarchy.
3. Click the **Create Index on Fields** setting to open its detail page.
4. In the **Value** box, enter an index in the following format:

   ```
   ObjectTypeName1= [FieldGroupName1.PropertyName1,...,FieldGroupNameN.PropertyNameN]
    |ObjectTypeNameN= [FieldGroupName1.PropertyName1
   ,...,FieldGroupNameN.PropertyNameN]
   ```

   Where:

   `ObjectTypeName1` is the name of the object type you want to add an index to.

   `FieldGroupName1` is a bundle definition associated with the object.

   `PropertyName1` is the name of a property in the bundle.

   Note:

   - Vertical bars (`|`) separate multiple index strings.
   - Commas (`,`) separates columns inside an index.
5. When finished, click **Save**.
6. Re-create the reporting schema.

Results

Depending on the size of the database, you can update the reporting schema through the application user interface or incrementally through scripts with assistance from your IBM representative.

For more details, see "About Updating the Reporting Schema" on page 60.

Example 1 - Adding an Index on Name and Reporting Period

Let's say you want to add an index on the Risk object type that includes the name and reporting period. The string would look as follows:

```
SOXRisk = [Core Attributes.Resource Name,
 Reporting Period Attributes.Reporting Period ID]
```

The `Core Attributes` bundle includes all of the following system parameters:

- `Latest Resource Version`
- `Resource Check Out Status`
- `Resource Check-in Date`
- `Resource Checked in By`
- `Resource Checked Out By`
- `Resource Content Type`
- `Resource Creation Date`
- `Resource Creator`
- `Resource Description`
- `Resource File Type`
- `Resource Full Path`
- `Resource ID`
- `Resource Name`
- `Resource Parent Folder`
- `Resource Subresource Type`
- `Resource Type`
- `Resource Visibility`

The `Reporting Period Attributes` bundle includes the following reporting period parameters:

- `Reporting Period ID`
- `Reporting Period Name`

Example 2 - Adding an Index on a Custom Field

Let's say you created a custom field called `Test Reviewer` on the Test object type and now want to add an index to this custom field. The index for the `Test Reviewer` custom field would be as follows:

```
SOXTest = [OpenPagesStandardTest.Test Reviewer]
```

Example 3: Adding an Index for Quick Filters and Custom Simple Strings

Indexes can help the performance of certain searches with Quick Filters and filters on custom simple string fields (except users and user groups).

The usual indexing technique is not applicable here, because Quick Filters and filters on custom simple string fields are commonly case insensitive and commonly implement "contains" logic. As such, even if a database index existed on the filtered field, it would not be used.

A typical use case is as follows:

- Filter performance appears inadequate.
- The user executing a filter has IBM OpenPages security access to a small fraction of the data.
- The number of records is high. This is a function of the number of object instances in the current reporting period and the number of reporting periods in the system.
- The width of records is high. This is a function of the number of custom properties.

For example, loss event data may be tightly restricted within a company. As such, indexing the LossEvent object type could improve filter performance.

```
LossEvent = [Reporting Period Attributes.Reporting Period ID,
             Core Attributes.Resource Parent Folder]
```

It is beneficial to filter on security access before applying any property filter. The security access filter will filter out a large percentage of data, leaving the property filter to work on fewer records.

Such an index will benefit all the filters on a given Object Type, so it only needs to be created once per Object Type.

Workflow Settings

This section contains the following topics for workflow configuration:

- "Setting the Display Size of the Workflow List"
- "Configuring a Mail Server for Workflow" on page 323
- "Configuring Workflow Actor Selectors" on page 323
- "Configuring Comments for Task Completion" on page 324

Setting the Display Size of the Workflow List

With the **Default Page Size** setting, you can control the number of workflow-related jobs and tasks that are displayed per page when a user clicks:

- The "Show All" button from the **My Tasks** and **My Jobs** tab on the Home page
- The **Jobs** or **Tasks** link under the Administration heading

By default, the number of workflow jobs and tasks that are displayed per page is 10.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | Platform | Workflow** folder hierarchy.
3. Click the **Default Page Size** setting to open its detail page.
4. In the **Value** box, type the number of jobs and tasks you want displayed per page.
5. When finished, click **Save**.

Configuring a Mail Server for Workflow

The following settings are used to configure your mail server and the sender's e-mail address for automatically generated remediation e-mails and standard (out-of-the-box) task messages.

Setting the Address of the Mail Server

You can use the **Mail Server** setting to configure your mail server so you can automatically send remediation e-mails and standard task messages from a workflow to users and/or groups.

By default, the mail server value is: *mail.yourcompany.com*

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | Platform | Workflow | Email** folder hierarchy.
3. Click the **Mail Server** setting to open its detail page.
4. In the **Value** box, type the name of your mail server and domain in the format provided.
5. When finished, click **Save**.

Setting the Sender's E-mail Address

You can use the **Mail From** setting to configure the sender's e-mail address for remediation e-mails and standard task messages automatically sent by a workflow to users and/or groups.

By default, the e-mail value is: *sysadmin@yourcompany.com*

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | Platform | Workflow | Email** folder hierarchy.
3. Click the **Mail From** setting to open its detail page.
4. In the **Value** box, type the name of the sender's e-mail address using a valid e-mail address and format.
5. When finished, click **Save**.

Configuring Workflow Actor Selectors

The following settings are used to configure user and/or group selectors for workflows.

Configuring the Reassign Task User Selector

By setting the minimum access value for users or groups in the **Associated Objects Minimum Access** setting, you can globally control which users or groups are displayed in the workflow task reassignment selection list.

The access values, listed in Table 54 on page 324, correspond to the type of permissions that each user or group must have for a related object. If a user or group has the minimum access that is specified in the setting, then that user or group will be displayed in the workflow task reassignment selection list.

Example

If the access value is set to 0, all users and groups are displayed in the task reassignment list. If the value is set to 3, only users or groups that have a

minimum of Read and Write permissions are displayed in the list (users or groups with Read only permission would be excluded).

By default, the **Associated Objects Minimum Access** value is set to 0 (all users and groups are displayed).

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | Applications | GRCM | Workflow | Actor Selector** folder hierarchy.
3. Click the **Associated Objects Minimum Access** setting to open its detail page.
4. In the **Value** box, type one of the following values:

Table 54. Minimum Access Values

If the access value is set to...	Then only users with these minimal permissions will be displayed in the task reassignment list...
0	All users and groups. This value is set by default.
1	Read
3	Read, Write
7	Read, Write, Delete
15	Read, Write, Delete, Manage
16	Associate
17	Read, Associate
19	Read, Write, Associate
23	Read, Write, Delete, Associate
31	Read, Write, Delete, Manage, Associate

5. When finished, click **Save**.

Configuring the Workflow Selector Starting Group

You can use the **Starting Group** setting to control which group displays at the beginning of the selection hierarchy.

By default, the starting group is set to `OpenPagesApplicationUsers`.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | Applications | GRCM | Workflow | Actor Selector** folder hierarchy.
3. Click the **Starting Group** setting to open its detail page.
4. In the **Value** box, type a valid group name.
5. When finished, click **Save**.

Configuring Comments for Task Completion

You can use the **Require Task Completion Comments** setting to configure whether or not a user is required to enter comments in the Comments box to complete an assigned workflow task.

By default, the value is set to `true` and comments are required to complete a task.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages** | **Applications** | **GRCM** | **Workflow** folder hierarchy.
3. Click the **Require Task Completion Comment** setting to open its detail page.
4. In the **Value** box, type one of the following values:

If the value is set to...	Then...
true	The **Comments** box is a required field for task completion. This value is set by default.
false	The **Comments** box is not a required field for task completion.

5. When finished, click **Save**.

Notification Manager Mail Server Settings

This section contains the following topics for mail server configuration:

- "Setting the Address of the Mail Server"
- "Configuring the Host Setting"

Setting the Address of the Mail Server

You can use the **Mail Server** setting to configure your mail server so you can automatically send e-mail notifications to users from your JSP-based reports or the Notification Manager utility.

Note: You can override this global setting by entering the name of a mail server in the notification 'Mail Server' parameter (for details, see "Creating a Notification" on page 597).

By default, the mail server value is: *mail.yourcompany.com*

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages** | **Applications** | **Common** | **Email** folder hierarchy.
3. Click the **Mail Server** setting to open its detail page.
4. In the **Value** box, type the name of your mail server and domain in the format provided.
5. When finished, click **Save**.

Configuring the Host Setting

Note: This setting is only used for backward compatibility.

If you have legacy or older JSP reports and want to send e-mail notifications to users from these legacy JSP-based reports or the Notification Manager utility, you must enable and configure the following settings.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).

2. Set the value in the **Show Hidden Settings** setting to `true` (for details, see "Showing Hidden Settings" on page 273).
3. Expand the **OpenPages** | **Platform** | **Publishing** | **Mail** folder hierarchy.
4. Click the name of a setting listed in the following table to open its detail page, and change the value as follows. Make sure to click **Save** after each setting change.

For this setting...	In the Value box on the setting detail page...
Enabled	Set the value to `true`.
From Address	Verify or enter the e-mail address of the sender using a valid e-mail address and format. By default, the value is: `sysadmin@yourcompany.com`
Host	Verify or enter the name of your mail server. By default, the value is: `mail.yourcompany.com`

5. `Reset the value` in the **Show Hidden Settings** setting `to false.`

Settings That Apply to Environment Migration

The environment migration settings are found in the **OpenPages** | **Applications** | **GRCM** | **Environment Migration** folder hierarchy.

For instructions on accessing the settings page, see "Accessing the Settings Page" on page 268.

Table 55. Environment Migration Settings

Setting	Definition
Asynchronous Timeout	The timeout value (in seconds) for AJAX calls on environment migration pages. The default is 120.
Export File Name Prefix	Prefix to be added to the environment migration export JAR file name. The default prefix `openpages` is used if no value is given. Prefix length is limited to 15 characters. If the prefix is longer than 15 characters, it is truncated. **Important:** • The following characters cannot be used in the prefix: `\ / | * : { } [ ] " ?` • Do not use the special characters as defined in CJK Compatibility Ideographs Unicode Block Name and the four-byte characters as defined in the CJK Unified Ideographs EXTENSION-B Unicode Block Name (such as 丈, 亡, 与, 乞, 丑, 工, 鵜, 腕, 氈, 鑓 and 鑓) in the Export File Name Prefix.
Process Log Report Page Spec	The location of the Process Log Report Page Spec. This value was previously fixed and can now be set. The default is `/_cw_channels/Reporting/Hidden Reports/CommandCenter/Administrative Reports/Environment Migration/Process Log Report.pagespec`

Table 55. Environment Migration Settings (continued)

Setting	Definition
Special Character Validation	Specifies whether or not special characters are checked while validating names of metadata. The default is **true**. Set to **false** to preserve legacy special character rules.

The **ImportConfiguration** and **ExportConfiguration** Application Permissions are required to allows members of user groups to access the environment migration tool for import and export. For details on these permissions, see " IBM OpenPages Application Permissions" on page 20.

For an overview of Environment Migration, see Chapter 17, "Migrating IBM OpenPages Environments," on page 479.

Chapter 14. Using Utilities

This chapter provides information about the utilities for backing up and restoring IBM OpenPages and CommandCenter files and databases, setting up a test environment, and purging the workflow database.

This chapter contains the following topics:

About the Backup and Restore Utilities

The Backup and Restore utilities are installed during the IBM OpenPages installation procedure.

They are available for backing up and restoring the IBM OpenPages environment:

- IBM OpenPages backup (OPBackup) and restore (OPRestore) — these utilities are used to backup and restore the IBM OpenPages application and database (see "Using the IBM OpenPages Backup Utility" on page 335 for details).
- CommandCenter backup (OPCCBackup) and restore (OPCCRestore) — these utilities are used to backup and restore IBM OpenPages CommandCenter files and Content Store (see "Using the CommandCenter Backup Utility" on page 343 for details).
- Users can choose to execute a live OPBackup. When running live OPBackup, OpenPages services are not restarted on the application server allowing for maximum uptime of OpenPages application. By default, OpenPages services will be restarted.

Note: Customers with database servers that are running the Oracle 11g Enterprise Edition must contact Oracle support and request the `p8795792_112010_Generic.zip` patch file before running the OPBackup and OPRestore and/or OPCCBackup and OPCCRestore utilities.

If this patch is not applied, the data import will fail with the following error messages:

```
ORA-39083: Object type INDEX failed to create with error:
ORA-14102: only one LOGGING or NOLOGGING clause may be specified
```

If you have already run your backup and need to restore data using that backup, contact your IBM representative for assistance.

Prerequisite: Oracle Admin Client

To use the IBM OpenPages -supplied backup and restore utilities, you must have the Oracle Admin Client software installed on both the IBM OpenPages application server and IBM OpenPages CommandCenter server machines.

Note: For the currently supported version of the Oracle Admin Client, see the *IBM OpenPages Release Notes* or refer to the *IBM OpenPages Installation* or *OpenPages Upgrade Guide* on your installation media.

About Oracle Data Pump

Oracle Data Pump provides a server-side infrastructure for very high-speed loading and unloading of data and metadata to and from the database.

Oracle Data Pump is used by the IBM OpenPages -supplied application and CommandCenter backup and restore utilities and was automatically configured during the IBM OpenPages Version 6.1.0 installation or upgrade process. If necessary, you can modify Oracle Data Pump settings.

Important:

- The Oracle Data Pump utility creates database backups on the database server. To ensure the database backups are available in the event of a server failure, make sure to copy these backup (dump) files to a different server or external device (such as a tape drive) once the OPBackup or OPCCBackup tool has completed.
- Before you use the CommandCenter backup utility for the first time, you must configure the Oracle Data Pump 'datapump' directory. You do this by running an SQL script. For details, see "Configuring or Updating the Oracle Data Pump Directory" on page 344.

  If you change the name or location of the 'datapump' directory, you can also use this script to update the configuration information.
- Oracle Data Pump commands IMPDP and EXPDP should be used as the IMP and EXP commands are not supported.

Configuring E-mail Notification for Backup Jobs

About E-mail Notification

If wanted, you can configure e-mail notification (which includes an attached log file) upon the completion of an IBM OpenPages application backup or CommandCenter backup job.

Note:

- Log files for e-mail notification are stored in the `logs` folder in the following location:
  - For OPBackup (IBM OpenPages application backup):

<OP_Home>|aurora|bin|logs with the timestamp on the log files.

– For OPCCBackup (CommandCenter backup):

<CC_Home>|tools|bin|logs with the timestamp on the log files.

- Make sure to set rules in your e-mail client to never send e-mails from the IBM OpenPages application server to the Spam or Junk mail folders.

Configuring Backup Job Notification

The following steps provide instructions for configuring e-mail parameters for IBM OpenPages application and CommandCenter backup jobs.

Procedure

1. Open a command or shell window and do one of the following.
   a. **For an OPBackup (IBM OpenPages application backup):**

      Navigate to the op-backup-restore.env file in the bin directory as follows.

      Where: <OP_Home> represents the installation location of the IBM OpenPages GRC Platform application.

      Windows <OP_Home>\aurora\bin

      By default <OP_Home> is C:\OpenPages

      AIX <OP_Home>/aurora/bin

      By default <OP_Home> is /opt/OpenPages

   b. **For a OPCCBackup (CommandCenter backup):**

      Navigate to the op-cc-backup-restore.env file in the bin directory as follows.

      Where: <CC_Home> represents the installation location of the CommandCenter application.

      Windows <CC_Home>\tools\bin

      By default, <CC_Home> is C:\OpenPages\CommandCenter

      AIX <CC_Home>/tools/bin

      By default, <CC_Home> is /opt/OpenPages/CommandCenter

2. Open the selected .env file in a text editor of your choice.
3. To configure e-mail notification, specify a value after the equal sign (=) for the following parameters (shown in Table 56) in the selected .env file:

Table 56. Backup E-mail Parameters

Parameter Name	Description
BACKUP_EMAIL_NOTIFICATION _SERVER=	The host name of the outgoing mail server.

Table 56. Backup E-mail Parameters (continued)

Parameter Name	Description
BACKUP_EMAIL_NOTIFICATION _TO_EMAIL_ID=	The name of one or more recipients that will receive the e-mail notification. The names appear in the `To:` field of the e-mail address. Multiple e-mail addresses must be delimited with a comma (,). **Note:** Do not enter a comma after the last e-mail address. **Example** emailid1@yourdomain.com,emailid2 @yourdomain.com
BACKUP_EMAIL_NOTIFICATION _FROM_EMAIL_ID=	The name that will appear as the sender of the notification e-mail in the `From:` field of the e-mail. The e-mail address will also be used as the personal name.
BACKUP_EMAIL_NOTIFICATION _SUCCESS_MSG_ FILE=BACKUP_SUCCESS_MSG.txt	The `BACKUP_SUCCESS_MSG.txt` is the default file containing the message text that will be used if the OPBackup.cmd completes successfully. You can modify the message text in the `BACKUP_SUCCESS_MSG.txt` file as wanted. The first line of the file is used as the e-mail's subject.
BACKUP_EMAIL_NOTIFICATION _FAIL_MSG_FILE= BACKUP_FAIL_MSG.txt	The `BACKUP_FAIL_MSG.txt` is the default file containing the message text that will be used if the OPBackup.cmd fails with errors. You can modify the message text in the `BACKUP_FAIL_MSG.txt` file as wanted. The first line of the file is used as the e-mail's subject.

4. Save the changes to the file and exit the editor.

Running Asynchronous Background Jobs and Administrative Functions

The IBM OpenPages GRC Platform supports asynchronous execution of processes in the background. The most common examples of these are FastMap web-based data import jobs, object resets, and reporting schema generation.

For example, once a user submits a data import file, that file is queued for loading and the import process occurs in the background. Since it is important that asynchronous background jobs run to completion, certain administrative operations in the application are suspended until all background jobs complete.

By default, the following administrative functions will not start until background jobs are completed:

- OPBackup command

- OPRestore command
- System Administrative Mode (SAM)

Note: To disable the default setting that checks for background jobs before starting OPBackup or OPRestore, see "Enabling and Disabling Asynchronous Background Processes Checking."

If asynchronous processes are found, error messages will be written to the opbackup restore log, such as:

```
-20001,'There are existing processes running. Please let them finish
or terminate them before proceeding.'
```

- or -

```
-20001,'There are existing object reset operations running. Please let
them finish or terminate them before proceeding.'
```

Example

The following is a sample error log message that occurred when an OPBackup command was initiated while the reporting schema was still being generated.

Note: The `.log` file name has the format `op_backup_<yyyy_mm_dd_hh_mm_ss>.log`

Where:

`<yyyy_mm_dd_hh_mm_ss>` represents the year_month_day_hour_minute_second. For example:

Windows	C:\OpenPages\openpages-backup-restore\ op_backup_2010_07_26_09_35_42.log
AIX	/opt/OpenPages/openpages-backup-restore/ op_backup_2010_07_26_09_35_42.log

A sample error log message follows.

```
can-proceed:
[exec] declare
[exec] *
[exec] ERROR at line 1:
[exec] ORA-20001: There are existing processes running. Please let them
finish or
[exec] terminate them before proceeding.
[exec] ORA-06512: at line 7
[exec]
[exec]
```

Enabling and Disabling Asynchronous Background Processes Checking

By default, the IBM OpenPages GRC Platform will not allow a backup (OPBackup) or restore (OPRestore) operation to start until all asynchronous background jobs run to completion.

Although we strongly recommend that all jobs run to completion before starting a backup or restore operation, this check can be enabled or disabled as follows.

Procedure

1. Open a command or shell window on the IBM OpenPages server.
2. Navigate to the `op-backup-restore.env` file in the `bin` directory as follows.

   Where: `<OP_Home>` represents the installation location of the IBM OpenPages GRC Platform application.

   Windows `<OP_Home>\aurora\bin`

   By default `<OP_Home>` is `C:\OpenPages`

   AIX `<OP_Home>/aurora/bin`

   By default `<OP_Home>` is `/opt/OpenPages`

3. Open the `op-backup-restore.env` file in a text editor of your choice.
4. Set the value of the `CHECK_BACKGROUND_PROCESSES` parameter in the file to one of the following:

If the value is set to...	Then...
true	The validation check for asynchronous background jobs is enabled and OPBackup/OPRestore will not start if background processes are still running. This is the default value.
false	The validation check for asynchronous background jobs is disabled and OPBackup/OPRestore will start even if background processes are still running.

5. When finished, save the changes to the file and exit the editor.

Encrypting Database Passwords in the Backup-Restore Utility Environment Files

Passwords used by the IBM OpenPages, workflow, and CommandCenter database user accounts within the backup-restore environment files are encrypted, by default, during installation. If you change the value of the password parameters within the following environment files, the new value will be in plain text until it is encrypted.

`op-backup-restore.env` database password parameters (file resides on the application server):

- `DB_SYSTEM_PWD=`
- `DB_SYS_PWD=`
- `DB_OP_PWD=`
- `DB_WF_PWD=`

`op-cc-backup-restore.env` database password parameters (file resides on the reporting server):

- `DB_SYSTEM_PWD=`
- `DB_CC_PWD=`

For security purposes, we strongly recommend that you encrypt the changed passwords by performing the following procedure.

Important: In a horizontal clustered environment, you must perform this procedure on each OpenPages Application Server in the horizontal cluster.

Procedure

1. To encrypt changed database password parameters in the `op-backup-restore.env` environment file, do the following:
   a. Open a command or shell window on the IBM OpenPages server.
   b. Navigate to the `bin` directory as follows:

      Where: `<OP_Home>` represents the installation location of the IBM OpenPages GRC Platform application.

      Windows `<OP_Home>\aurora\bin`

      By default `<OP_Home>` is `C:\OpenPages`

      AIX `<OP_Home>/aurora/bin`

      By default `<OP_Home>` is `/opt/OpenPages`

   c. Execute the following backup command:

      Windows `OPBackup.cmd secure`

      AIX `./OPBackup.sh secure`

2. To encrypt changed database password parameters in the `op-cc-backup-restore.env` environment file, do the following:
   a. Open a command or shell window on the reporting server.
   b. Navigate to the bin directory as follows:

      Where: `<CC_Home>` represents the installation location of the CommandCenter application.

      Windows `<CC_Home>\tools\bin`

      By default, `<CC_Home>` is `C:\OpenPages\CommandCenter`

      AIX `<CC_Home>/tools/bin`

      By default, `<CC_Home>` is `/opt/OpenPages/CommandCenter`

   c. Execute the following backup command:

      Windows `OPCCBackup.cmd secure`

      AIX `./OPCCBackup.sh secure`

Using the IBM OpenPages Backup Utility

OPBackup is the IBM OpenPages backup utility that backs up the necessary OpenPages files and database content on the server where it is run. The OPBackup utility creates a backup file that can be used by the OpenPages restore utility (OPRestore).

When you use the OPBackup utility, the following IBM OpenPages resources are backed up:

- The IBM OpenPages application and workflow databases

- The IBM OpenPages storage folder and its content
- The IBM OpenPages application environment files

Important: In a horizontal environment, if the IBM OpenPages Backup Utility is run on a non-administrative server, application and workflow databases will not be included in the backup. To include application and workflow databases in a backup file, run the IBM OpenPages Backup Utility on an administrative server.

Depending on your configuration, an OPBackup job may not start until all asynchronous background jobs run to completion (see "Running Asynchronous Background Jobs and Administrative Functions" on page 332).

Optionally, you can configure e-mail notification (with an attached log file) upon the completion of an OPBackup. For details, see "Configuring E-mail Notification for Backup Jobs" on page 330.

Modifying the Backup-Restore Environment File

The IBM OpenPages storage location is set during the installation process. Use the following scenarios to determine if you need to modify the `OPSTORAGE_LOCATION` parameter in the `op-backup-restore.env` file.

By default, the `op-backup-restore.env` file is located in the `bin` directory as follows: `<OP_Home>|aurora|bin`

Where: `<OP_Home>` represents the installation location of the IBM OpenPages GRC Platform application. By default, this is:	
Windows	`C:\OpenPages`
AIX	`/opt/OpenPages`

Scenario 1: The Root Installation Path of the IBM OpenPages Storage Location Changed After Installation

If you modify the root path of the IBM OpenPages storage location in the `storageservers` table after installation, make sure you update the `OPSTORAGE_LOCATION` parameter in the `<OP_Home>|aurora|bin|op-backup-restore.env` file to match the new root path (IBM OpenPages storage location).

If these locations do not match, the OPBackup utility will capture incorrect or stale storage folders.

Scenario 2: The OPBackup Utility is Running on a Non-Administrative Server

If your are running the OPBackup utility on a non-administrative server, you must update the `OPSTORAGE_LOCATION` parameter in the `<OP_Home>|aurora|bin|op-backup-restore.env` file on the non-administrative server to point to the remote location of the `openpages_storage` folder on the administrative server.

Make sure to use forward slashes as the path separator in this UNC path.

Example

```
//<host_server>/openpages_storage
```

Where:

<host_server> is the name of the administrative server.

Backing Up Custom OpenPages Files

Custom OpenPages files, such as SiteSync or scheduled job files that are custom to your environment, can be included in the backup using an OpenPages manifest file. A manifest file is a text file that contains the full path name to any directory or file that needs to be included in the backup.

Important:

- You must list all of your custom directories and files in a manifest. If you have any questions about the location of your custom data, contact OpenPages Customer Support.
- In a horizontal clustered environment, you must perform this procedure on each OpenPages Application Server in the horizontal cluster.

Procedure

1. Log on to the current OpenPages application server.
2. Navigate to the <OP_Home>|aurora|bin directory and open the op_backup.manifest file in a text editor.

   Where: <OP_Home> represents the installation location of the IBM OpenPages GRC Platform application.

   Windows <OP_Home>\aurora\bin

   By default <OP_Home> is C:\OpenPages

   AIX <OP_Home>/aurora/bin

   By default <OP_Home> is /opt/OpenPages

3. Enter the full path name to all custom directory name or a specific file. Each directory or file must be on a separate line in the file.
4. Save the manifest file using the current location and name.

Running the OPBackup Command

When you use the IBM OpenPages application backup utility, you run the OPBackup command in a command or shell window. The OPBackup command does the following:

- Stops all IBM OpenPages services before performing any backup operation
- Backs up IBM OpenPages application and environment files
- Exports the IBM OpenPages application database
- Restarts the services when the backup activities are complete

Note: Oracle Data Pump backup files are created on the database server.

See "Running a Live OpenPages Backup" on page 338 if you want to perform a backup without stopping services.

Procedure

1. Open a command or shell window on the IBM OpenPages server.
2. Navigate to the bin directory as follows:

   Where: <OP_Home> represents the installation location of the IBM OpenPages GRC Platform application.

Windows <OP_Home>\aurora\bin

By default <OP_Home> is C:\OpenPages

AIX <OP_Home>/aurora/bin

By default <OP_Home> is /opt/OpenPages

3. Execute the following backup command:

Windows `OPBackup <path-to-backup-location>`

AIX `OPBackup.sh <path-to-backup-location>`

Where:

Note: <path-to-backup-location> is the full path of the directory where the backed up files are located on the IBM OpenPages GRC Platform application server.

If a file path is not specified, the OPBackup command uses, by default, the backup location specified in the BACKUP_LOCATION parameter of the <OP_Home>|aurora|bin|op-backup-restore.env file.

The following table lists the default database export location for .dmp files specified in the environment file.

Where: <SID> is the Oracle System Identifier (for example, OP or OP11G).

If you purchased Oracle Database from...	For this operating system...	Then the default backup location on the database server is...
IBM (Oracle embedded installer)	**Windows**	c:\openpages_data\repository\server112_se_x64\admin\<SID>\dpdump
	AIX	/opt/openpages_data/repository/server112_se_x64/admin\<SID>/dpdump
A vendor other than IBM	**Windows**	<oracle_base>\admin\<SID>\dpdump
	AIX	<oracle_base>/admin/<SID>/dpdump

Running a Live OpenPages Backup

A live OpenPages backup means that the OpenPages application can continue running while the backup is in progress. OpenPages services are not stopped during the backup.

Note: Run live OpenPages backups during off-peak hours as the backup consumes processing resources.

It is possible to encounter the errors such as the following during the database export portion of the live OP backup:

```
[exec] ORA-31693: Table data object "OPENPAGES"."table_name"
       failed to load/unload and is being skipped due to error:
[exec] ORA-02354: error in exporting/importing data
[exec] ORA-01555: snapshot too old: rollback segment number #
       with name "rollback_segment_name" too small
```

This might happen if there is a relatively high level of data modification transactional activity on the system during the backup. Run live OP backup when transactional activity is low. If this is not possible or not desirable, or if the error keeps happening, it maybe possible to avoid this error by setting UNDO_RETENTION initialization parameter to a higher (possibly much higher) value, at least for the duration of the backup. Setting UNDO_RETENTION to a higher value, may result in a growth of UNDO table space, so it should be done by an experienced database administrator or with the assistance of IBM Support.

To use the IBM OpenPages application backup utility live, you run the OPBackup command with the nosrvrst option. This does the following:

- Backs up IBM OpenPages application and environment files
- Exports the IBM OpenPages application database

Note: Oracle Data Pump backup files are created on the database server.

Procedure

1. Open a command or shell window on the IBM OpenPages server.
2. Navigate to the bin directory as follows:

   Where: <OP_Home> represents the installation location of the IBM OpenPages GRC Platform application.

   Windows <OP_Home>\aurora\bin

   By default <OP_Home> is C:\OpenPages

   AIX <OP_Home>/aurora/bin

   By default <OP_Home> is /opt/OpenPages

3. Execute the following backup command:

   Windows OPBackup <path-to-backup-location> nosrvrst

   AIX OPBackup.sh <path-to-backup-location> nosrvrst

   Where:

   Note: <path-to-backup-location> is the full path of the directory where the backed up files are located on the IBM OpenPages GRC Platform application server.

   If a file path is not specified, the OPBackup command uses, by default, the backup location specified in the BACKUP_LOCATION parameter of the <OP_Home>|aurora|bin|op-backup-restore.env file.

   The following table lists the default database export location for .dmp files specified in the environment file.

   Where: <SID> is the Oracle System Identifier (for example, OP or OP11G).

If you purchased Oracle Database from...	For this operating system...	Then the default backup location on the database server is...
IBM (Oracle embedded installer)	**Windows**	`c:\openpages_data\repository\server112_se_x64\admin\<SID>\dpdump`
	AIX	`/opt/openpages_data/repository/server112_se_x64/admin\<SID>/dpdump`
A vendor other than IBM	**Windows**	`<oracle_base>\admin\<SID>\dpdump`
	AIX	`<oracle_base>/admin/<SID>/dpdump`

About OPBackup Generated Files

About the OPBackup Log File

The backup process creates a log file, which is identified by a unique name in the `<backup-directory-name>` folder. Each time you run the `OPBackup` command, a separate log file is generated.

About IBM OpenPages Backed-Up Content

The backup process creates a `ZIP` file (`.zip`) in the `<backup-directory-name>` directory. This `ZIP` file contains the necessary backed up data files including the database dump file.

Note:

- IBM OpenPages application database export files are created on the database server.
- If a backup file is very large (4 GB or larger), you should configure the OPBackup utility to use gzip (GNU zip). Gzip produces an archive with an extension of .tar.gz. To view and extract the contents of the archive file, use WinZip® 12 (or higher) or WinRAR® 3.71 (or higher).
- The OPBackup utility adds a military timestamp on the `.zip` and log files it creates.

The `ZIP` file can be used as a parameter to the `OPRestore` command to restore the installation-specific OpenPages files and the database. Each time the `OPBackup` command is run, a separate `ZIP` file is created and each data file is identified by a unique name.

Configuring OPBackup to Use GZIP

If a `ZIP` backup file grows beyond the 4-GB limit of ZIP file capacity, you can configure the OPBackup utility to use gzip (GNU zip). Once the file is configured, new backup files will have a `.tar.gz` extension. The OPRestore utility will detect if a file is in ZIP or gzip format and process it accordingly.

Procedure

1. From a command or shell window, navigate to the `op-backup-restore.env` file in the `bin` directory as follows.

Where: <OP_Home> represents the installation location of the IBM OpenPages GRC Platform application.

Windows <OP_Home>\aurora\bin

By default <OP_Home> is C:\OpenPages

AIX <OP_Home>/aurora/bin

By default <OP_Home> is /opt/OpenPages

2. Open the op-backup-restore.env file in a text editor of your choice.
3. Change the following setting in the file from false to true:
   USE_GZIP_COMPRESSION=true
4. Save the changes to the file and exit the editor.

Enabling and Disabling Storage Backup

By default, the IBM OpenPages GRC Platform backup includes the storage folder and its content. You can disable storage backup by setting the BACKUP_OP_STORAGE parameter in the op-backup-restore.env file.

Procedure

1. Open a command or shell window on the IBM OpenPages server.
2. Navigate to the op-backup-restore.env file in the bin directory as follows.
   Where: <OP_Home> represents the installation location of the IBM OpenPages GRC Platform application.

   Windows <OP_Home>\aurora\bin

   By default <OP_Home> is C:\OpenPages

   AIX <OP_Home>/aurora/bin

   By default <OP_Home> is /opt/OpenPages

3. Open the op-backup-restore.env file in a text editor of your choice.
4. Set the value of the BACKUP_OP_STORAGE parameter in the file to one of the following:

If the value is set to...	Then...
true	The storage folder and its content are backed up. This is the default value.
false	The storage folder and its content are not backed up.

5. When finished, save the changes to the file and exit the editor.

Using the IBM OpenPages Restore Utility

OPRestore is the IBM OpenPages restore utility that restores the necessary OpenPages files and database content on the server from which it was originally run. The OPRestore utility uses a backup file created by the IBM OpenPages backup utility (OPBackup).

Note: To refresh a "test" environment, see “Refreshing a Test Environment from Backup Files” on page 356.

As part of the restoration process, the following IBM OpenPages resources are restored:

- The IBM OpenPages application and workflow databases
- The IBM OpenPages storage folder and its content
- The IBM OpenPages application environment files

Important: In a horizontal environment, if IBM OpenPages backup is run on a non-administrative server, application and workflow databases are not included in the backup, so will not be restored.

Depending on your configuration, an OPRestore job may not start until all asynchronous background jobs run to completion (see “Running Asynchronous Background Jobs and Administrative Functions” on page 332).

Running the OPRestore Command

Note: If using Oracle Data Pump with IBM OpenPages 5.5.2.3 and higher — before you begin the restore operation — you must copy each database dump file (`.dmp`) that will be used by OPRestore from your backup location to the OpenPages backup directory on the database server.

Procedure

1. Stop the CommandCenter service if it is running.
2. From a command or shell window, navigate to the `bin` directory as follows:

   Where: `<OP_Home>` represents the installation location of the IBM OpenPages GRC Platform application.

   Windows `<OP_Home>\aurora\bin`

   By default `<OP_Home>` is `C:\OpenPages`

   AIX `<OP_Home>/aurora/bin`

   By default `<OP_Home>` is `/opt/OpenPages`

3. Execute the following command:

   Windows `OPRestore <backup-file-name> <path-to-backup-location>`

   AIX `OPRestore.sh <backup-file-name> <path-to-backup-location>`

   Where:

   `<backup-file-name>` is the name of the backup file (without the `.zip` or `tar.gz` file extension)

   Note: `<path-to-backup-location>` is the full path of the directory where the backed up files are located on the IBM OpenPages GRC Platform application server.

   If a file path is not specified, the `OPBackup` command uses, by default, the backup location specified in the `BACKUP_LOCATION` parameter of the `<OP_Home>|aurora|bin|op-backup-restore.env` file.

What to do next

Preferences related to the long string text index won't be exported by “Running the OPBackup Command” on page 337, and therefore are not restored. You must “Create a Long String Index” on page 374 pointing to the database server you are restoring to.

About OPRestore Log Files

The restore process creates a log file identified by a unique name in the `<backup-directory-name>` folder. Each time you run the `OPRestore` command, a separate log file is created.

Note: Oracle Data Pump log files for database imports are created on the database server.

Using the CommandCenter Backup Utility

OPCCBackup is the CommandCenter utility that backs up the necessary CommandCenter files and the Content Store. The OPCCBackup utility creates a backup file that can be used by the CommandCenter restore utility (OPCCRestore).

When you use the OPCCBackup utility, the following CommandCenter resources are backed up.

- CommandCenter reports
- Content Store
- Branding and environment files

Optionally, you can configure e-mail notification (with an attached log file) upon the completion of an OPCCBackup. For details, see “Configuring E-mail Notification for Backup Jobs” on page 330.

About Configuring Oracle Data Pump on First Time Use

Note: This task is required.

Before you use the CommandCenter backup utility for the first time, you must configure Oracle Data Pump by running an SQL script. For details on running the script, see “Configuring or Updating the Oracle Data Pump Directory” on page 344.

The script configures a ‘datapump’ storage directory for the user name specified in the <user_name> parameter. If a ‘datapump’ storage directory was already configured for the specified user name, the script will display an appropriate message.

About the CommandCenter File Storage Directory

By default, `OP_DATAPUMP_DIRECTORY` is the name of the directory used for storing CommandCenter Content Store database backup files. The path to this directory on the database server varies and depends on how it was defined.

If the `OP_DATAPUMP_DIRECTORY` storage directory does not already exist on the database server, you must run the script to create the directory.

Configuring or Updating the Oracle Data Pump Directory

Note: The script used in this procedure requires access to the following installation DVD: `OP_6.1_<Embedded|Non_Embedded>_DVD_1`

Use the following SQL*Plus script to:

- Create the Oracle Data Pump 'datapump' directory for **first time use** of the CommandCenter backup utility.
- Update configuration information if you modified the log file name or 'datapump' directory location to reflect changes in your environment.

Procedure

1. Log on to a machine with SQL*Plus and a connection to the CommandCenter database instance.
2. Open a command or shell window and do the following:
   a. Either navigate to the `OP_6.1_<Embedded|Non_Embedded>_ DVD_1` on your network drive or insert the DVD from your installation kit.
   b. Navigate to the following folder:
      `OP_6.1_Configuration|Database|UPGRADE_SCRIPTS|OP601X_TO_OP6100`
3. Run the `update-datapump-directory.sql` script as follows and substitute values for each parameter:

   ```
   sqlplus /nolog @sql-wrapper update-datapump-directory <log_file_name>
   <tns_name_alias> SYSTEM <password> <create|update> <directory_location>
   <user_name>
   ```

   Note: All parameters are required.

   Where:

This parameter...	Represents...
`<log_file_name>`	The user-defined name of the log file that the script will create and write information to. **Examples** **AIX** `/tmp/update-datapump.log` **Windows** `C:\temp\update-datapump.log`
`<tns_name_alias>`	The database TNS entry to be used by the CommandCenter database instance on the CommandCenter server machine.
`<password>`	The password for the Oracle `SYSTEM` user account.
`<create|update>`	Specify one of the following values: • `create` - use this if you are configuring Data Pump for first time use. • `update` - use this if you are modifying the `<Directory Location>` parameter.
`<directory_location>`	The full directory path on the database server where the backed up files will be placed.

This parameter...	Represents...
<user_name>	The user name to be used with the Cognos account for the CommandCenter Database Schema (Content Store).

Running the OPCCBackup Command

When you use the CommandCenter backup utility, you run the OPCCBackup command in a command or shell window. The OPCCBackup command uses Oracle Data Pump to export the database (services can continue to run during the backup).

Note: Oracle Data Pump backup files are created on the database server.

Procedure

1. From a command or shell window, navigate to the bin directory as follows:

   Where: <CC_Home> represents the installation location of the CommandCenter application.

   Windows <CC_Home>\tools\bin

   By default, <CC_Home> is C:\OpenPages\CommandCenter

   AIX <CC_Home>/tools/bin

   By default, <CC_Home> is /opt/OpenPages/CommandCenter

2. Execute the following backup command:

   Windows OPCCBackup <path-to-backup-location>

   AIX OPCCBackup.sh <path-to-backup-location>

   Where:

   <path-to-backup-location> is the full path of the directory where the backed up files are located on the CommandCenter server. The file path is optional.

   Note: If no file path is specified, the OPCCBackup command uses, by default, the backup location specified in the BACKUP_LOCATION parameter of the <CC_Home>|tools|bin|op-cc-backup-restore.env file.

   The following table lists the default Content Store database export location specified in the environment file.

   Where: <SID> is the Oracle System Identifier (for example, OP or OP11G).

If you purchased Oracle Database from...	For this operating system...	Then the default backup location on the database server is...
IBM (Oracle embedded installer)	**Windows**	c:\openpages_data\repository\server112_se_x64\admin\<SID>\dpdump
	AIX	/opt/openpages_data/repository/server112_se_x64/admin\<SID>/dpdump

If you purchased Oracle Database from...	For this operating system...	Then the default backup location on the database server is...
A vendor other than IBM	**Windows**	<oracle_base>\admin\<SID>\dpdump
	AIX	<oracle_base>/admin/<SID>/dpdump

About OPCCBackup Generated Files

About the OPCCBackup Log File

The backup process creates a log file, which is identified by a unique name in the <backup-directory-name> folder. Each time you run the OPCCBackup command, a separate log file is generated.

About CommandCenter Backed-Up Content

The backup process creates a ZIP file (.zip) in the <backup-directory-name> directory. This ZIP file contains the necessary backed up data files including the database dump file.

Note:

- Content Store database export files (.dmp) are created on the database server.
- If a backup file is very large (4 GB or larger), you should configure the OPCCBackup utility to use gzip (GNU zip). Gzip produces an archive with an extension of .tar.gz. To view and extract the contents of the archive file, use WinZip® 12 (or higher) or WinRAR® 3.71 (or higher).
- The OPCCBackup utility adds a military timestamp on the .zip and log files it creates.

The ZIP file can be used as a parameter to the OPCCRestore command to restore the installation-specific OpenPages files and the database. Each time the OPCCBackup command is run, a separate ZIP file is created and each data file is identified by a unique name.

Configuring OPCCBackup to Use GZIP

If a ZIP backup file grows beyond the 4-GB limit of ZIP file capacity, you can configure the OPCCBackup utility to use gzip (GNU zip). Once the file is configured, new backup files will have a .tar.gz extension. The OPCCRestore utility will detect if a file is in ZIP or gzip format and process it accordingly.

Procedure

1. From a command or shell window, navigate to the op-cc-backup-restore.env file in the bin directory as follows.

   Where: <CC_Home> represents the installation location of the CommandCenter application.

   Windows <CC_Home>\tools\bin

   By default, <CC_Home> is C:\OpenPages\CommandCenter

   AIX <CC_Home>/tools/bin

   By default, <CC_Home> is /opt/OpenPages/CommandCenter

2. Open the op-cc-backup-restore.env file in a text editor of your choice.

3. Change the following setting in the file from `false` to `true`:
   `USE_GZIP_COMPRESSION=true`
4. Save the changes to the file and exit the editor.

Using the CommandCenter Restore Utility

OPCCRestore is the IBM OpenPages CommandCenter utility that restores the necessary CommandCenter files and Content Store on the server from which it was originally run. The OPCCRestore utility uses a backup file created by the OpenPages CommandCenter backup utility (OPCCBackup).

Note: To refresh a "test" environment, see "Refreshing a Test Environment from Backup Files" on page 356.

As part of the restoration process, the following CommandCenter resources are restored:

- CommandCenter reports
- Content Store
- Branding and environment files

Command Center reports/Content Store/Branding and environment files.

Running the OPCCRestore Command

You can restore backed up CommandCenter data using the OPCCRestore utility as follows.

Procedure

1. Stop the CommandCenter service on the administrative server and any non-administrative servers in the cluster. For details, see "Starting and Stopping the CommandCenter Server" on page 474.
2. Stop the IBM Cognos Configuration tool, if it is running, on all cluster members.
3. From a command or shell window, navigate to the `bin` directory as follows:
   Where: `<CC_Home>` represents the installation location of the CommandCenter application.

   Windows `<CC_Home>\tools\bin`

   By default, `<CC_Home>` is `C:\OpenPages\CommandCenter`

   AIX `<CC_Home>/tools/bin`

   By default, `<CC_Home>` is `/opt/OpenPages/CommandCenter`

4. On the administrative CommandCenter server, execute the following command:

   Windows `OPCCRestore <backup-file-name> <path-to-backup-location>`
   AIX `OPCCRestore.sh <backup-file-name> <path-to-backup-location>`

   Where:

   `<backup-file-name>` is the name of the backup file (without the `.zip` or `tar.gz` file extension).

Note: <path-to-backup-location> is the full path of the directory where the backed up files are located on the CommandCenter server. The file path is optional.

Note: If no file path is specified, the OPCCRestore command uses, by default, the backup location specified in the BACKUP_LOCATION parameter of the <CC_Home>|tools|bin|op-cc-backup-restore.env file.

5. Start the CommandCenter service on the administrative server and on any non-administrative servers in the cluster. For details, see "Starting and Stopping the CommandCenter Server" on page 474.

About OPCCRestore Log Files

The restore process creates a log file identified by a unique name in the <backup-directory-name> folder. Each time you run the OPCCRestore command, a separate log file is created.

Note: Oracle Data Pump log files for database imports are created on the database server.

Using Oracle Online Database Backup (RMAN) for Point-In-Time Recovery

This section describes how to perform an online backup of the IBM OpenPages database, using custom OpenPages scripts that utilize Oracle's Recovery Manager (RMAN) facility.

This section assumes that the user is familiar with basic Oracle database backup and recovery operations, as well as use of RMAN. For links to Oracle user documentation on general use of RMAN for online database backup and recovery, see the following table.

Table 57. Oracle RMAN Documentation

Title	Link(s)
Oracle® Database Backup and Recovery User's Guide 11g Release 2 (11.2)	Introduction to Backup And Recovery Getting Started with RMAN Backup Area
Oracle® Database Backup and Recovery Reference 11g Release 2 (11.2)	RMAN Commands

About Oracle Online Database Backups

Unlike the IBM OpenPages OPBackup utility, the Oracle online database backup function does not require shutting down access to database operations before backing up the database. It can perform an incremental backup in the background at a designated interval while allowing full user access to the IBM OpenPages database and IBM OpenPages services. It also allows "point in time" recovery of the IBM OpenPages database with minimal chance of data loss.

In contrast, OPBackup and OPRestore can only do a full backup and restore of the database and other files (not incremental). Because full backups are typically

performed less frequently than incremental backups, the possibility of significant data loss in the event of a system crash is greater than for the Oracle online database backup and recovery solution.

Note:

- The Oracle online database backup function can only perform a physical bit-for-bit backup of a single IBM OpenPages database instance and only on one machine.
- Operation of online database backup in an Oracle RAC (cluster) environment is not supported.

In contrast, OPBackup performs a logical backup of all database instances in the cluster, as well as the IBM OpenPages storage directory and application environment files.

Running Oracle Online Database Backups (RMAN)

Setting up and running Oracle online database backups consists of these tasks:

"Plan the Size of the Backup Area"

"Copy the Online Backup Scripts to a Local Directory" on page 350

"Modify the Environment Variables in the RMAN-ENV Script" on page 350

"Configure the Database for Online Backup" on page 352

"Run Incremental Online Backups" on page 353

Plan the Size of the Backup Area

The backup area is the location where the Oracle online database backup function stores the backup copy of the database instance plus the redo logs and other database-related files.

The online redo log represents the currently running incremental database backup, and the archived redo logs represent previous incremental backups. You must estimate the maximum size of the backup area in order to set the appropriate environment variable, as described in "Modify the Environment Variables in the RMAN-ENV Script" on page 350.

As a guideline, we recommend a backup area that is 3x the size of the database, which is based on the sum of the database, database copy, and archived log files.

Ideally, the size of the backup area must be large enough to store all of the following:

- A copy of the database instance
- All online redo logs
- Any archived redo logs that have not been backed up elsewhere.
- A copy of the database control file and the SPFILE

At a minimum, the backup area should be able to store at least 24 hours of archived redo logs that have not been backed up.

Copy the Online Backup Scripts to a Local Directory

To access the scripts for online database backup, copy them from the OpenPages installation DVD to any local directory on the database server. You can execute the scripts from the local directory.

Procedure

1. Log on to the OpenPages database server as a user with administrative privileges.
2. Open a command or shell window and do the following:
   a. Either navigate to the `OP_6.1.0 _<Embedded|Non_Embedded>_ DVD_1` on your network drive or insert the DVD from your installation kit.
   b. Navigate to the `INSTALL_SCRIPTS` directory at the following location:
      `OP_6.1.0 _Configuration|Database|INSTALL_SCRIPTS`
3. From the `INSTALL_SCRIPTS` directory copy the following scripts to a local directory on the database server.
   - Environment-specific online backup scripts:

Windows	AIX
rman-env.cmd	rman-env.sh
rman-init.cmd	rman-init.sh
rman-daily.cmd	rman-daily.sh
recover-db.cmd	recover-db.sh

   - Additional online backup scripts:

```
enable-archivelog-mode.sql
disable-archivelog-mode.sql
check-fra-size.sql
update-fra-size.sql
```

Note:

- The name of the local directory where you are copying the scripts must not contain any space characters.
- You can execute the scripts described in the remainder of this section from the local directory, or add the directory to your PATH environment variable so that you can execute them from any directory.

Modify the Environment Variables in the RMAN-ENV Script

Once you have determined the size of the backup area, edit the environment variable values in the `rman-env` script as follows.

Procedure

1. Open the `rman-env.cmd` (Windows) or `rman-env.sh` (AIX) script in a text editor on the database server and edit the following environment variables for your Oracle database environment as shown in Table 58.

Table 58. Environment Variables in RMAN-ENV Script

Environment Variable	Description
ORACLE_HOST_NAME=	Fully qualified network identifier for the database server machine. The host name can be found in the HOST parameter in the `tnsnames.ora` file. **Example**: `mydbhost.openpages.com`

Table 58. Environment Variables in RMAN-ENV Script (continued)

Environment Variable	Description
ORACLE_SID=	SID of the IBM OpenPages database instance you are backing up. The SID can be found in the SERVICE_NAME parameter in the `tnsnames.ora` file. **Example**: `op11`

`ORACLE_HOME=`	The Oracle database Home directory on the database server where the Oracle software is installed, including the database. This is the same as the value of the ORACLE_HOME environment variable for the database server.
	
	Examples
	
	Database and application servers on the same machine:
	
	Windows
	
	`C:\openpages_data\repository\ server112_se_x64\software`
	
	AIX
	
	`/opt/oracle/openpages_data/repository/ server112_se_x64/software`
	
	Database and application servers on different machines:
	
	Windows
	
	`C:\openpages_data\repository\ client112_ac_x64\software`
	
	AIX
	
	`/opt/oracle/openpages_data/repository/ client112_ac_x64/software`

ORACLE_DATAFILE_LOC=	The Oracle data Home directory on the database server. This is the location where the Oracle data is stored.
	
	Examples
	
	Windows
	
	`C:\openpages_data\repository\ database112_se_x64\ordata\<server_name>`
	
	AIX
	`opt/openpages_data/repository/ database112_se_x64/ordata/<server_name>`

FLASH_RECOVERY_AREA=	Directory or file system where the backup area will be located on the database server. **Example**: `c:\temp\arch` (Windows)

Table 58. Environment Variables in RMAN-ENV Script (continued)

Environment Variable	Description
FLASH_RECOVERY_AREA_SIZE=	Maximum size of the backup area, specified in either megabytes (M) or gigabytes (G). You can specify any size up to the maximum allowed by the operating system on the database server. Examples • 500M (500 megabytes) • 20G (20 gigabytes)
LISTENER_PORT=	Listener port number of the Oracle database instance you are backing up. The listener port number can be found in the PORT parameter in the `tnsnames.ora` file. **Example**: 1521
ORACLE_HOME_NAME=	Name assigned to ORACLE_HOME at installation time. The Oracle Home Name can be found in the SERVER parameter in the `inventory.xml` file in the `<Oracle_Home>\software\inventory\ContentsXML` directory. **Example**: OPServer

2. Save the script file.

Results

Note:

- Once you enable online backup mode for a database instance, do not make any changes to the corresponding `rman-env` script. If you need to increase the size of the backup area, see "Adjusting the Size of the Backup Area" later in this chapter for more information. Never modify the `rman-env` script to adjust the size of the backup area once online database backup mode is enabled.
- If you need to back up a different database instance, make a copy of the `rman-env` script in a different directory and modify the parameters as appropriate. The `FLASH_RECOVERY_AREA` parameter must specify a different location than that of your other online database backups.

Configure the Database for Online Backup

Run the `rman-init` script to create the required directories and scripts for database recovery and to configure the parameters that you entered in the `rman-env` script for Oracle online database backup.

To run the script, execute the following command:

Windows

```
rman-init.cmd <tns_name_alias> SYS <sysdba_password>
```

AIX

```
rman-init.sh <tns_name_alias> SYS <sysdba_password>
```

Where:

`<tns_name_alias>` is the TNS alias of the OpenPages database instance as it is known on the network. If necessary, you can retrieve this alias from the `tnsnames.ora` file.

<sysdba_password> is the Oracle SYS account password.

Example (Windows)

```
rman-init.sh op11 SYS SYSPWD
```

If there are errors when running this script, the script output will list the directory location containing the error log. The error log file name is `enable-archivelog-more.log`.

Important: The script described in this section restarts the database. It is recommended that you alert users that they will be temporarily unable to access the database until the script has finished running.

Run Incremental Online Backups

About Running the Rman-daily Script: The `rman-daily` script can be run manually or on a scheduled basis using standard operating system scheduler functions (such as `cron`).

You can run the script at any interval, not just daily. The script can be run without disrupting access to the database, even while the database is open and in use.

When you run this script, the following takes place:

- RMAN makes a level 0 incremental backup copy of the database instance and stores it in the backup area. If no backup currently exists yet, this is a full, physical, bit-for-bit backup. Otherwise, only data blocks that have changed since the last backup are included in the incremental backup.
- RMAN also makes a backup copy of the database control file and SPFILE in the backup area.
- Once the backup is successfully completed, all of the archived redo logs in the backup area are cleared, freeing up additional storage space in the backup area.

Run the Rman-daily Script:

Once you have configured the database for online backup, you can run the `rman-daily` script to perform online backups.

To run the script, execute the following command:

Windows

```
rman-daily.cmd <tns_name_alias> SYS <sysdba_password>
```

AIX

```
rman-daily.sh <tns_name_alias> SYS <sysdba_password>
```

Where:

<tns_name_alias> is the TNS alias of the IBM OpenPages database instance as it is known on the network. If necessary, you can retrieve this alias from the `tnsnames.ora` file.

<sysdba_password> is the Oracle SYS account password.

Example (AIX)

```
rman-daily.sh op11 SYS SYSPWD
```

Review Log Files:

The rman-daily script produces a log file (rman-daily.log) that lists each component that was backed up. The log is recreated (overwritten) each time that you run the rman-daily script.

The directory location of the rman-daily.log is:

Windows
<FLASH_RECOVERY_AREA>\<ORACLE_SID>\logs

AIX <FLASH_RECOVERY_AREA>/<ORACLE_SID>/logs

Where:

<FLASH_RECOVERY_AREA> and <ORACLE_SID> are the values of those parameters in the rman-env script.

The log file lists the following information for the online database backup:

- Backup sets (incremental backups)
- Copies of data files
- Copies of control files
- Temp files

Managing the Backup Area

In order to accommodate growth of the database instance, you may need to adjust the size of the backup area. This section describes how to monitor and increase the size of the backup area.

Monitoring the Size of the Backup Area

To monitor and display the size of the backup area, use the following script:

```
sqlplus /nolog @sql-wrapper check-fra-size <log_file_name> <tns_name_alias>
 SYSTEM <system_password>
```

Where:

- <log_file_name> is the directory location, including the log file name that you specify, where any errors or messages relating to this script are logged. If you specify only the log file name, it is stored in the current working directory.
- <tns_name_alias> is the TNS alias of the OpenPages database instance as it is known on the network. If necessary, you can retrieve this alias from the tnsnames.ora file.
- <system_password> is the Oracle SYSTEM account password.

The script displays the following information (in megabytes):

- Used Space — Space that is already used and not available for online database backups.
- Allocated Space — Maximum size of the backup area, including used and free space. This is the same as the value of the FLASH_RECOVERY_AREA_SIZE parameter in the rman-env script.
- Used-Reclaimable — Space that is free for use in online database backups.

Example:

```
sqlplus /nolog @sql-wrapper check-fra-size C:\OpenPages\logs op11 SYSTEM SYSTEMPWD
```

Displays the used, allocated, and free space for database instance op11.

Adjusting the Size of the Backup Area

Occasionally, you may need to modify the size of the backup area. For example, you may see the following warning message in the Oracle Alert log:

```
ORA-19815: WARNING: db_recovery_file_dest_size of xxxxx bytes is 100.00% used,
 and has 0 remaining bytes available
```

You need to increase the size of the backup area to make more space available for online database backups. You can increase or decrease the size of the backup area by running either of two scripts described in this section.

Important: Never delete files manually from the backup area to free up space. Attempting to do so will cause the following error: `RMAN-06059: expected archived log not found`.

Reclaiming Used Space by Running the RMAN-DAILY Script:

Running the `rman-daily` script reclaims previously used space in the backup area, freeing it up for use in online database backups.

Adjusting Space by Running the UPDATE-FRA-SIZE Script:

If you want to adjust the maximum size of the backup area to a specific value, run the following script:

```
sqlplus /nolog @sql-wrapper update-fra-size <log_file_name> <tns_name_alias>
 SYS <sysdba_password> <new_size>
```

Where:

- `<log_file_name>` is the directory location, including the log file name that you specify, where any errors or messages relating to this script are logged. If you specify only the log file name, it is stored in the current working directory.
- `<tns_name_alias>` is the TNS alias of the OpenPages database instance as it is known on the network. If necessary, you can retrieve this alias from the `tnsnames.ora` file.
- `<sysdba_password>` is the Oracle SYS account password.
- `<new_size>` is the updated size of the backup area (use M for megabytes or G for gigabytes). For example, you would specify 20 gigabytes as **20G**.

Example:

```
sqlplus /nolog @sql-wrapper update-fra-size <log_file_name> op11 SYS SYSPWD 15G
```

Adjusts the backup area for database instance op11 to 15 gigabytes.

Important: The script described in this section restarts the database. It is recommended that you alert users that they will be temporarily unable to access the database until the script has finished running.

Disabling Online Backup of the Database Instance

Run the following script to turn off archive logging mode, which disables Oracle online database backup for the specified database instance. This simply stops the service that runs online database backup; it does not remove any files or data already stored in the backup area.

```
sqlplus /nolog @sql-wrapper disable-archivelog-mode <log_file_name> <tns_name_alias>
 SYS <sysdba_password>
```

Where:

- `<log_file_name>` is the directory location, including the log file name that you specify, where any errors or messages relating to this script are logged. If you specify only the log file name, it is stored in the current working directory.
- `<tns_name_alias>` is the TNS alias of the OpenPages database instance as it is known on the network. If necessary, you can retrieve this alias from the `tnsnames.ora` file.
- `<sysdba_password>` is the Oracle SYS account password.

Example:

```
sqlplus /nolog @sql-wrapper disable-archivelog-mode <log_file_name> op11 SYS SYSPWD
```

Important:

- The script described in this section restarts the database. It is recommended that you alert users that they will be temporarily unable to access the database until the script has finished running.
- After disabling online database backup mode, if you want to re-enable online database backup mode for the database instance, do not use the `rman-init` or `rman-daily` scripts. Doing so may cause unpredictable database behavior or other problems. To re-enable online database backup mode, contact your IBM representative for assistance.

Performing Oracle Online Database Crash Recoveries

If a system crash or other problem either corrupts the database instance or causes it to fail, the database must be recovered from the online backup. The actual recovery procedure may vary depending on the nature of the crash, which parts of the database were damaged, and your system environment. For that reason, database recoveries must only be performed by an IBM representative.

Refreshing a Test Environment from Backup Files

The best method for refreshing an existing test environment is to have it replicated from the production environment. By using your production environment's backup files, you can update a test environment that closely matches your production environment as of the backup date.

Make sure you have access to both the production or "source" and test or "target" servers.

Note: Oracle Data Pump backup files are created on the database server.

To refresh a test environment, perform the following tasks.

Prerequisites

The following are required:

- The test or "target" server and production or "source" server must have the same installed version of the IBM OpenPages application — including patches.
- You must have access to the following DVD either on your installation media or from a shared network drive:

  `OP_6.1.0 _<Embedded|Non_Embedded>_DVD_1`

Process Overview

The process for refreshing a test environment involves the following tasks:

- "Back Up and Copy IBM OpenPages Application Production Data"
- "Back Up IBM OpenPages Application Test Data"
- "Backup Workflow Properties in the Test Environment"
- "Delete Data on the Test Database System" on page 358
- "Copy the Production Database Dump (.dmp) File to the Test Database Server" on page 359
- "Import the Production Data into the Test Environment" on page 359
- "Update the OpenPages Storage Location in the Database" on page 361
- "Update the Workflow Database in the Test Environment" on page 362
- "Update CommandCenter Data in the Test Environment" on page 364
- "Import Properties Specific to Cluster Members in Your Test Environment" on page 363
- "Modify SSO and LDAP Configuration in the Test Environment" on page 368
- "Copy Custom Deliverables to the Test Environment" on page 368
- "Start OpenPages and Workflow Servers in the Test Environment" on page 369
- "Update URL Host Pointers for CommandCenter Reports" on page 370

Back Up and Copy IBM OpenPages Application Production Data

The exported data from the production backup file will be used later to refresh data on the test server.

Procedure

1. Log on to your production IBM OpenPages server as a user with administrative permissions.
2. Run the IBM OpenPages backup utility (`OPBackup`) as described in Using the OpenPages Backup Utility to backup the IBM OpenPages application and workflow databases.
3. Copy the IBM OpenPages backup `.zip` or `.tar.gz` file to your test server.

Back Up IBM OpenPages Application Test Data

Procedure

1. Log on to your test IBM OpenPages server as a user with administrative permissions.
2. Run the IBM OpenPages backup utility (`OPBackup`) as described in Using the OpenPages Backup Utility to backup the IBM OpenPages application and workflow databases.

Backup Workflow Properties in the Test Environment

Procedure

1. Log on to your test IBM OpenPages server as a user with administrative permissions.
2. Export the workflow properties on your test server for later use as follows:
   a. Open a command or shell window and navigate to the following directory:
   `<Workflow_Home>|server|deployment|bin`

Where: <Workflow_Home> represents the installation location of the Fujitsu Interstage BPM server. By default, this is:	
Windows	c:\Fujitsu\InterstageBPM
AIX	/opt/Fujitsu/InterstageBPM

b. From the bin directory, execute the exportProperties command as follows:

Windows:

```
exportProperties.bat <output-file> <opworkflow_db_user> <opworkflow_db_password>
```

AIX:

```
exportProperties.sh <output-file> <opworkflow_db_user> <opworkflow_db_password>
```

Where:

<output-file> is the name of the file containing the exported workflow properties. If no directory is specified, the file is created in the bin directory.

<opworkflow_db_user> is the IBM OpenPages workflow user name for accessing the workflow database.

<opworkflow_db_password> is the IBM OpenPages workflow password for accessing the workflow database.

Examples

Windows

```
exportProperties.bat ibpm.properties opworkflow opworkflow
```

AIX

```
exportProperties.sh ibpm.properties opworkflow opworkflow
```

Delete Data on the Test Database System

Procedure

1. If necessary, log on to your IBM OpenPages test server as a user with administrative permissions.
2. Open a command or shell window and do the following:
   a. Either navigate to the OP_6.1.0 _<Embedded|Non_Embedded>_ DVD_1 on your network drive or insert the DVD from your installation kit.
   b. Navigate to the INSTALL_SCRIPTS directory at the following location:
      OP_6.1.0 _Configuration|Database|INSTALL_SCRIPTS
3. From the INSTALL_SCRIPTS directory, run the AuroraDbDelete.sql script as follows:
   a. Log on to SQL*Plus as the IBM OpenPages database user (for example: sqlplus openpages/openpages@test).
   b. Run the following script to drop and recreate objects in the user schema on the test server:

      ```
      @AuroraDbDelete
      ```

   c. Using the same SQL*Plus session, log on as the workflow database user (for example: connect opworkflow/opworkflow@test).
   d. Run the same script again to drop and recreate the workflow schema on the test server:

      ```
      @AuroraDbDelete
      ```

   e. When finished, log out of SQL*Plus.

Copy the Production Database Dump (.dmp) File to the Test Database Server

Procedure

1. Locate the database dump (.dmp) file directory on the source production and target test database servers.

   Note:

   To find the 'datapump' directory for either the source or target database, run the following SQL query as the system user:

   ```
   select directory_name, directory_path from dba_directories
   where directory_name = upper ('OP_DATAPUMP_DIRECTORY');
   ```

   By default, the 'datapump' directory on the database server is <oracle-server-directory>|admin|<sid>|dpdump
2. Copy both the IBM OpenPages and workflow database dump (.dmp) files from the Oracle datapump directory on the production database server to the datapump directory on the test database server.

For this .dmp file...	The default file name will be similar to this...
IBM OpenPages	OPENPAGES_<timestamp>.DMP
Workflow	OPWORKFLOW_<timestamp>.DMP

   Note: Make sure to copy the .dmp file with the timestamp that matches when you ran the OPBackup command.

Import the Production Data into the Test Environment

Important: You must import the IBM OpenPages database before importing the workflow database.

Procedure

1. Open a command or shell window and set the NLS_LANG environment variable as follows.

   Windows

   In the Command Prompt window where you will be invoking the import commands, execute the following command:

   ```
   set NLS_LANG=AMERICAN_AMERICA.AL32UTF8
   ```

   AIX

   Open the .profile file in the logged in user's home directory in a text editor and enter the following line if it is missing in the file:

   ```
   export NLS_LANG=AMERICAN_AMERICA.AL32UTF8
   ```

   Save the change to the file, and either execute the .profile in your shell window or log on again.
2. Import the IBM OpenPages database on the test database server from the backup files in "Back Up and Copy IBM OpenPages Application Production Data" on page 357 as follows.

   Note: The Oracle Data Pump command IMPDP is used as the IMP command is not supported.

From the same command or shell window, run the following command to import the IBM OpenPages database:

```
impdp <op_db_user>/<op_db_password>@<SID> DIRECTORY=
 OP_DATAPUMP_DIRECTORY DUMPFILE=<openpages_dump_file>
 LOGFILE=openpages_import.log
```

Where:

Parameter	Description
<op_db_user>	The IBM OpenPages user name for accessing the IBM OpenPages database.
<op_db_password>	The IBM OpenPages password for accessing the IBM OpenPages database.
<SID>	The Oracle System Identifier (for example, OP or OP11G).
<openpages_dump_file>	The .dmp file name of the backed up IBM OpenPages application database.

Example

```
impdp openpages/openpages@OP11G DIRECTORY=
 OP_DATAPUMP_DIRECTORY DUMPFILE=openpages_backup_YYYY_MM_DD_HH_MI_SS.dmp
 LOGFILE=openpages_import.log
```

Note: If the source schema name and target schema names are different, the schema must be remapped during import. Add the following argument to the impdp command above to remap the schema:

```
Remap_schema=<source_schema>:<target_schema>
```

Example

```
impdp openpages/openpages@OP11G DIRECTORY=OP_DATAPUMP_DIRECTORY
 DUMPFILE=openpages_backup_YYYY_MM_DD_HH_MI_SS.dmp
 LOGFILE=openpages_import.log remap_schema=opuser:openpages
```

3. Import the workflow database on the test database server from the backup files in "Back Up and Copy IBM OpenPages Application Production Data" on page 357 as follows.

   From the same command or shell window, run the following command to import the workflow database:

```
impdp <workflow_db_user>/<workflow_db_password>@<SID>
 DIRECTORY=OP_DATAPUMP_DIRECTORY
 DUMPFILE=<workflow_dump_file> LOGFILE=opworkflow_import.log
```

   Where:

Parameter	Description
<workflow_db_user>	The IBM OpenPages workflow user name for accessing the workflow database.
<workflow_db_password>	The IBM OpenPages workflow password for accessing the workflow database.
<SID>	The Oracle System Identifier (for example, OP or OP11G).
<workflow_dump_file>	The .dmp file name of the backed up IBM OpenPages workflow database.

Example (Windows)

```
impdp opworkflow/opworkflow@OP11G DIRECTORY=OP_DATAPUMP_DIRECTORY
 DUMPFILE=opworkflow_backup_YYYY_MM_DD_HH_MI_SS.dmp
 LOGFILE=opworkflow_import.log
```

Note: If the source schema name and target schema names are different, the schema must be remapped during import. Add the following argument to the `impdp` command above to remap the schema:

```
Remap_schema=<source_schema>:<target_schema>
```

Example (Windows and AIX):

```
impdp opworflow/opworkflow@OP11G DIRECTORY=OP_DATAPUMP_DIRECTORY
 DUMPFILE=opworkflow_backup_YYYY_MM_DD_HH_MI_SS.dmp
 LOGFILE=opworkflow_import.log remap_schema=myworkflow:opworkflow
```

Update the OpenPages Storage Location in the Database

Procedure

1. If necessary, log on to your test IBM OpenPages server as a user with administrative permissions.
2. Copy all the files under the `openpages-storage` folder from the production backup `.zip` file to the `openpages-storage` location on the test server.

   By default, the storage location is `<OP_Home>|openpages-storage.`

Where: `<OP_Home>` represents the installation location of the IBM OpenPages GRC Platform application. By default, this is:	
Windows	`C:\OpenPages`
AIX	`/opt/OpenPages`

3. Open a command or shell window and do the following:
   a. Either navigate to the `OP_6.1.0 _<Embedded|Non_Embedded>_ DVD_1` on your network drive or insert the DVD from your installation kit.
   b. Navigate to the `INSTALL_SCRIPTS` directory at the following location:

      `OP_6.1.0 _Configuration|Database|INSTALL_SCRIPTS`
4. From the `INSTALL_SCRIPTS` directory, run the `update-storage` SQL wrapper script with the following parameters (see Table 59 for a description) to update the `openpages-storage` directory location in the database:

```
sqlplus /nolog @sql-wrapper.sql update-storage <log-file>  <oracle_tns_alias>
  <op_db_user> <op_db_password>  <storage-type> <storage-server-name>
  <host-name> <os-type> <path-or-UNC-name>
```

Where:

Table 59. Update Storage Wrapper Script Parameters

Parameter	Description
`<log-file>`	The name of the log file that the script will create and write information to.
`<oracle_tns_alias>`	The database alias for the OpenPages database instance, as set during the Oracle database installation.
`<op_db_user>`	The IBM OpenPages user name for accessing the IBM OpenPages database.
`<op_db_password>`	The IBM OpenPages password for accessing the IBM OpenPages database.
`<storage-type>`	The type of file storage to be used. Valid values are: • `LFS` (local file system) • `UNC` (Universal Naming Convention) **Note:** Once you move from LFS to UNC, you cannot go back to using LFS.

Table 59. Update Storage Wrapper Script Parameters (continued)

Parameter	Description
<storage-server-name>	The name of the storage server.
<host-name>	The host name of the machine.
<os-type>	The type of operating system. Valid values are: • Windows • Unix
<path-or-UNC-name>	The file path or UNC of the storage location.

Examples

- **LFS**

  Windows

```
sqlplus /nolog @sql-wraper.sql
 update-storage c:\temp\upd-storage-output.log
 op11 openpages openpages LFS eng11 eng11
 Windows c:\OpenPages\openpages-storage
```

  AIX

```
sqlplus /nolog @sql-wrapper.sql
 update-storage /home/op/upd-storage-output.log
 op11 openpages openpages LFS  aix11 aix11
 Unix /usr/opdata/openpages-storage
```

- **UNC**

  Windows

```
sqlplus /nolog @sql-wrapper.sql
 update-storage c:\temp\update-storage-output.log
 op11g openpages openpages UNC eng11
 eng11 Windows openpages-storage
```

  AIX

```
sqlplus /nolog @sql-wrapper.sql
 update-storage /home/op/upd-storage-output.log
 op11g openpages openpages UNC aix11 aix11
 Unix /usr/opdata/openpages-storage
```

Update the Workflow Database in the Test Environment

Procedure

1. If necessary, log on to your test IBM OpenPages server as a user with administrative permissions.
2. Delete all rows from the workflow `ibpmproperties` table as follows:
   a. Log on to SQL*Plus as a workflow database user into the target database server.
   b. Run the following SQL statements to delete all rows from the `ibpmproperties` table:

```
delete from ibpmproperties;
commit;
```

3. From the command or shell window, import the workflow properties that were exported in "Backup Workflow Properties in the Test Environment" on page 357 as follows:
   a. Navigate to the `<Workflow_Home>|server|deployment|bin` directory.
   b. Execute the `importProperties` command as follows:

Windows
```
importProperties.bat <full-path>\
<output-backup-filename> <opworkflow_db_user> <opworkflow_db_password>
```

AIX
```
importProperties.sh <full-path>/
<output-backup-filename> <opworkflow_db_user> <opworkflow_db_password>
```

Where:

<full-path> is the path to the location of the output file.

<output-backup-filename> is the name of the output file containing the exported workflow properties from step 2 of "Backup Workflow Properties in the Test Environment" on page 357.

<opworkflow_db_user> is the IBM OpenPages workflow user name for accessing the workflow database.

<opworkflow_db_password> is the IBM OpenPages workflow password for accessing the workflow database.

Examples

Windows

```
importProperties.bat c:\Fujitsu\InterstageIBPM\temp\
ibpm.properties opworkflow opworkflow
```

AIX

```
importProperties.sh /opt/Fujitsu/InterstageBPM/temp/
ibpm.properties opworkflow opworkflow
```

Import Properties Specific to Cluster Members in Your Test Environment

Procedure

1. If necessary, log on to your test IBM OpenPages server as a user with administrative permissions.
2. In the Command Prompt window or AIX shell, navigate to the cluster member directory:

   Windows:

   <Workflow_Home>\server\deployment\WLS-Cluster<server_name>-InterstageBPMCS<#>

   AIX:

   <Workflow_Home>/server/deployment/WAS-Cluster<server_name>-IBPMNode<#>Server

   Where:

   <Workflow_Home> is the directory where Fujitsu Interstage BPM is installed, by default:

   Windows: c:\Fujitsu\InterstageBPM

   AIX: /opt/Fujitsu/InterstageBPM

   <server_name> is the name of the IBM OpenPages application server.

   <#> represents the number of the cluster member. In a clustered environment, the number for each managed server increments by one.
3. Execute the importProperties command as follows:
   - **Windows**:

     ```
     importProperties.bat <Workflow_Home>\server\deployment\
     WLS-Cluster<server_name>-InterstageBPMCS<#>\
     ibpm.properties <opworkflow_db_user> <opworkflow_db_password>
     ```

     Where:

<Workflow_Home> represents the installation location of the Fujitsu Interstage BPM server. By default, this is: c:\Fujitsu\InterstageBPM.

<server_name> is the name of the IBM OpenPages application server.

<#> represents the number of the cluster member. In a clustered environment, the number for each managed server increments by one.

<opworkflow_db_user> is the IBM OpenPages workflow user name for accessing the workflow database.

<opworkflow_db_password> is the IBM OpenPages workflow password for accessing the workflow database.

Example

```
importProperties.bat c:\Fujitsu\InterstageBPM\server\deployment\
WLS-Clusterop-app-InterstageBPMCS1\ibpm.properties opworkflow opworkflow
```

- **AIX**:
  a. Open the setIBPMenv.sh file in a text editor.
  b. Replace the masked password in the DATABASE_PASSWORD parameter with the workflow database password.

     The password has been automatically masked using asterisks (***) during the installation. You need to replace the mask with clear text.
  c. Save the file.

     Note: Before executing importProperties.sh, make sure that the user performing the installation has the permission to execute the script. If the user does not have the permission to execute importProperties.sh, enter the following command:

     ```
     chmod 755 importProperties.sh
     ```
  d. Run ./importProperties.sh
  e. Mask the password in the DATABASE_PASSWORD parameter with asterisks. For example, DATABASE_PASSWORD=*****
  f. Save and close the setIBPMenv.sh file.

4. Repeat Step 3 for each cluster member.

Update CommandCenter Data in the Test Environment

Before You Begin

Before you run the CommandCenter backup utility (OPCCBackup) make sure to verify the following:

- You have access to both the source and target database servers.
- The <CC_user> has Read and Write permission to the OP_DATAPUMP_DIRECTORY.

  Where: <CC_user> is the name of the Cognos content store database user.

  If not, you must grant the proper permissions on both the production and test servers to the <CC_user> account on the 'datapump' directory as follows:

  1. Log on to a machine with SQL*Plus and access to the database server.
  2. Run the following SQL command as the system user:

     ```
     grant read,write on directory OP_DATAPUMP_DIRECTORY to <CC-user>;
     ```
- Full permission is granted to the CommandCenter|tools|bin folder on the target CommandCenter server.

Back Up CommandCenter Production Data and Files

The exported data from the production backup file will be used later to refresh data on the test server.

Procedure

1. If necessary, log on to your production CommandCenter server as a user with administrative permissions.
2. Run the CommandCenter backup utility (OPCCBackup) as described in Using the CommandCenter Backup Utility to backup the CommandCenter database and configuration files.

   Note: If the mail server for notification e-mails has not been setup for running CommandCenter backups, the output from the OPCCBackup command might end with the following error:

   ```
   BUILD FAILED
   c:\machine3\CommandCenter\tools\bin\op-cc-backup-email-notification.xml:31:
    Problem while sending mime mail:
   ```

   This error can be safely ignored as long as the step above the error says BUILD SUCCESSFUL.
3. Copy the production CommandCenter server backup .zip or .tar.gz file to the CommandCenter backup-restore directory on the test server.
4. Copy the database dump (.dmp) file from the Oracle 'datapump' directory on the source database server to the 'datapump' directory on the target database server.

   Make sure you copy the dump file with the timestamp that matches when you ran the OPCCBackup command. By default, the file will be named similar to OPENPAGES_CC_<timestamp>.DMP.

   Note:

   To find the 'datapump' directory for either the source or target database, run the following SQL query as the system user:

   ```
   select directory_name, directory_path from dba_directories
   where directory_name = upper ('OP_DATAPUMP_DIRECTORY');
   ```

   By default, the 'datapump' directory on the database server is <oracle-server-directory>|admin|<sid>|dpdump

Back Up CommandCenter Test Data and Files

Procedure

1. If necessary, log on to your test IBM OpenPages server as a user with administrative permissions.
2. Run the CommandCenter backup utility (OPCCBackup) as described in Using the CommandCenter Backup Utility to backup the CommandCenter database and configuration files.

Restore CommandCenter Data and Files to the Test Environment

Procedure

1. If necessary, log on to your test IBM OpenPages server as a user with administrative permissions.
2. From the INSTALL_SCRIPTS directory, run the AuroraDbDelete.sql script as follows:
   a. Log on to SQL*Plus as the Cognos database user (for example: sqlplus cognos/cognos@test).
   b. Run the following script to drop and recreate objects in the user schema on the test server:

```
@AuroraDbDelete
```

c. When finished, log out of SQL*Plus.

3. Import the CommandCenter database on the target (test) database server from the backup file from the source (production) database server as follows.

   From a command or shell window, run the following command to import the CommandCenter database:

```
impdp <cognos_db_user>/<cognos_db_password>@<SID>
 DIRECTORY=OP_DATAPUMP_DIRECTORY
 DUMPFILE=<cc_dump_file> LOGFILE=cc_import.log
```

   Where:

Parameter	Description
<cognos_db_user>	The Cognos user name for accessing the Cognos database.
<cognos_db_password>	The Cognos password for accessing the Cognos database.
<SID>	The Oracle System Identifier (for example, OP or OP11G).
<cc_dump_file>	The .dmp file name of the backed up CommandCenter database.

Example

```
impdp cognos/cognos@OP11G DIRECTORY=OP_DATAPUMP_DIRECTORY
 DUMPFILE=openpages_cc_YYYY_MM_DD_HH_MI_SS.dmp
 LOGFILE=openpages_cc_import.log
```

Note: If the source schema name and target schema names are different, the schema must be remapped during import. Add the following argument to the impdp command above to remap the schema:

```
Remap_schema=<source_schema>:<target_schema>
```

Example

```
impdp cognos/cognos@OP11G DIRECTORY=OP_DATAPUMP_DIRECTORY
 DUMPFILE=openpages_cc_YYYY_MM_DD_HH_MI_SS.dmp
 LOGFILE=openpages_cc_import.log remap_schema=cognos8:cognos
```

Change Password References for CommandCenter Data Sources

The following procedure describes how to manually update the signon password for the IBM OpenPages user account to access the Oracle data source.

Depending on the type of installation, one or both of the following Oracle data source links will be displayed in the IBM Cognos Administration tool for the CommandCenter reporting framework:

This data source...
Is used for this reporting framework...

OpenPages DataSource
Reporting Framework V6

Oracle Native Driver
Legacy Reporting Framework (upgraded systems only)

Note: Both the OpenPages DataSource and Oracle Native Driver data sources connect to the same database repository and use the same authentication information (signons).

Procedure

1. Open a browser window and log on to the CommandCenter portal as a user with administrative privileges.

   By default, the URL is `http://<server_name>/cognos8`.

   Where: `<server_name>` is the name of the CommandCenter server
2. Do one of the following to launch IBM Cognos Administration:
   - If the Cognos splash page appears, then click the **Administer IBM Cognos Content** link.
   - If the IBM Cognos Connection page appears, then click **Launch** and select **IBM Cognos Administration**.
3. On the **Configuration** tab, click **Data Source Connections** in the left pane (if not already selected).
4. On the Directory > Cognos page, click the **More** link in the same row as the data source you want (for example, `OpenPages DataSource`).
5. On the Perform an Action page, under **Available actions**, click the **View connections** link.
6. On the **Directory** > **Cognos** > **<** `name of data source` > page, click the **More** link in the same row as the selected data source.
7. On the Perform an Action page for the data source, under **Available actions**, click the **View signons** link.
8. On the **Directory** > **Cognos** > **<** `name of data source` **>** signons page, do the following:
   a. Under the **Actions** column, click the '**Set properties - <** `name of data source` **>**' icon.
   b. On the **Set properties-<** `name of data source` > page, click the **Signon** tab.
9. On the **Signon** tab:
   a. Click the **Edit the signon** link.
   b. Update the password.
   c. When finished, click **OK**.

Update Database Connection References for CommandCenter

Procedure

1. Open a browser window and log on to the CommandCenter portal as a user with administrative privileges.

   By default, the URL is `http://<server_name>/cognos8`.

   Where: `<server_name>` is the name of the CommandCenter server
2. Do one of the following to launch IBM Cognos Administration:
   - If the Cognos splash page appears, then click the **Administer IBM Cognos Content** link.
   - If the IBM Cognos Connection page appears, then click **Launch** and select **IBM Cognos Administration**.
3. On the **Configuration** tab, click **Data Source Connections** in the left pane (if not already selected).
4. On the Directory > Cognos page, click the link for the **OpenPages DataSource**.
5. On the Directory > Cognos > OpenPages DataSource page, do the following:
   a. Under the **Actions** column, click the '**Set properties - OpenPages DataSource**'  icon.

b. On the Set properties - OpenPages DataSource page, click the **Connection** tab.

6. On the **Connection** tab, next to the **Connection String** box, click the pencil icon to edit the field.
7. On the edit page, do the following:
   a. In the **SQL*Net connect string** box, change the SQL*Net connect string to the TNS alias of the OpenPages database on the target environment.
   b. When finished, click **OK**.
8. Click **OK** again.
9. If this is an upgraded legacy system, repeat the steps in this task for the `Oracle Native Driver`, if it exists.

Modify SSO and LDAP Configuration in the Test Environment

If you are using SSO and/or LDAP in the test environment, modify the configuration for each if needed. Otherwise, skip this task.

Copy Custom Deliverables to the Test Environment

If you are using custom deliverables, perform the following task.

Copy Custom Triggers and Custom Workflow Java Actions

You must copy any custom Java actions and triggers that have been deployed on the production server to the test environment. These custom actions and triggers are added to a zip file, openpages-ext.jar, by the OPBackup utility.

If you have any questions about the location of your custom data, contact IBM representative.

Procedure

1. If necessary, log on to your test IBM OpenPages server as a user with administrative permissions.
2. Update the `openpages-ext.jar` in the test environment as follows:
   a. From the production backup `.zip` files in "Back Up and Copy IBM OpenPages Application Production Data" on page 357, navigate to the `openpages-ext.jar` in the `<OP_Home>|aurora|lib` directory.

      Where: `<OP_Home>` represents the installation location of the IBM OpenPages application.

      Windows `<OP_Home>\aurora\lib\openpages-ext.jar`

      By default `<OP_Home>` is `C:\OpenPages`

      AIX `<OP_Home>/aurora/lib/openpages-ext.jar`

      By default `<OP_Home>` is `/opt/OpenPages`

   b. Copy the `openpages-ext.jar` from the production backup file into the `<OP_Home>|aurora|lib` directory on your test machine and overwrite the existing `.jar` file there.
3. Update the .class files in the test environment so all custom Java Action sets can be opened from the Interstage BPM console as follows:
   a. From the production backup `openpages-ext.jar`, extract all custom Java Action `.class` files using the `jar` command from the `<Workflow_Home>|server|instance|default|attachments` directory.

Where: <Workflow_Home> represents the installation location of the Fujitsu Interstage BPM server. By default, this is:	
Windows	c:\Fujitsu\InterstageBPM
AIX	/opt/Fujitsu/InterstageBPM

For example:

```
jar xvf openpages-ext.jar
```

The result is that all of the class files are extracted into the current folder.

b. Copy the extracted .class files, while preserving the full package folder structure, into the <Workflow_Home>|server|instance|default|attachments directory on your test machine.

These .class files are needed to open Java action sets from the IBPM Console.

c. Copy the .class files, while preserving the package folder structure, to the following directory on each client machine used by workflow authors where Interstage BPM Studio is installed.

These .class files are needed to open Java action sets from the IBPM Console:

```
<Workflow_Studio_Home>\InterstageBPM_studio\ibpm\Data\attachments
```

Where:

<Workflow_Studio_Home> represents the installation location of Fujitsu Interstage BPM Studio on the client machine. By default, this is c:\Fujitsu\InterstageBPM.

Copy Other Custom Deliverables

If you have other custom deliverables, such as UI helpers, JSP reports, and so forth, then perform the following steps.

If you have any questions about the location of your custom data, contact your IBM representative.

Procedure

1. From the production backup .zip files in "Back Up and Copy IBM OpenPages Application Production Data" on page 357, extract all custom files such as:
   - JAR files
   - JSP files
   - JavaScript files
   - Image files
2. Copy these files into their respective folders on the target machine (should match the source install).

Start OpenPages and Workflow Servers in the Test Environment

When finished, start IBM OpenPages services on the servers in your test environment. For details, see "Starting and Stopping OpenPages Application Servers" on page 465.

Update URL Host Pointers for CommandCenter Reports

Modify the URL host pointer settings and then propogate these changes to the reporting schema on the application server (does not require services to be restarted).

For details, see “Updating URL Host Pointers for CommandCenter Reports” on page 387.

About the Workflow Purge Utility

The IBM OpenPages Workflow Purge Utility is intended to be run when database administrators want to reduce the size of the workflow database, by selectively removing data related to completed jobs, terminated jobs, and tasks, thereby increasing overall application performance. The utility provides the ability to purge completed and terminated jobs from the IBM OpenPages database instance that are older than a specified date. Purging jobs creates a smaller, more efficient database that results in enhanced performance by removing unneeded jobs and associated data and allows you to perform quicker upgrades.

Using the Workflow Purge Utility, you can remove all records in the database related to completed and terminated jobs and any associated sub-jobs (or child jobs), while maintaining the referential integrity of the database. This utility is not meant to be run daily but only when administrators evaluate the workflow data growth and feel that it is time to remove unwanted data.

The Workflow Purge Utility generates a list of jobs that will not be purged and moves them to a temporary table. The utility will then dump the remaining (completed on or after the selected date or running) jobs, truncate the appropriate tables, then move the non-purged jobs back to their original table, where they will function as expected.

The utility will purge all completed jobs prior to the cut off date entered as well as all terminated jobs. The utility will not purge any running jobs.

For hierarchical jobs, if any top-level job is not completed or terminated, the whole job tree remains. In this case, there may be some child jobs that are completed or terminated that will not be purged.

Note:

- The utility will not purge a workflow that has multiple associated jobs if any job is still running.
- The utility will purge a workflow that has multiple associated jobs if the top-level job is terminated.

Running the Workflow Purge Utility

The Workflow Purge Utility reduces the size of the workflow dataset and to improve overall performance. You can run the utility from any system with access to SQL*Plus that can connect to the database server.

Before you begin

Before running the Workflow Purge Utility, review the following:

- Perform a full backup of the IBM OpenPages database instance before running the utility. See the "Using the IBM OpenPages Backup Utility" on page 335 for information for your current IBM OpenPages version. •
- Stop all OpenPages and workflow services prior to running the utility. See "About Stopping IBM OpenPages Application Servers" on page 470 for information stopping the IBM OpenPages services in your current IBM OpenPages version.
- Obtain the user name and password for the Oracle account that owns the IBM OpenPages application database schema.
- Obtain the user name and password for the Oracle account that owns the IBM OpenPages workflow database schema.
- Obtain the TNS alias name (SID) of the IBM OpenPages application database schema.

Procedure

1. Log on to a system as a user with Administrator privileges. You can use any system with access to SQL*Plus that can connect to the OpenPages database server.
2. Open a command or shell window, navigate to the bin directory as follows.

   Where: <OP_Home> represents the installation location of the IBM OpenPages GRC Platform application.

   Windows <OP_Home>\aurora\bin\workflow-purge-utility

   By default <OP_Home> is C:\OpenPages

   AIX <OP_Home>/aurora/bin/workflow-purge-utility

   By default <OP_Home> is /opt/OpenPages

3. Run the following batch command:

   Windows

   ```
   WorkflowPurgeUtility.bat <SID> <username> <password>
   <workflow_user> <workflow_password> <cut_off_date>
   ```

   AIX

   ```
   WorkflowPurgeUtility.sh <SID> <username> <password>
   <workflow_user> <workflow_password> <cut_off_date>
   ```

Parameter name	Description
<SID>	The system ID or TNS alias for the OpenPages database instance.
<username>	The OpenPages application schema user name.
<password>	The OpenPages application schema owner password.
<workflow_user>	The workflow schema user name.
<workflow_password>	The workflow schema owner password.

Parameter name	Description
<cut_off_date>	The date before which you want to purge completed jobs, in the YYYYMMDD format. All completed (prior to the specified date), terminated jobs, and associated sub-jobs will be purged. All completed jobs equal to or later than the specified date will remain. **Note:** If you enter a future date, all completed jobs will be purged.

Example

```
WorkflowCleanup.bat OP openpages openpages opworkflow opworkflow
20120225
```

Any completed jobs prior to the February 25, 2012 date will be purged. The cut off date has no effect on terminated jobs.

Results

When the utility is complete, the command window displays a message and refers you to the log file for specific details on the purge.

Note: Stopping the utility while it is running is not recommended.

Impact of the Workflow Purge Utility

The utility performs general tasks to the IBM OpenPages database instance:

1. Creates the temporary tables, views, packages, and stored procedures used by the utility.
2. Creates a list of processes (process instance IDs) to retain after purge and inserts the process instance IDs into the OP_TEMP_INSTANCEID table.
3. Locates private process definition IDs that are referenced by any process instances and inserts these private process definition IDs into OP_TEMP_PROCDEFINITIONID table. A private process definition is an internal copy of a published process definition for use by IBM OpenPages to start jobs. Inserts other process definitions that are in draft, published, or obsolete state into the OP_TEMP_PROCDEFINITIONID table. No published process definition is purged by this utility.
4. Moves data to temporary tables, filtering on the list of the process instance IDs and process definition IDs created in Step 2 to retain jobs that are not completed (running) or completed on and after the cut off date.
5. Disables any foreign key constraints on the tables to be purged.
6. Truncates the original tables.
7. Moves data back to its original tables.
8. Re-enables constraints on those tables.
9. Stores the percent of data purged in the OP_TEMP_PURGE_PERCENT table.
10. Drops temporary tables, views, packages, and stored procedures used by the utility, except the OP_TEMP_PURGE_PERCENT table.

Refer to the logs in the directory where the utility is installed for details on the purge.

Utilities for Filtering on Long String Field Content

You can filter based on the content of long string fields if the Oracle Text feature has been enabled. This is also known as full text searching.

Long string fields allow users to enter values over 4KB in length. To apply filters on the content of these long string fields, first "Enable Oracle Text" feature. If the Oracle Text feature is not enabled, attempts to filter on the content of long string fields will generate errors. For details on setting up long text fields, see "Working with Long String Fields" on page 142.

There are five utilities provided to help manage full text searching:

- "Enable Oracle Text"
- "Create a Long String Index" on page 374
- "Create a Schedule Job to Synchronize a Long String Index" on page 375
- Optimize a Large Text Index
- "Drop a Long String Index" on page 377
- "Modifying the List of Stop Words" on page 378

To apply filters with long string fields, you must change the **OpenPages | Platform | Database | Text Indexes** setting to **true**.

If the value is set to...	Then...
true	Filtering is enabled on long string fields.
false	Filtering is disabled on long string fields. The default is **false**.

For details on working with settings, see "Accessing the Settings Page" on page 268.

Enable Oracle Text

Enable the Oracle Text feature to perform filtering based on the contents of fields with long string data types. Scripts are provided for both Windows and AIX.

Procedure

1. Log on to the Oracle database server as a user with database administrator privileges.

   Note: You can only enable Oracle Text from the database server.
2. Open a command or shell window, navigate to the bin directory as follows.

   Where: `<OP_Home>` represents the installation location of the IBM OpenPages GRC Platform application.

   Windows `<OP_Home>\aurora\bin`

   By default `<OP_Home>` is `C:\OpenPages`

   AIX `<OP_Home>/aurora/bin`

   By default `<OP_Home>` is `/opt/OpenPages`

Note: If the database server is not on the same machine as the IBM OpenPages server, you must copy the script, and the SQL files it invokes, to the database server.

3. Run the following batch command:

   Windows

   ```
   EnableOpenPagesTextIndexing.bat <SID> <SYSDBA_USER_NAME>
   <SYSDBA_PASSWORD> <OPX_USER_NAME> <OPWORKFLOW_USER>
   ```

   AIX

   ```
   EnableOpenPagesTextIndexing.sh <SID> <SYSDBA_USER_NAME>
   <SYSDBA_PASSWORD> <OPX_USER_NAME> <OPWORKFLOW_USER>
   ```

   Note: All parameters are required.

Parameter name	Description
<SID>	The system ID or TNS alias for the OpenPages database instance.
<SYSDBA_USER_NAME>	Database SYSDBA account. Usually 'SYS' user.
<SYSDBA_PASSWORD>	Password for SYSDBA user account.
<OPX_USER_NAME>	OpenPages application schema owner name.
<OPWORKFLOW_USER>	The workflow schema user name.

Results

The database is now enabled for indexing. Use "Create a Long String Index" script to create the index.

Create a Long String Index

Create a long string text index to support filtering based on the contents of fields with long string data types. Scripts are provided for both Windows and AIX.

Before you begin

Oracle Text must be enabled. See "Enable Oracle Text" on page 373.

Procedure

1. Log on to a system as a user with Administrator privileges. You can use any system with access to SQL*Plus that can connect to the OpenPages database server.
2. Open a command or shell window, navigate to the bin directory as follows.

   Where: <OP_Home> represents the installation location of the IBM OpenPages GRC Platform application.

   Windows <OP_Home>\aurora\bin

   By default <OP_Home> is C:\OpenPages

   AIX <OP_Home>/aurora/bin

   By default <OP_Home> is /opt/OpenPages

Note: If the database server is not on the same machine as the IBM OpenPages server, you must copy the script, and the SQL files it invokes, to the database server.

3. Run the following batch command:

   Windows

   ```
   CreateOpenPagesTextIndex.bat <SID> <OPX_USER_NAME>
   <OPX_USER_PASSWORD> <MEMORY_LIMIT> <PARALLEL_INDEXING_DEGREE>
   ```

   AIX

   ```
   CreateOpenPagesTextIndex.sh <SID> <OPX_USER_NAME>
   <OPX_USER_PASSWORD> <MEMORY_LIMIT> <PARALLEL_INDEXING_DEGREE>
   ```

Parameter name	Description
<SID>	The system ID or TNS alias for the OpenPages database instance.
<OPX_USER_NAME>	OpenPages application schema owner name.
<OPX_USER_PASSWORD>	OpenPages application schema owner password.
<MEMORY_LIMIT>	Specifies the amount of run-time memory to use for indexing, in megabyte or gigabyte values. For example, valid values include 128M and 2G.
<PARALLEL_INDEXING_DEGREE>	Parallel degree for parallel indexing. The actual degree of parallelism might be smaller depending on system resources.

Results

An index is created for long string fields.

Create a Schedule Job to Synchronize a Long String Index

Create a schedule to synchronize the long string index. Scripts are provided for both Windows and AIX.

Procedure

1. Log on to a system as a user with Administrator privileges. You can use any system with access to SQL*Plus that can connect to the OpenPages database server.
2. Open a command or shell window, navigate to the bin directory as follows.

   Where: <OP_Home> represents the installation location of the IBM OpenPages GRC Platform application.

   Windows <OP_Home>\aurora\bin

   By default <OP_Home> is C:\OpenPages

   AIX <OP_Home>/aurora/bin

   By default <OP_Home> is /opt/OpenPages

Note: If the database server is not on the same machine as the IBM OpenPages server, you must copy the script, and the SQL files it invokes, to the database server.

3. Run the following batch command:

Windows

```
ManageOpenPagesTextIndexRefreshJob.bat <SID> <OPX_USER_NAME>
<OPX_USER_PASSWORD> <START_JOBS_AFTER_DAYS> <JOB_START_HOUR>
<REFRESH_FREQ_IN_HOURS> <REFRESH_FREQ_IN_MINS> <MEMORY_LIMIT>
<PARALLEL_INDEXING_DEGREE> <MAX_SYNC_TIME>
```

AIX

```
ManageOpenPagesTextIndexRefreshJob.sh <SID> <OPX_USER_NAME>
<OPX_USER_PASSWORD> <START_JOBS_AFTER_DAYS> <JOB_START_HOUR>
<REFRESH_FREQ_IN_HOURS> <REFRESH_FREQ_IN_MINS> <MEMORY_LIMIT>
<PARALLEL_INDEXING_DEGREE> <MAX_SYNC_TIME>
```

Parameter name	Description
<SID>	The system ID or TNS alias for the OpenPages database instance.
<OPX_USER_NAME>	OpenPages application schema owner name.
<OPX_USER_PASSWORD>	OpenPages application schema owner password.
<START_JOBS_AFTER_DAYS>	Number of days between today and the scheduled starting date of the job. For example, 0 for today, 1 for tomorrow.
<JOB_START_HOUR>	The hour (on a 24-hour clock) of the scheduled starting date of the job. For example, 18 for 1800 hours or 6 p.m.
<REFRESH_FREQ_IN_HOURS>	Intervals (in hours) between each job. This value is combined with **<REFRESH_FREQ_IN_MINS>** value. Maximum of combined values is 999.
<REFRESH_FREQ_IN_MINS>	Intervals (in minutes) between each job. This value is combined with **<REFRESH_FREQ_IN_HOURS>**. Maximum of combined values is 999.
<MEMORY_LIMIT>	Specifies the amount of run-time memory to use for indexing, in megabyte or gigabyte values. For example, valid values include 128M and 2G.
<PARALLEL_INDEXING_DEGREE>	Parallel degree for parallel indexing. The actual degree of parallelism might be smaller depending on system resources.
<MAX_SYNC_TIME>	Maximum time (in minutes) the index synchronization job can run.

Results

Index synchronization jobs will run at the interval specified.

Note: Changes to long string fields are not available for filtering until the next scheduled index job runs.

For example, ManageOpenPagesTextIndexRefreshJob.bat OP opadmin opadmin 1 3 24 0 2G 0 60 schedules indexing synchronization to start at 3 a.m. starting on the next day, and then repeat every day following at the same time. There is a 2 gigabyte memory limit, no parallel indexing, and the job can run no more than an hour.

Drop a Long String Index

Remove the long string index. An index must be dropped before it can be recreated. Scripts are provided for both Windows and AIX.

Procedure

1. Log on to a system as a user with Administrator privileges. You can use any system with access to SQL*Plus that can connect to the OpenPages database server.
2. Open a command or shell window, navigate to the bin directory as follows.

   Where: <OP_Home> represents the installation location of the IBM OpenPages GRC Platform application.

   Windows <OP_Home>\aurora\bin

   By default <OP_Home> is C:\OpenPages

   AIX <OP_Home>/aurora/bin

   By default <OP_Home> is /opt/OpenPages

   Note: If the database server is not on the same machine as the IBM OpenPages server, you must copy the script, and the SQL files it invokes, to the database server.
3. Run the following batch command:

   Windows

   ```
   DropOpenPagesTextIndex.bat <SID> <OPX_USER_NAME>
   <OPX_USER_PASSWORD>
   ```

   AIX

   ```
   DropOpenPagesTextIndex.sh <SID> <OPX_USER_NAME>
   <OPX_USER_PASSWORD>
   ```

Parameter name	Description
<SID>	The system ID or TNS alias for the OpenPages database instance.
<OPX_USER_NAME>	OpenPages application schema owner name.
<OPX_USER_PASSWORD>	OpenPages application schema owner password.

Results

You must recreate the index before filtering on the content of long string fields again. For details on creating a long string index, see “Create a Long String Index” on page 374.

Modifying the List of Stop Words

You can change the default list of stop words used by the Oracle Text feature. A stop word a word that does not get indexed. When querying an Oracle Text index for a stop word, Oracle Text won't return data for the query.

In the "Create a Long String Index" on page 374 script, we create a stopword list called OP_STOPLIST when creating the Oracle Text index. It is empty at the time of index creation if user doesn't make any changes to our scripts. We also provide a script called `CustomIndexing_ManageStopWords.sql` that enables user to add stop words into OP_STOPLIST.

Procedure

1. Open `CustomIndexing_ManageStopWords.sql` with a text editor
2. Add a stop word for each word you would like to add by copying the commented out sections listed below:

```
/*
    ADD_STOPWORD_TO_ARRAY
    (
    p_name               => 'me'
    );
    */
```

   For example, if you want to add the stop word "the", copy the section above, remove the comment sign, and replace "me" with "the" as below. Repeat the same step for each word you want to add.

```
  ADD_STOPWORD_TO_ARRAY
    (
    p_name               => 'the'
    );
```

   Stop words added to this file will not take effect until the next time you re-index. This file is used as the most updated list of stop words when the index is recreated. When running `CustomIndexing_Step2_IndexCreate.sql`, all current stop words in OP_STOPLIST are removed. It is a good idea to keep this file up to date.

String Concatentation Utility

String concatenation lets you merge up to 8 simple strings into a new long text field (long string data type). Long text fields have two sub categories - medium long and large long. Medium long can support a text size up to 32KB.

You must log in as an administrator to perform string concatenation. You can use any system with access to SQL*Plus that can connect to the OpenPages database server.

String concatenation is a database operation. A SQL template file is provided to specify parameters for the action. See "Running String Concatenation" on page 379 for the procedure.

For more information on long text fields, see "Working with Long String Fields" on page 142.

Running String Concatenation

The String Concatenation utility runs an SQL file that you edit to provide input and output parameters.

Important:

- The String Concatenation utility puts the system into System Administration Mode (SAM) prior to concatenating any fields. No other activity can happen while the script is running.
- You can concatenate into an existing long text field, but **only** if that field has not been used in any way. Attempting to concatenate into a long text field that has been used causes the utility to fail.

Tip: Run the script in preview mode (a setting in the `field_concat_template.sql` file) to check the results before doing the concatenation.

Procedure

1. Log on to a system as a user with Administrator privileges. You can use any system with access to SQL*Plus that can connect to the OpenPages database server.
2. Navigate to the `field-concat-utility` folder located in the `bin` directory:

   Where: `<OP_Home>` represents the installation location of the IBM OpenPages GRC Platform application.

   Windows `<OP_Home>\aurora\bin`

   By default `<OP_Home>` is `C:\OpenPages`

   AIX `<OP_Home>/aurora/bin`

   By default `<OP_Home>` is `/opt/OpenPages`

3. Copy the contents of the SQL template `field_concat_template.sql` into a new file.
4. Edit the new SQL file to provide the values necessary. Only edit the values in the declaration section of the SQL file. For details, see "About the String Concatenation SQL File" on page 380.

   Important: Many of the parameters specified in the SQL file have requirements, restrictions, and cautions noted. These are important for a successful concatenation.

   Tip: When editing your copy of the `field_concat_template.sql` file with multi-byte characters, and saving the file in Unicode, your editor may insert a Byte Order Mark (BOM) into the file. Some applications (such as a text editor or a browser) display the BOM as an extra line in the file, while others display unexpected characters, such as `ï»¿`. If you save the file in UTF-8 encoding (leaving the BOM in the file) and run the string concatenation script, you get an error message (`SP2-0734: unknown command beginning "ï»¿---------..."`), but the script continues to run without a problem. This error has no effect on the script running, but if you prefer not to see the error, save the file without a Byte Order Mark.
5. Execute the following command:

   Windows
   ```
   field_concat <SID> <op_db_user> <op_db_password>
     <field_concat_template_file>
   ```

AIX
```
field_concat.sh <SID> <op_db_user> <op_db_password>
  <field_concat_template_file>
```

Where:

Parameter name	Description
<SID>	The system ID or TNS alias for the OpenPages database instance.
<username>	The OpenPages application schema user name.
<password>	The OpenPages application schema owner password.
<field_concat_template_file>	The name of the SQL file created in step 3.

Tip: To see details on database operation messages, run the following SQL statement:

```
select exception_text from error_messages where ERROR_MESSAGE_ID = &ERROR_MESSAGE_ID;
```

Results

If the destination long text field does not exist, it is created and populated with values according to the values specified in the SQL file.

If the destination long text field exists, but is not used in any way, it is populated with values according to the values specified in the SQL file.

For details on the SQL file, see "About the String Concatenation SQL File."

About the String Concatenation SQL File

OpenPages includes a template SQL file (`field_concat_template.sql`). Use a copy of this file to specify the parameters to submit with the `field_concat` command.

Important: Many of the parameters specified in the SQL file have requirements, restrictions, and cautions noted. These are important for a successful concatenation.

See "Running String Concatenation" on page 379.

Parameters

Table 60. `field_concat_template.sql` Parameters

Parameter	Description
`l_actor_name`	The user name making the change. The user must log in as an administrator. The script puts the system into System Administration Mode (SAM) prior to concatenating any fields.

Table 60. field_concat_template.sql Parameters (continued)

Parameter	Description
l_field_group_name_src<#>	The name of the field group containing the simple string field. **Where**: <#> is a value from 01 to 08. **Important:** • l_field_group_name_src<#> and l_property_name_src<#> are always specified in pairs. • These parameters must have values specified in order. For example, l_field_group_name_src01 must have a value before l_field_group_name_src02 is specified. • Specified field groups must be associated with an object type.
l_property_name_src<#>	The name of the source simple string field. **Where**: <#> is a value from 01 to 08. **Important:** • The source must be a simple string. • At least one source must be specified. • The source must already exist • l_field_group_name_src<#> and l_property_name_src<#> are always specified in pairs. • These parameters must have values specified in order. For example, l_property_name_src01 must have a value before l_property_name_src02 is specified. • A property can only be specified once in the set of fields to concatenate. • Only the resource description system property is supported.

Table 60. `field_concat_template.sql` Parameters (continued)

Parameter	Description

`l_separator`	The separator to use between concatenated fields. The default separator is null.
	
	If you concatenate only one source into the destination, the separator character is not used.
	Important:
	• To use "&" as a separator, encode it as `chr(38)`.
	For example:
	`l_separator OP_GLOBALS.DB_Max_String_T := chr(38);`
	• The separator string can be no longer than 100 bytes.
	• If the destination field has a rich text display type, characters in the separator sequence must be encoded.
	For example, to represent a less-than sign ("<"), encode it as:
	`l_separator OP_GLOBALS.DB_Max_String_T := chr(38)||'lt ';`

`l_object_type_name`	The name of the object type containing the destination long text field. **Important:** The object type must be the same for the destination as it is for the source.
`l_field_group_name`	The name of the field group containing the destination long text field. **Important:** • The destination field group must exist. • The destination field group must be a customer field group, not a system field group.
`l_property_name`	The name of the destination field. **Important:** • The name destination field must either not exist, or if it does exist, must not used anywhere. • If the destination field does not already exist, the `l_large_text_length` parameter must be specified. • If the destination field does exist, it must be of data type `Long String`. • If the destination field is Rich Text, and source fields are a mix of Text and Rich Text, then there is the possibility that the concatenated value will not display properly in the UI. Such operations should be executed with caution.

Table 60. field_concat_template.sql Parameters (continued)

Parameter	Description
l_property_desc	The description of the destination long text field.
l_large_text_length	The length property of the destination field. The default is OP_OBJ_MODEL_MGR.g_dl_longtext_medium. **Important:** If the destination does not exist, this parameter must be specified, as either OP_OBJ_MODEL_MGR.g_dl_longtext_medium or OP_OBJ_MODEL_MGR.g_dl_longtext_large.
l_is_done_by_vendor	Set to true to add the concatenation to audit trail. The default is OP_Globals.sc_False. Valid values are: • OP_Globals.sc_True • OP_Globals.sc_False See "Auditing Configuration Changes" on page 388
l_remote_address	The remote address to perform the audit trail. The default is null. Any value is ignored if l_is_done_by_vendor is OP_Globals.sc_False.
l_remote_host	The remote host to perform the audit trail. The default is null. Any value is ignored if l_is_done_by_vendor is OP_Globals.sc_False.
l_preview_only	Set to true to only print the changes that will be made by script. No changes are actually made. The default is OP_Globals.sc_False. Valid values are: • OP_Globals.sc_True • OP_Globals.sc_False **Tip:** Run the script in preview mode (a setting in the field_concat_template.sql file) to check the results before doing the concatenation.

Table 60. field_concat_template.sql Parameters (continued)

Parameter	Description
l_override_objtp_logic	Set to true to override any logic applied to the object types, such as their relationships. The default is OP_Globals.sc_False. Valid values are: • OP_Globals.sc_True • OP_Globals.sc_False If l_object_type_name is left blank, and the source and destination field groups are associated to different object types, the script will fail unless you set this parameter to OP_Globals.sc_True. Each source field group and destination field group must associate with the same object type or set of object types. For example, the following scenario will fail unless this parameter is set to OP_Globals.sc_True: • Source field group A is associated to object types X and Y. • Source field group B is associated only to object type X. • Destination field group is associated only to object type X.

Sample

Note: The following sample includes only those declarative statements that are subject to your changes.

```
declare
  l_actor_name              ACTORINFO.NAME%type                 := 'OPAdmin';
  l_field_group_name_src01  BUNDLEDEFS.NAME%type                := 'QA10_SS_1';
  l_property_name_src01     PROPERTYDEFS.NAME%type              := 'QA10_Simple2';
  l_field_group_name_src02  BUNDLEDEFS.NAME%type                := 'QA10_LargeText';
  l_property_name_src02     PROPERTYDEFS.NAME%type              := 'QA10_S3';
  l_field_group_name_src03  BUNDLEDEFS.NAME%type                := 'Core Attributes';
  l_property_name_src03     PROPERTYDEFS.NAME%type              := 'Resource Description';
  l_field_group_name_src04  BUNDLEDEFS.NAME%type                := 'MG_7';
  l_property_name_src04     PROPERTYDEFS.NAME%type              := 'MG_S7';
  l_field_group_name_src05  BUNDLEDEFS.NAME%type                := 'MG_4';
  l_property_name_src05     PROPERTYDEFS.NAME%type              := 'MG_S4';
  l_field_group_name_src06  BUNDLEDEFS.NAME%type                := 'MG_5';
  l_property_name_src06     PROPERTYDEFS.NAME%type              := 'MG_S5';
  l_field_group_name_src07  BUNDLEDEFS.NAME%type                := 'MG_6';
  l_property_name_src07     PROPERTYDEFS.NAME%type              := 'MG_S6';
  l_field_group_name_src08  BUNDLEDEFS.NAME%type                := 'MG_3';
  l_property_name_src08     PROPERTYDEFS.NAME%type              := 'MG_S3';
  l_separator               OP_GLOBALS.DB_Max_String_T          := ',';
  l_object_type_name        ASSETTYPES.NAME%type                := 'SOXBusEntity';
  l_field_group_name        BUNDLEDEFS.NAME%type                := 'QA10_LargeText';
  l_property_name           PROPERTYDEFS.NAME%type              := 'TEST101';
  l_property_desc           PROPERTYDEFS.DESCRIPTION%type       := 'MGMGMGMGDescription';
  l_large_text_length       PROPERTYDEFS.DATA_LENGTH%type       := OP_OBJ_MODEL_MGR.g_dl_longtext_medium;
  l_is_done_by_vendor       OP_Globals.Flag_String_T            := OP_Globals.sc_False;
  l_remote_address          i18n_audit_trail.remote_address%type := '';
```

```
l_remote_host             i18n_audit_trail.remote_host%type    := '';
l_preview_only            OP_Globals.Flag_String_T             := OP_Globals.sc_False;
l_override_objtp_logic    OP_Globals.Flag_String_T             := OP_Globals.sc_False;
```

Chapter 15. System Maintenance

This chapter contains the following topics:

Updating URL Host Pointers for CommandCenter Reports

If, for example, you want to refresh a test environment from a production database or if you want to change port settings in a production environment, you must update the URL host pointers on the application server so that links in CommandCenter reports work properly.

You can update links in reports by modifying URL host pointer settings, and then propagating these reporting schema changes to the application server.

To update the reporting schema, you can do either of the following:

- Run an SQL script that incrementally updates the reporting schema with the changes (recommended).

  - OR -

- Use the IBM OpenPages application user interface to recreate the entire reporting schema.

Procedure

1. Open a browser window and log on to the IBM OpenPages application user interface as a user with administrator privileges.
2. Change the Object URL Generator settings as follows:
   a. From the menu bar, click the **Administration** menu and choose **Settings**.
   b. Expand the **OpenPages | Platform | Reporting Schema | Object URL Generator** folder hierarchy.
   c. Update the **Object Generator URL** settings in Table 61, as required, to point to the application server (such as a test application server). Make sure to click **Save** after modifying each setting.

Table 61. Object Generator URL Settings

Setting Name	Description
Host	The changed name of the application server. **Example** : `test-eng1`

Table 61. Object Generator URL Settings (continued)

Setting Name	Description
Port	The changed port number of the application server. **Example :** 7009 (Oracle WebLogic) or 10108 (IBM WebSphere®)
Protocol	The changed protocol for accessing the application server. Valid values are either `http` or `https`.

3. To update the changed URL setting on the application server (such as, a test application server) update the reporting schema using one of the following methods:
   - **Method 1:** Run the following SQL script to incrementally update the reporting schema (recommended):
     a. From a machine with SQL*Plus and access to the database server, log on to SQL*Plus as the IBM OpenPages database user (for example, `openpages`).
     b. Run the following SQL statements to update the reporting schema:

```
begin
OP_RPS_MGR.SET_DETAIL_PAGE_URL_IN_RPS_RT;
end;
/
```

     - OR -
   - **Method 2:** Recreate the entire reporting schema using the application user interface. For details, see "Creating or Re-creating the Reporting Schema" on page 60.

Auditing Configuration Changes

The IBM OpenPages GRC Platform provides you with the capability of tracking configuration changes made to your system through the CommandCenter generated *Configuration Audit Report*.

Accessing the CommandCenter Configuration Audit Report

To view and generate the *Configuration Audit Report*, you must have the CommandCenter reporting schema and framework enabled and configured on your system.

Procedure

1. From the menu bar, select **Reporting** and do one of the following:
   - Select **OpenPages V6, Audit Reports, Configuration**.
   - Click **All Reports**, and navigate to the OpenPages V6 folder (if necessary, click the plus sign to expand the folder tree). In the folder tree, expand the **Audit Reports, Configuration** folders.
2. Click **Configuration Audit** to run the report.
3. On the Configuration Audit Report page, specify the date range for the reporting data as follows:
   a. In the start date box, type a start date or click the calendar arrow and select a start date.
   b. In the end date box, type an end date or click the calendar arrow and select an end date.
   c. Click Finish to generate the report.

The CommandCenter Configuration Audit Report

The Configuration Audit Report tracks any metadata changes made to:

- Field Groups - such as modifications made to object field definitions and enumerated string values.
- Object Types - such as the inclusion of Field Groups and changes in parent and/or child object relationship rules (for example, cardinality setting changes or enabling/ disabling object type relationships).
- Application Text or Object Text - such as translation changes to locale-specific display labels for object types, object fields, and enumerated string values. You can enable or disable the auditing of translated text. By default, auditing is enabled. For details on enabling or disabling the auditing of translated text, see the topic "Setting Localization Options" on page 276.
- Profiles - such as modifying object views and showing or hiding object types and fields.
- Settings - such as non-machine specific settings contained in the OPX Repository.

Table 62 describes the various audited configuration changes contained in the report under the following column headings:

Table 62. Audit Configuration Column Headings

This report column...	Contains this type of data...
Object	The type of object that was modified.
Category	A category or classification under the object type.
Action Type	The type of action performed on the object.
Action Date	The date the action was performed.
Created by	The name of the user who performed the action.
Old Value	The value before it was modified.
New Value	The value after it was modified.

Changing Passwords and IP Addresses

You may need to update or change the Oracle or Oracle WebLogic system password, or a server IP address. When you do, you will also need to update the password in various places inside the OpenPages configuration files and property files.

This section contains the following topics:

Changing Oracle Password References

To change a password reference, you must do the following:

"Change Oracle Password References on the OpenPages Application and Workflow Servers" on page 390).

"Change Reporting Framework Password References" on page 392.

"Change Password References for CommandCenter Data Sources" on page 393).

If you need information about encrypting database passwords in the backup and restore utility environment files, see "Encrypting Database Passwords in the Backup-Restore Utility Environment Files" on page 334.

Before You Begin

Before you change password references for data sources in OpenPages, make sure you have the following:

- Administrative access to the following machines and application:
  - IBM OpenPages application server
  - IBM OpenPages CommandCenter server
  - IBM OpenPages CommandCenter portal
- The current and new password for the following database users:
  - IBM OpenPages database user
  - Workflow database user
  - Oracle WebLogic system account user

Change Oracle Password References on the OpenPages Application and Workflow Servers

The process for changing the database password on the IBM OpenPages application and workflow servers requires the following tasks:

"Modify the JDBC Data Source Password"

"Modify the Aurora Property File" on page 392

Important: Make a backup copy of each file before modifying it.

Modify the JDBC Data Source Password:

This task includes instructions for modifying the JDBC data source in the Oracle WebLogic Server Administration Console and IBM WebSphere Integrated Solutions Console for the application and workflow servers. Select the instructions that correspond to your particular environment.

Oracle WebLogic - Modify the JDBC Data Source Password:

Note: The information in this topic applies only to Oracle WebLogic environments.

Procedure

1. Stop all IBM OpenPages application services except for the following administrative service:

If changing the reference on this server...	Then only this service should be running...
application	`OpenPagesAdminServer`
workflow	`InterstageBPMAdminServer`

2. Open a browser window and log on to the Oracle WebLogic Server Administration Console as a user with administrative privileges.

   By default, the URL is `http://<host_name>:<port>/console`

Where:

<host_name> is the name of the server where Oracle WebLogic is installed.

<port> is the server port number. By default, the installation port numbers are:

- 7001 for the IBM OpenPages server (IBM OpenPages Domain)
- 49901 for the workflow server (IBPMDomain)

3. In the Change Center pane of the Console, click **Lock & Edit** (if not already selected).
4. On the Home page, in the Domain Configurations pane, under the heading **JDBC**, click the **Data Sources** link.
5. On the Summary of JDBC Data Sources page, depending on your server selection, do the following:

For updating this server...	Click this link in the Data Sources table...
application	IBM OpenPages Data Source
workflow	InterstageBPM-CDataSource

6. On the Settings for <server-name>Data Source page, do the following:
   a. On the **Configuration** tab, click the **Connection Pool** tab.
   b. In the **Password** box, type a new password.
   c. In the **Confirm Password** box, type the same password again.
   d. When finished, click **Save**.
   e. In the Change Center pane, click **Activate Changes** and log out.

   Note: The password becomes encrypted when you save your change.

WAS - Modify the JDBC Data Source Password:

Note: The information in this topic applies only to IBM WebSphere environments.

Procedure

1. Open a browser window and log on to the IBM WebSphere Integrated Solutions Console as a user with administrative privileges.

   By default, the URL is http://<host_name>:<port>/ibm/console

   Where:

   <host_name> is the name of the server where the IBM WebSphere is installed.

   <port> is the server port number. By default, the installation port numbers are:

   - 9060 for the IBM OpenPages server (IBM OpenPages Cell)
   - 9061 for the workflow server (IBPMCell)
2. Expand **Resources** then **JDBC** in the left pane and click the **Data sources** link.
3. In the Data sources pane, depending on your server selection, do the following:

For updating this server...	Click this link in the Data sources table...
application	CWTxDataSourceXA
workflow	iFlowDataSourceOracle

4. On the **Configuration** tab, under the **Related Items** heading, click the link for **JAAS - J2C authentication data**.
5. In the JAAS - J2C authentication data pane, depending on your server selection, do the following:

For updating this server...	Click this link in the JAAS-J2C authentication data table...
application	OpenPages JDBC authentication entry
workflow	iFlowAuthDAOracle

6. In the pane for the selected authentication data table, under the **General Properties** heading, do the following:
   a. In the **Password** box, type the new password.
   b. When finished, click **Apply**.
7. In the **Messages** box, click **Save**.
8. Click **OK**.

Modify the Aurora Property File:

Note: The information in this topic applies to Windows and AIX environments.

Procedure

1. Open a command or shell window and navigate to the <OP_Home>|aurora|conf directory.

Where: <OP_Home> represents the installation location of the IBM OpenPages GRC Platform application. By default, this is:	
Windows	C:\OpenPages
AIX	/opt/OpenPages

2. Locate the aurora.properties file in the conf directory and do the following:
   a. Make a backup copy of the file before modifying it.
   b. Open the file in a text editor of your choice.
   c. Search the file for the string 'database.PASSWORD'.
   d. Change the value following the equal sign to the new password.
   e. Save your changes and exit the editor.

      Note: The password becomes encrypted when the services are restarted.

Change Reporting Framework Password References

Note: The information in this topic applies to Windows and AIX environments.

If you change the password of the user account that is used by CommandCenter for updating the reporting framework, you must manually modify the password value in the framework.properties file on the CommandCenter server, and then restart services to re-encrypted the password.

Procedure

1. Log on to the CommandCenter server as a user with administrative permissions.
2. Stop the OpenPages Framework Model Generator service.
3. Navigate to the CommandCenter|framework|conf folder.
   By default, the path is:

   Windows C:\OpenPages\CommandCenter\framework\conf

AIX /opt/OpenPages/CommandCenter/framework/conf

4. Locate the framework.properties file in the conf folder and do the following:
   a. Make a backup copy of the file before modifying it.
   b. Open the framework.properties file in a text editor of your choice.
   c. Locate the following code lines in the file:

      ```
      op.password=<password value>
      op.user=OpenPagesAdministrator (this is the default user)
      ```

      Where: <password value> is the password that corresponds to the user account value in the op.user property.
   d. Edit the password property with the new value (the new password will be in clear text). If you also changed the user account, edit that value as well.
   e. When finished, save the change to the file.
5. Restart the OpenPages Framework Model Generator service.

   Note: The passwords will be automatically re-encrypted the next time the service accesses the files.
6. Update the reporting framework (see "Updating the Reporting Framework" on page 64).
7. When finished, update the data source password for the reporting framework (see "Change Password References for CommandCenter Data Sources").

Change Password References for CommandCenter Data Sources

The following procedure describes how to manually update the signon password for the IBM OpenPages user account to access the Oracle data source.

Depending on the type of installation, one or both of the following Oracle data source links will be displayed in the IBM Cognos Administration tool for the CommandCenter reporting framework:

This data source...
: **Is used for this reporting framework...**

OpenPages DataSource
: Reporting Framework V6

Oracle Native Driver
: Legacy Reporting Framework (upgraded systems only)

Note: Both the OpenPages DataSource and Oracle Native Driver data sources connect to the same database repository and use the same authentication information (signons).

Procedure

1. Open a browser window and log on to the CommandCenter portal as a user with administrative privileges.

   By default, the URL is http://<server_name>/cognos8.

   Where: <server_name> is the name of the CommandCenter server
2. Do one of the following to launch IBM Cognos Administration:
   - If the Cognos splash page appears, then click the **Administer IBM Cognos Content** link.

- If the IBM Cognos Connection page appears, then click **Launch** and select **IBM Cognos Administration**.

3. On the **Configuration** tab, click **Data Source Connections** in the left pane (if not already selected).
4. On the Directory > Cognos page, click the **More** link in the same row as the data source you want (for example, `OpenPages DataSource`).
5. On the Perform an Action page, under **Available actions**, click the **View connections** link.
6. On the **Directory** > **Cognos** > **<** `name of data source` > page, click the **More** link in the same row as the selected data source.
7. On the Perform an Action page for the data source, under **Available actions**, click the **View signons** link.
8. On the **Directory** > **Cognos** > **<** `name of data source` **>** signons page, do the following:
   a. Under the **Actions** column, click the '**Set properties - <** `name of data source` **>**' icon.
   b. On the **Set properties-<** `name of data source` > page, click the **Signon** tab.
9. On the **Signon** tab:
   a. Click the **Edit the signon** link.
   b. Update the password.
   c. When finished, click **OK**.

Changing the Oracle WebLogic Password for the IBM OpenPages and Workflow Accounts

To improve security, Oracle recommends frequently changing the 'system' user account password that was set during installation. It is also recommended that every Oracle WebLogic Server deployment (including managed application servers) have a unique password.

Important: The Oracle Weblogic passwords for both the OpenPages and workflow accounts should be changed to the same value.

Procedure

1. Stop all services as follows:
   - When changing the Oracle WebLogic password for the OpenPagesAdminServer, stop all OpenPages managed servers and workflow servers. The OpenPagesAdminServer must be running. If you stopped the OpenPagesAdminServer, restart it.
   - When changing the Oracle WebLogic password for the workflow server, stop all workflow managed servers and OpenPages servers, including the OpenPagesAdminServer. The workflow Admin Server must be running. If you stopped the workflow Admin Server , restart it.
2. Open a browser window and log on to the Oracle WebLogic Server Administration Console as a user with administrative privileges.

   By default, the URL is `http://<host_name>:<port>/console`

   Where:

   `<host_name>` is the name of the server where Oracle WebLogic is installed.

   `<port>` is the server port number. By default, the installation port numbers are:
   - `7001` for the IBM OpenPages server (`IBM OpenPages Domain`)

- 49901 for the workflow server (IBPMDomain)

3. In the Change Center pane of the Console, click **Lock & Edit** (if not already selected).
4. On the Home page, in the Domain Configurations pane, under the heading **Your Application's Security Settings**, click the **Security Realms** link.
5. On the **Summary of Security Realms** page, click the **myrealm** link in the Realms table.
6. On the **Settings for myrealm** page, click the **Users and Groups** tab.
7. In the **Users and Groups** pane:
   a. Click the **Users** tab (if not already selected).
   b. Click the link for the 'system' user account in the Users table.

      By default, this is weblogic.
8. On the **Settings for <** user-name > page:
   a. Click the **Passwords** tab.
   b. In the **New Password** box type a new password.
   c. In the **Confirm New Password** box type the new password again.
   d. When finished, click **Save**.
9. Click on **Release Configuration** and log out of the console.
10. Stop the Admin server.
11. Make a backup copy of the boot.properties file.

    For the OpenPages server, the boot.properties file is in <OP_Home>\OpenPagesDomain.

    For the workflow server, the boot.properties file is in <Workflow_Home>\IBPMDomain.
12. Edit boot.properties and change the password parameter in the file (make sure there are no spaces or other characters).

    Note:

    - Do not change or add anything else in this file.
    - The server will encrypt the new password in the file after restart.

    Example:

    When you first open the boot.properties file, it would look something like this (the values are encrypted):

    ```
    #Fri Apr 13 13:58:53 EDT 2012
    password={AES}J7ugLj8LSt1wjn/p0cSRT//fBiL+HZNoxNVWYJ2JX4I\=
    username={AES}7MbsTqLYf8ibEWPqbPUK/KjHehv8grHK0OQ8VGiuB98\=
    ```

    You would edit the password parameter, with the password of your choice, replacing everything after "password=" so the parameter would look something like this:

    ```
    #Fri Apr 13 13:58:53 EDT 2012
    password=newPassword
    username={AES}7MbsTqLYf8ibEWPqbPUK/KjHehv8grHK0OQ8VGiuB98\=
    ```
13. Save and close the boot.properties file.
14. Make a backup copy of the configfile.secure file.

    The configfile.secure file is in <OP_Home>\bin.
15. Edit configfile.secure and change the weblogic.management.password parameter in the file to match the new password you entered into the boot.properties file.

Note:

- Do not change or add anything else in this file.
- The server will encrypt the new password in the file after restart.

Example:

When you first open the `configfile.secure` file, the `weblogic.management.password` parameter would look something like this (the values are encrypted):

```
weblogic.management.password={AES}Jd60DLKIF6XTanLvAwQzzezN8iYf65sNlFEt8ZiwTNA\=
```

Edit the `weblogic.management.password` parameter to match the password you entered into the `boot.properties` file, replacing everything after "weblogic.management.password=" so the parameter would look something like this:

```
weblogic.management.password=newPassword
```

16. Rename all the domain folders for OpenPages and Workflow as follows:
    - **OpenPages**

      Rename all the OpenPages domain folders in `<OP_Home>\OpenPagesDomain\servers` leaving the "OpenPagesAdminServer".
    - **Workflow**

      Rename all the workflow domain folders in `<Workflow_Home>\IBPMDomain\servers` leaving the "AdminServer".

    The purpose of renaming the domain folders is to backup the original domains and ensure that the new password information is used.
17. Start the domains **manually** from the command line.
    - **OpenPages**
      a. Start the Admin server with `startWebLogic.cmd`.

         On success, an examination of `boot.properties` would show the `password` value encrypted, and you can log into Oracle WebLogic with the new password.

      b. From `<OP_Home>\OpenPagesDomain\bin` run the following command for each IBM OpenPages instance on this system: `startOPServer.cmd <server-name>-OpenPagesServer<#>`

         Where: `<server-name>` is the name of the server, and `<#>` is the number of the managed server.

         Example:

         ```
         startOPServer.cmd managedserver01-OpenPagesServer1
         startOPServer.cmd managedserver01-OpenPagesServer2
         ```
    - **Workflow**
      a. Start the Admin server with `startWebLogic.cmd`.

         On success, an examination of `boot.properties` would show the `password` value encrypted, and you can log into Oracle WebLogic with the new password.

      b. From `<Workflow_Home>\IBPMDomain\bin` run the following command for each IBM OpenPages instance on this system: `startIBPMServer.cmd <server-name>-InterstageBPMCS<#>`

         Where: `<server-name>` is the name of the server, and `<#>` is the number of the managed server.

         Example:

         ```
         startIBPMServer.cmd managedserver01-InterstageBPMCS1
         startIBPMServer.cmd managedserver01-InterstageBPMCS2
         ```

18. Repeat steps 11 - 17 on the non-admin servers as well.

    Note:
    - When using an administration server and managed servers in a domain, the managed server must always use the password for the administration server in the domain. Always change the password for the administration server through the Oracle WebLogic Server Administration Console. When the Oracle WebLogic Server is rebooted, the new password is propagated to all the managed servers in the domain.
    - Not all changes take effect immediately—some require a restart of IBM OpenPages services (see "Starting and Stopping OpenPages Application Servers" on page 465).
19. In the Change Center pane, click **Release Configuration**.
20. Restart all services.

Changing the Workflow Server Multicast IP Address in Oracle WebLogic

Note: The information in this topic applies only to Oracle WebLogic environments.

The Fujitsu Interstage BPM software uses multicasting to communicate between workflow members in a clustered environment. To update the IBM OpenPages workflow server multicast IP address in Oracle WebLogic, use the following instructions.

Note:
- The multicast IP address must be unique within the network address space.
- In a horizontal clustered environment, the same multicast IP address must be used on all member workflow servers.

Procedure

1. Verify that the workflow service (`InterstageBPMAdminServer`) is running.
2. Open a browser window and log on to the `IBPMDomain` in the Oracle WebLogic Server Administration Console as a user with administrative privileges.

   By default, the URL is http://<host_name>:49901/console

   Where:

   `<host_name>` is the name of the server where Oracle WebLogic is installed
3. In the Change Center pane of the Console, click **Lock & Edit** (if not already selected).
4. Expand the **Environment** tree in the Domain Structure pane and click **Clusters**.
5. On the Summary of Clusters page in the Clusters table listing, click the `InterstageBPMCluster` link.
6. On the Settings for InterstageBPMCluster page, do the following:
   a. Click the **Configuration** tab (if not already selected).
   b. Under **Configuration,** select the **Messaging** tab.
   c. Change the value in the **Multicast Address** field.
   d. Click **Save**.
7. Click the **Activate Changes** button in the **Change Center** to implement the changes and log out of the Console.

8. Restart all services. See "Starting and Stopping OpenPages Application Servers" on page 465 for details.

Updating the Oracle Enterprise Manager Database Control Tool

If either the static IP address of the database server changes or the database host name changes, then the web-based Oracle Enterprise Manager Database Control tool (`https://<server_name>:<port>/em`), which is used for managing the Oracle database, will no longer function properly and requires reconfiguration.

Note: The Oracle database server requires a static IP address.

Before You Begin

Before you run the commands to resolve the configuration change, make sure you have the following information:

- Database SID
- Listener port number
- Password for SYS user
- Password for SYSMAN user
- Password for DBSNMP user
- Email address for notifications (optional)
- Outgoing Mail (SMTP) server for notifications (optional)

Resolving Configuration Changes in the Tool

To resolve configuration changes so the Oracle Enterprise Manager Database Control tool functions properly, you must first deconfigure and then reconfigure the tool as follows.

Procedure

1. Open a command or shell window.
2. Change directory to `ORACLE_HOME|bin` as follows:

   Windows cd %ORACLE_HOME%\bin
   AIX cd $ORACLE_HOME/bin

3. Type the following command to deconfigure the Oracle Enterprise Manager Database Control tool:

   ```
   emca -deconfig dbcontrol db -repos drop
   ```

4. Type the following command to reconfigure the Oracle Enterprise Manager Database Control tool:

   ```
   emca -config dbcontrol db -repos create
   ```

Changing the IP Address of an Application Server

If you change the application server's IP address, or the server uses more than one network interface card (NIC) to create multiple network interfaces, you need to modify the Windows `hosts` file to point to the primary NIC.

In the case of multiple NICs, without specifying the IP address of each NIC, the Oracle WebLogic or IBM WebSphere Server may listen on the wrong NIC.

On Windows, the Oracle WebLogic server picks up the fully qualified domain name from the first entry in the %SYSTEMROOT%\system32\drivers\etc\hosts file.

On AIX, the IBM WebSphere server picks up the fully qualified domain name from the first entry in the /etc/hosts file.

Procedure

1. Log on to the IBM OpenPages application server as a user with administrative permissions.
2. Open a command window (using the **Run as Administrator** option), or a shell window.
3. Navigate to the following directory:

   Windows:
   %SYSTEMROOT%\system32\drivers\etc\

   AIX: /etc
4. Open the hosts file in a text editor of your choice.
5. On a separate line, enter the IP address and host name of the primary NIC.
6. If there are multiple NICs, enter the IP address and host name of the other NICs on that server on separate lines.
7. Save and close the file.
8. Stop the IBM OpenPages services.
9. For Oracle WebLogic servers only, delete the OpenPages and Workflow folders which represent the nodes on the server.
   a. Navigate to <OP_Home>\OpenPagesDomain\servers. Where <OP_Home> represents the installation location of the IBM OpenPages GRC Platform application. By default, this is C:\OpenPages.
   b. Delete the OpenPagesAdminServer folder, if it exists.
   c. Delete the folders that contain the server name which represents the nodes on the server (<servername>-OpenPagesServer<#>). For example, MyServer01-OpenPagesServer1.
   d. Navigate to <Workflow_Home>\IBPMDomain\servers. Where <Workflow_Home> represents the installation location of the Fujitsu Interstage BPM server. By default, this is C:\Fujitsu\InterstageBPM.
   e. Delete the AdminServer folder, if it exists.
   f. Delete the folders that contain the server name which represents the nodes on the server (<servername>-InterstageBPMCS<#>) For example, MyServer01-InterstageBPMCS1.
10. Start the IBM OpenPages services. For information on starting and stopping services, see Chapter 16, "Starting and Stopping Servers," on page 465

Changing Database References

If you have, for example, upgraded from an old database server to a new one, migrated from a non-RAC to a RAC environment, or are moving from a shared database environment to a standalone environment, then you must change several references on the IBM OpenPages GRC Platform application and reporting servers to point from the old to the new database instance.

To change database references, you must do the following:

"Modify the Connection URL for the JDBC Data Source" on page 400

"Modify Database References in the Application Configuration Files" on page 402

"Modify Database Connection References for the Reporting Server" on page 404

Before You Begin

Before you change database references, make sure you have the following:

- Administrative access to the following machines and application:
  - IBM OpenPages application server
  - IBM OpenPages CommandCenter server
  - IBM OpenPages CommandCenter portal
  - Oracle WebLogic or WAS (if global security is enabled) system account user and password
- The Oracle System Identifier (SID) of the new database instance.

Modify the Connection URL for the JDBC Data Source

This task includes instructions for modifying the JDBC data source in the Oracle WebLogic Server Administration Console and IBM WebSphere Integrated Solutions Console for the application and workflow servers. Select the instructions that correspond to your particular environment.

Oracle WebLogic - Modifying the Data Source Connection URL for Oracle WebLogic

Note: The information in this topic applies only to Oracle WebLogic environments.

Procedure

1. Stop all IBM OpenPages application services except for the following administrative service:

If changing the reference on this server...	Then only this service should be running...
application	`OpenPagesAdminServer`
workflow	`InterstageBPMAdminServer`

2. Open a browser window and log on to the Oracle WebLogic Server Administration Console as a user with administrative privileges.

   By default, the URL is `http://<host_name>:<port>/console`

   Where:

   `<host_name>` is the name of the server where Oracle WebLogic is installed.

   `<port>` is the server port number. By default, the installation port numbers are:

   - `7001` for the IBM OpenPages server (`IBM OpenPages Domain`)
   - `49901` for the workflow server (`IBPMDomain`)
3. In the Change Center pane of the Console, click **Lock & Edit** (if not already selected).
4. On the Home page, in the Domain Configurations pane, under the heading **JDBC**, click the **Data Sources** link.
5. On the Summary of JDBC Data Sources page, depending on your server selection, do the following:

For updating this server...	Click this link in the Data Sources table...
application	`IBM OpenPages Data Source`

For updating this server...	Click this link in the Data Sources table...
workflow	InterstageBPM-CDataSource

6. On the Settings for <server-name>Data Source page, do the following:
   a. Click the **Configuration** tab (if not already selected).
   b. Click the **Connection Pool** tab.
   c. In the **URL** box, type the new database connection URL. The URL format will look similar to the following:

      jdbc:oracle:thin:@//<host-name>:<port>/<SID>

      Where:

      <host-name> is the host name of the server where Oracle WebLogic is installed.

      <port> is the server port number.

      <SID> is the Oracle System Identifier (for example, OP11G).

      Example

      jdbc:oracle:thin:@//eng11:7001/OP11G
   d. When finished, click **Save**.
   e. In the Change Center pane, click **Activate Changes** and log out.

      Note: The password becomes encrypted when you save your change.

WAS - Modifying the Data Source Connection URL for IBM Websphere:

Note: The information in this topic applies only to IBM WebSphere environments.

Procedure

1. Open a browser window and log on to the IBM WebSphere Integrated Solutions Console as a user with administrative privileges.

   By default, the URL is http://<host_name>:<port>/ibm/console

   Where:

   <host_name> is the name of the server where the IBM WebSphere is installed.

   <port> is the server port number. By default, the installation port numbers are:
   - 9060 for the IBM OpenPages server (IBM OpenPages Cell)
   - 9061 for the workflow server (IBPMCell)
2. Expand **Resources** then **JDBC** in the left pane and click the **Data sources** link.
3. In the Data sources pane, depending on your server selection, do the following:

For updating this server...	Click this link in the Data sources table...
application	CWTxDataSourceXA
workflow	iFlowDataSourceOracle

4. On the **Configuration** tab in the **Data sources** > **<Data-source-name** right pane, do the following:
   a. Navigate to the heading **Common and required data source properties**.
   b. In the **URL** box, type the new database connection URL. The URL format will look similar to the following:

      jdbc:oracle:thin:@//<host-name>:<port>/<SID>

      Where:

<host-name> is the host name of the server where the IBM WebSphere is installed.

<port> is the server port number.

<SID> is the Oracle System Identifier (for example, OP11G).

Example

```
jdbc:oracle:thin:@//eng11:1521/OP11G
```

c. When finished, click **Apply**.

5. In the **Messages** box, click **Save**.
6. Click **OK**.

Modify Database References in the Application Configuration Files

Note: The information in this topic applies to Windows and AIX environments.

Use the following instructions to update database references in these files: aurora.properties, setIBPMEnv, and op-backup-restore.env. Once the values are updated, you will need to restart all administrative and managed servers to effect the changes.

Modify the Database Reference in the Aurora Properties File Procedure

1. Open a command or shell window and navigate to the <OP_Home>|aurora|conf directory.

Where: <OP_Home> represents the installation location of the IBM OpenPages GRC Platform application. By default, this is:	
Windows	C:\OpenPages
AIX	/opt/OpenPages

2. Locate the aurora.properties file in the conf directory and do the following:
   a. Make a backup copy of the file before modifying it.
   b. Open the file in a text editor of your choice.
   c. Search the file for the string 'database.URL'.
   d. Change the value following the equal sign to the new database connection URL. The URL format will look similar to the following:

      ```
      database.URL=jdbc\:oracle\:thin\:@//<host-name>\:<port>/<SID>
      ```

      Example

      ```
      database.URL=jdbc\:oracle\:thin\:@//eng11\:1521/OP11G
      ```

   e. Save your changes and exit the editor.

Modify the Database Reference in the Workflow Command File Procedure

1. Open a command or shell window and navigate to the <Workflow_Home>|server|deployment|bin directory.

Where: <Workflow_Home> represents the installation location of the Fujitsu Interstage BPM server. By default, this is:	
Windows	c:\Fujitsu\InterstageBPM

AIX	/opt/Fujitsu/InterstageBPM

2. Locate the following command file in the bin directory:

   Windows setIBPMEnv.cmd
   AIX setIBPMEnv.sh

3. Do the following:
   a. Make a backup copy of the file before modifying it.
   b. Open the file in a text editor of your choice.
   c. Search the file for the string 'set dbUrl'.
   d. Change the value following the equal sign to the new database connection URL. The URL format will look similar to the following:

      ```
      set dbUrl=jdbc:oracle:thin:@//<host-name>:<port>/<SID>
      ```

      Example

      ```
      set dbUrl=jdbc:oracle:thin:@//eng11:1521/OP11G
      ```

   e. Save your changes and exit the editor.

Modify Database References in the IBM OpenPages Backup and Restore Environment File

Procedure

1. Open a command or shell window and navigate to the <OP_Home>|aurora|bin directory.

Where: <OP_Home> represents the installation location of the IBM OpenPages GRC Platform application. By default, this is:	
Windows	C:\OpenPages
AIX	/opt/OpenPages

2. Locate the op-backup-restore.env file in the bin directory and do the following:
   a. Make a backup copy of the file before modifying it.
   b. Open the file in a text editor of your choice.
   c. Search the file for the following strings:
      - DATABASE_URL=jdbc:oracle:thin:@//<host-name>:<port>/<SID>
      - DB_SID=<SID>
      - DB_ALIAS=<SID>
   d. Change the value following the equal sign to the new database connection URL and SID.

      Example

      ```
      DATABASE_URL=jdbc\:oracle\:thin\:@//eng11\:1521/OP11G
      DB_SID=OP11G
      DB_ALIAS=OP11G
      ```

   e. Save your changes and exit the editor.

Restart All Application Servers

When finished modifying the database reference values in the files, restart all administrative and managed servers to effect the changes. See "Starting and Stopping OpenPages Application Servers" on page 465 for details.

Modify Database Connection References for the Reporting Server

Note: The information in this topic applies to Windows and AIX environments.

Use the following instructions to update database references in Cognos Connection, Cognos Configuration, and the `op-backup-restore.env` file. Once the values are updated, you will need to restart all administrative and managed servers to effect the changes.

Modify Database Connection References in Cognos Connection

You will need to change the database connection reference values for both the `IBM OpenPages DataSource` and `Oracle Native Driver`.

Procedure

1. Ensure that both the IBM OpenPages GRC Platform and IBM Cognos servers are running.
2. Open a browser window and log on to the IBM OpenPages GRC Platform application user interface as a user with administrative permissions.
3. From the navigation bar, select **Reporting** and click **Cognos Connection**.
4. On the IBM Cognos Connection window, click the **Launch** link and select **IBM Cognos Administration**.
5. In the IBM Cognos Administration window, click the **Configuration** tab.
6. On the Directory > Cognos page, click the link for the **OpenPages DataSource**.
7. On the Directory > Cognos > <data-source-name> page, do the following:
   a. Under the **Actions** column, click the '**Set properties - OpenPages DataSource**'  icon.
   b. On the Set properties - OpenPages DataSource page, click the **Connection** tab.
8. On the **Connection** tab, do the following:
   a. Next to the **Connection String** box, click the pencil icon.
   b. On the Edit the connection string - Oracle page, edit the SID value in the **SQL*Net connect string** field.
   c. When finished, click **OK**.
9. Return to the Directory > Cognos page, and click the link for the **Oracle Native Driver** and repeat Steps 7-8 for the Oracle Native Driver.
10. When finished, exit Cognos Connection.

Modify the Database Reference in the CommandCenter Backup and Restore Environment File

Procedure

1. Open a command or shell window and navigate to the `<CC_Home>|tools|bin` directory.

   Where: `<CC_Home>` represents the installation location of the CommandCenter application.

Windows <CC_Home>\tools\bin

By default, <CC_Home> is C:\OpenPages\CommandCenter

AIX <CC_Home>/tools/bin

By default, <CC_Home> is /opt/OpenPages/CommandCenter

2. Locate the op-cc-backup-restore.env file in the bin directory and do the following:
   a. Make a backup copy of the file before modifying it.
   b. Open the file in a text editor of your choice.
   c. Search the file for the string 'DB_ALIAS'.
   d. Change the value following the equal sign to the new database SID. The format will look similar to the following:

      DB_ALIAS=<SID>

      Example

      DB_ALIAS=OP11G
   e. Save your changes and exit the editor.

Modify Database Connection References in Cognos Configuration

Procedure

1. Log on to the reporting server as a user with administrative privileges.

   Note: For AIX installs, log on as a non-root user.
2. Start the IBM Cognos Configuration tool as follows:
   a. Open a Command Prompt window (using the **Run as Administrator** option) or AIX shell and navigate to the <Cognos_Home>|bin64 directory.

Where: <Cognos_Home> represents the installation location of the Cognos application. By default, this is:	
Windows	C:\OpenPages\Cognos\cognos\c8
AIX	/opt/OpenPages/Cognos/cognos/c8_64

   b. Execute one of the following commands to open the tool:

      Windows cogconfig.bat

      AIX ./cogconfig.sh

3. In the left pane, do the following:
   a. Expand **Data Access** (if not already expanded).
   b. Under **Content Manager**, click **cognos8**.
4. In the right pane, modify the values for the following properties:
   a. Database server and port number (for example, eng11:1527).
   b. User ID and password
   c. Service name (for example, OP11G).
5. When finished, exit from Cognos Connection.

Restart the CommandCenter Server

When finished modifying the database reference values in the files, restart the CommandCenter server to effect the changes. See "Starting and Stopping the CommandCenter Server" on page 474 for details.

Changing Default Port Numbers

The IBM OpenPages GRC Platform installer sets several default ports during installation, such as the ports for the OpenPages server and the workflow server.

After installing IBM OpenPages GRC Platform, you can change the OpenPages ports to a different ports, if needed. For example, in the event of a port conflict, where another application is using these port ranges, you can change the OpenPages ports to avoid the conflict.

In the case of a port conflict, we recommend that you change all of the OpenPages application and workflow (IBPM) server ports to a new range by following the instructions in this section.

Important:

- Do not change the port number for the OpenPages administrative server or the workflow administrative sever.

  By default, the OpenPages administrative port for Windows/Oracle WebLogic Server are 7001 and 49901 respectively. The administrative port for AIX/IBM WebSphere Application Server, the administrative ports are 9060 and 9061.
- To modify port numbers on other application servers in a cluster, you must repeat the following tasks on each cluster member.

Task Overview for Changing Default Port Numbers

The following provides an overview of the tasks for changing port numbers for IBM OpenPages application and workflow servers.

Check Port Number Availability

Before changing the port numbers, make sure that the new ports you are going to use are available.

To determine if another application is using a specific port, log onto the application server where you need to change the port. Open a command or shell window and execute the following command:

Windows

```
netstat -an | findstr <port number>
```

AIX

```
netstat -an | grep <port_number>
```

Changing OpenPages Application Ports for an Oracle WebLogic Server Environment

Note: The information in this topic applies only to Oracle WebLogic environments.

If your OpenPages environment uses an Oracle WebLogic Server, use these steps to complete the task Change Port Values for OpenPages and Workflow Servers.

To change the port used by the IBM OpenPages application, launch the Oracle WebLogic Server Administration Console and change the ports within the application server.

Because the locations where you need to specify updated port numbers differ based on which port(s) you change, review each task below to make sure you changed the port in all required locations.

- "Stop the IBM OpenPages Application Server"
-

Stop the IBM OpenPages Application Server

Before changing the ports, make sure that the managed IBM OpenPages application server you are working with is stopped. Only the IBM OpenPages admin and workflow admin servers must be running.

Important: DO NOT use the `stopAllServers` script, as the script will attempt to stop any other applications associated with OpenPages ports.

Update Port Numbers in the Administration Console

Use the following steps to change the port number for the OpenPages application in the Oracle WebLogic Server Administration Console.

Procedure

1. Open a browser window and log on to the Oracle WebLogic Server Administration Console for OpenPages as a user with administrative privileges.

   By default, the URL is http://<server_name>:7001/console

   Where:

   <server_name> is the name of the server where Oracle WebLogic Server is installed and 7001 is the default OpenPages admin port.
2. In the Change Center pane of the Console, click **Lock & Edit** (if not already selected).

Update the OpenPages Application Server Listen Port:

Procedure

Change the port numbers for the OpenPages application server as follows:

1. In the Console's Domain Structure pane, expand the **Environment** tree and click **Servers**.
2. On the Summary of Servers page, click the **Configuration** tab (if not already selected).
3. In the Servers table listing, click the name of the application server for which you want to change port numbers. For example:

   <server_name>-OpenPagesServer<#>

   Where:

   <server_name> is the name of the application server.

   <#> is the number of the server.
4. On the **Settings for <Server_Name>** page for the selected server, on the **General** tab, change the value in the following fields:

   Listen Port - the port used by the OpenPages application. By default, this port is 7009.

   SSL Listen Port - the SSL port used by the OpenPages application. By default, this port is 7010.

   Important: The SSL Listen Port must be the port number following the Listen Port.
5. Click **Save**.

Update the Ports for the Messaging Bridge Between the OpenPages Application Server and the Workflow Server:

Each IBM OpenPages application server is associated with a workflow server. After changing the IBM OpenPages application port number, you must update the port numbers for the workflow server messaging bridge on the IBM OpenPages server, which allows the IBM OpenPages server to exchange JMS messages with the workflow server.

There are two listings for each OpenPages instance. Each server bridge needs to be updated.

Example

```
server01-OpenPagesServer1-OP2IBPMBridge
server01-OpenPagesServer1-OPInternalBridge
```

Procedure

1. In the Console's **Domain Structure** pane, expand the **Services** tree then **Messaging** in the left pane and click **Bridges**.
2. In the Bridges table listing on the **Summary of Messaging Bridges** page, do the following:
   a. Locate the server for which you need to change the port in the **Name** column. There are two listings in the table for each OpenPages instance. Each server bridge needs to be updated.
   b. In the **Source Bridge Destination** column, click the `OP2IBPMBridgeSource` entry for the application server you want to configure.

      Example : `server01-OpenPagesServer1-OP2IBPMBridgeSource`
3. On the **Settings for <Server_Name>-OP2IBPMBridgeSource** page, do the following:
   a. Change the port value in the **Connection URL** field to the new OpenPages application port.
   b. Click **Save**.
   c. Click the browser **Back** button or click the **Summary of Messaging Bridges** link at the top of the page to return to the **Summary of Messaging Bridges** page.
4. In the **Source Bridge Destination** column, click the `OPInternalBridgeSource` entry for the application server you want to configure.

   Example :
   `server01-OpenPagesServer1-OPInternalBridgeSource`
5. On the **Settings for <Servert_Name>-OPInternalBridgeSource** page, do the following:
   a. Change the port value in the **Connection URL** field to the new OpenPages application port.
   b. Click **Save**.
   c. Click the browser **Back** button or click the **Summary of Messaging Bridges** link at the top of the page to return to the **Summary of Messaging Bridges** page.
6. In the **Target Bridge Destination** column, click the `OPInternalBridgeTarget` entry for the application server you want to configure.

   Example :
   `server01-OpenPagesServer1-OPInternalBridgeTarget`
7. On the **Settings for <Server_Name>-OPInternalBridgeTarget** page, do the following:
   a. Change the port value in the **Connection URL** field to the new OpenPages application port.
   b. Click **Save**.
8. If you need to change the ports for any other OpenPages instance on this server, repeat these steps for each.
9. Click the **Activate Changes** button in the **Change Center** to implement the changes.

Update the Ports for the Messaging Bridge Between the Workflow Server and the OpenPages Application Server:

You must also update the port numbers for the messaging bridge on the workflow server associated with the OpenPages application server where you changed the port.

Procedure

1. Open a browser window and log on to the Oracle WebLogic Server Administration Console for the workflow server as a user with administrative privileges.

   By default, the URL is `http://<server_name>:49901/console`

   Where `<server_name>` is the name of the server where workflow server is installed and `49901` is the workflow admin port.
2. In the **Change Center** pane of the Console, click **Lock & Edit** (if not already selected).
3. In the **Domain Structure** pane, expand the **Services** tree then **Messaging** in the left pane and click **Bridges**.
4. In the **Bridges** table listing on the **Summary of Messaging Bridges** page, do the following:
   a. Locate the server for which you need to change the port in the **Name** column. There are two listings in the table for each workflow server instance.

      Example

      The following two entries reference workflow server instance 1 on server `server01:`

      ```
      server01-InterstageBPMCS1-OP2IBPMBridge
      server01-InterstageBPMCS1-OPInternalBridge
      ```
   b. In the **Target Bridge Destination** column, click the `OP2IBPMInternalBridgeTarget` entry for the application server you want to configure.

      Example :
      `server01-InterstageBPMCS1-OP2IBPMBridgeTarget`
   c. On the **Settings for <Server_Name>OP2IBPMBridgeTarget** page, change the port value in the **Connection URL** field to the OpenPages application port.
   d. Click **Save**.
5. If you need to change the ports for any other OpenPages instance on this server, repeat these steps for each.
6. Click the **Activate Changes** button in the **Change Center** to implement the changes.

Update Port Values in OpenPages Property Files

If you changed the OpenPages application port (`7009`), and/or the workflow server application port (`49951`), you must manually change the port values in the following properties files for the OpenPages application server for which you changed the ports: `aurora.properties`, `-sosa.properties`, and `-server.properties`.

If you did not change any of these ports, skip to task “Update Port Values in the Server Property Files” on page 429.

Update Port Values in the Aurora Property File (aurora.properties):

Procedure

1. Log on to the OpenPages admin server associated with the application server for which you changed ports as a user with administrator privileges.
2. Open a Command Prompt window (using the **Run as Administrator** option) and navigate to the `<OP_Home>|aurora|conf` directory.

Where: <OP_Home> represents the installation location of the OpenPages application, by default:

Windows
C:\OpenPages

3. Locate the aurora.properties file in the conf directory and open the file in a text editor of your choice.
   a. Update the port in the following property with the new OpenPages application port number (by default 7009):

      application.url.path=
      url.service.port=

   b. When finished, save and close the file.

Update Port Values in the OpenPages Sosa Property File (-sosa.properties):

Procedure

1. In the Command Prompt window, remain in the <OP_Home>|aurora|conf directory.
2. Locate the -sosa.properties file for the application server for which you changed ports and make a backup copy of the file. File names have the following format:

   Windows:

   <server_name>-OpenPagesServer<#>-sosa.properties

   Where:

   <server_name> is the name of the OpenPages application host server.

   <#> is the number of the server.
3. Open the selected -sosa.properties in a text editor of your choice and do the following:
   a. If you changed the OpenPages application port number (by default, 7009) update the port in the following property:

      application.url.path=

   b. When finished, save and close the file.

Update Port Values in the OpenPages Server Property File (-server.properties):

Procedure

1. In the Command Prompt window, remain in the <OP_Home>|aurora|conf directory.
2. Locate the -server.properties file for the application server for which you changed ports and make a backup copy of the file. File names have the following format:

   Windows

   <server_name>-OpenPagesServer<#>-server.properties

   Where:

   <server_name> is the name of the OpenPages application host server.

   <#> is the number of the server.
3. Open the selected application -server.properties file in a text editor of your choice and do the following:
   a. Update the port in the following properties with the new OpenPages application port number (by default, 7009):

```
url.service.rule=
security.providerurl=
url.service.port=
url.service.workflow=
jta.providerurl=
url.service.security=
jms.providerurl=
url.service.repository=
url.path.openpages=
url.service.transformation=
url.repositoryService=
url.service.sitegenerator=
webclient.http.server.port=
service.client.providerurl=
url.service.clientapi=
```

b. Save and close the file.

Update Port Values in the Workflow Server Properties Files (-server.properties):

If you changed the OpenPages bootstrap port, OpenPages application port, and/or workflow application port, you need to update the ports in the server properties file for which you changed the port(s).

Associated servers will have the same number, for example:

```
<OpenPages_Server>-OpenPagesServer<1>-server.properties
<OpenPages_Server>-InterstageBPMCS<1>-server.properties
```

Procedure

1. In the Command promptl window, remain in the `<OP_Home>|aurora|conf` directory.
2. Locate the `-server.properties` file for the selected workflow server and make a backup copy of the file. File names have the following format:

   `<server_name>-InterstageBPMCS<#>-server.properties`

   Where:

   `<server_name>` is the name of the workflow host server.

   `<#>` is the number of the node or server.
3. Open the selected workflow `-server.properties` file in a text editor of your choice and do the following:
   a. Update the port in the following properties with the new OpenPages application port number (by default, 7009):

   ```
   url.service.rule=
   security.providerurl=
   url.service.port=
   url.service.workflow=
   url.service.security=
   url.service.repository=
   url.service.transformation=
   url.path.openpages=
   url.service.sitegenerator=
   url.repositoryService=
   service.client.providerurl=
   webclient.http.server.port=
   url.service.clientapi=
   ```

b. Save and close the file.

Update ObjectManager properties file (ObjectManager.properties):

You need to update the port in the ObjectManager properties file.

Procedure

1. In the Command prompt window, navigate to the following directory:
   `<OP_Home>\bin`
2. Open the `ObjectManager.properties` file in a text editor of your choice and do the following:
   a. Update the following property with the new OpenPages application port:
      `openpages.service.port=`
   b. Save and close the file.

Update Port Values in the Database

If you updated any of the default OpenPages ports, you must update the port value(s) in the `REGISTRY_ENTRIES` table in the OpenPages database as follows.

Procedure

1. Log on to a machine with SQL*Plus and access to the database server.
2. Run the following SQL commands to update the port number in the `REGISTRY_ENTRIES` table:

   ```
   update registryentries set value='<new_port_number>'
   where path='/OpenPages/Platform/Reporting Schema/Object URL
   Generator/Port';
   commit;
   ```

   where `<new_port_number>` is the new OpenPages application server port number.
3. When the commands are complete, log out of SQL*Plus.

Update Port Values on the Reporting Server

If you changed the OpenPages application port number (`7009`), you must update the associated CommandCenter instance with the new port number

Procedure

1. Log onto the reporting server as a user with administrator privileges.
2. Open a Command Prompt window (using the **Run as Administrator** option) and navigate to the `<Cognos_Home>|configuration` directory.

   Where:

   `<Cognos_Home>` represents the installation location of the Cognos application. By default:

   Windows
   `C:\OpenPages\Cognos\cognos\c8\configuration`
3. Locate the `OpenPagesSecurityProvider_OpenPagesSecurityRealm.properties` file and make a backup copy of the file.
4. Open the `OpenPagesSecurityProvider_OpenPagesSecurityRealm.properties` file in a text editor of your choice and do the following:
   a. Replace the existing OpenPages application port number (`7009`) update the following property with the new OpenPages application port number:
      `openpages.application.url=`

b. When finished, save and close the file.

Changing OpenPages Application Ports for an IBM WebSphere Application Server Environment

Note: The information in this topic applies only to IBM WebSphere environments.

Because the IBM OpenPages application on the IBM WebSphere Application Server uses port ranges, if you need to change one of the IBM OpenPages GRC Platform environment port numbers, we recommend that you change all of the IBM OpenPages application and workflow (IBPM) server ports to a new range by following the instructions in this section.

By default, the OpenPages application on the IBM WebSphere Application Server uses the port range 10101-10120, and workflow (IBPM) server uses the port range 20101-20120.

Stop the OpenPages and Workflow Application Servers

Before changing the ports, make sure that all managed OpenPages application servers and all managed workflow servers are stopped. Only the OpenPages admin server must be running.

Important: **DO NOT** use the `stopAllServers.sh` script, as the script will attempt to stop any other applications associated with OpenPages ports.

Procedure

1. Log on to the admin server as a user with administrator privileges.
2. To stop an OpenPages application server, do the following:
   a. Open an AIX shell and navigate to the `<OP_Home>/profiles/<server_name>-OPNode1/bin` directory.

      Where: `<OP_Home>` represents the installation location of the OpenPages application, by default:

      `/opt/OpenPages`

   b. Enter the commands as follows to stop each OpenPages application server and workflow application server for which you want to change the port numbers:

      `./stopServer.sh <host_name>-OPNode1Server<#>`

      Where `<#>` is the number of the OpenPages application server.

Update the Port Numbers in the Admin Console

Use the following steps to change the default port numbers on an OpenPages application server.

Procedure

1. Open a browser window and navigate to the following address to launch IBM WebSphere Integrated Solutions Console for the OpenPages application, by default:

   `http://<server_name>:9060/ibm/console`

   Where:

   `<server_name>` is the name of the server where the IBM WebSphere Application Server is installed and `9060` is the default OpenPages application port.

2. Log on to the IBM WebSphere Integrated Solutions Console as a user with administrative privileges.
3. Expand **Servers** then **Server Types** in the left pane and click the **WebSphere application servers** link.
4. In the list on the **Application servers** page, click the name of the application server for which you want to change port numbers. For example:

   `<server_name>-OPNode1Server<#>`

   Where:

   `<server_name>` is the name of the application server.

   `<#>` is the number of the server.
5. On the **Application servers** > **<server-name>** page for the selected server, under the **Communications** heading, click the **Ports** link.
6. On the **Ports** page for the selected server, click the link to the port that you want to change.

   Note: When changing ports, we recommend you change all the ports shown on the **Ports** page for each server and maintain all ports in a specific range.
7. On the **<port type>** page for the selected port, do the following:
   a. Enter a new port number in the **Port** field.
   b. Click **Apply**.
   c. In the **Messages** box that appears at the top of the page, click **Save** to commit the changes to the master configuration.
8. Repeat Steps 4-7 as needed to change other ports on the selected server.
9. If you changed the OpenPages application port (by default, `10108`) and/or OpenPages application SSL port (by default, `10111`), update the port numbers in the default OpenPages application virtual hosts created by the IBM WebSphere Application Server as follows:
   a. In the left pane of the IBM WebSphere Integrated Solutions Console, expand **Environment** then click **Virtual Hosts**.
   b. In the list on the **Virtual Hosts** page, click **default_host**.
   c. On the **Virtual Hosts > default_host** page, under the **Additional Properties** heading, click **Host Aliases**.
   d. On the **Host Aliases** page, click the appropriate * link to update the OpenPages application (`WC_defaulthost`) port you changed above. The port numbers listed are the previous port numbers for each port.

      For example, if the application port for the OpenPages instance you changed was `10108`, click the * in the same row as `10108`.
   e. On the **Configuration** tab, enter the new port number in the **Port** field.
   f. Click **Apply**.
   g. In the **Messages** box that appears at the top of the page, click **Save** to commit the changes to the master configuration.
   h. On the **Host Aliases** page, click * to select the OpenPages application (`WC_defaulthost_secure`) SSL port, by default `10111`. The port numbers listed are the previous port numbers for each port.
   i. On the **Configuration** tab, enter the new port number in the **Port** field.
   j. Click **Apply**.
   k. In the **Messages** box that appears at the top of the page, click **Save** to commit the changes to the master configuration.

Update Ports to the Java Messaging Service

If you changed the IBM WebSphere Service Integration Bus (SIB) messaging service endpoint port for the OpenPages application server (by default, 10115), you need to change other settings within the OpenPages application server and the workflow server.

If you did not change the SIB Endpoint Address, skip to the task "Update Port Values in OpenPages Property Files" on page 418.

The IBM WebSphere Application Server uses the Java Message Service (JMS) to enable Java clients and applications to create, send, receive, and read asynchronous requests.

Procedure

1. "Update the Java Messaging Ports on OpenPages Server"
2. "Update the Java Messaging Ports on Workflow Server" on page 417

Update the Java Messaging Ports on OpenPages Server:

Launch the IBM WebSphere Integrated Solutions Console for the OpenPages application and update the OpenPages ports used by the Java Messaging Service.

Procedure

1. On the IBM WebSphere Integrated Solutions Console for the OpenPages application (`http://<server_name>:9060/ibm/console`), update the OpenPages topic connection factories with the new port number(s) set above.

   A topic connection factory is used by the IBM WebSphere Application Server to send messages between Java clients within your environment.

   a. Expand **Resources** then **JMS** in the left pane and click the **Topic Connection Factories** link.
   b. In the list on the Topic connection factories page, click the **OPTCF** link.
   c. Under General Properties, locate the **Provider endpoints** field in the **Connections** group.
   d. Update the port number in the **Provider endpoints** field for the IBM WebSphere SIB messaging service with the new SIB endpoint address for the OpenPages server:
      `<server_name>:<SIB_ENDPOINT_ADDRESS>:BootstrapBasicMessaging`.

      If necessary, refer to the **Application servers** > **<server_name>-OPNode1Server#** > **Ports** page for the current OpenPages SIB Endpoint Address port.
   e. Click **Apply**.
   f. In the **Messages** box that appears at the top of the page, click **Save** to commit the changes to the master configuration.
2. Update the OpenPages server activation specifications with the new port number(s) set above.
   a. In the **Resources** > **JMS** tree in the left pane, click the **Activation specifications** link.
   b. In the list on the **Activation Specifications** page, click **NotificationTopic** for the server which you changed the SIB port.
   c. Under General Properties, locate the **Provider endpoints** field in the **Destination** group.

d. Update the port number in the **Provider endpoints** field to the new OpenPages SIB port number: `<server_name>:<SIB_ENDPOINT_ADDRESS>:BootstrapBasicMessaging`.
e. Click **Apply**.
f. In the **Messages** box that appears at the top of the page, click **Save** to commit the changes to the master configuration.
g. In the list on the **Activation Specifications** page, click **SQNotificationTopic** for the server which you changed the SIB port.
h. Repeat the steps above to change the OpenPages SIB endpoint address: `<server_name>:<SIB_ENDPOINT_ADDRESS>:BootstrapBasicMessaging`
i. In the **Messages** box that appears at the top of the page, click **Save** to commit the changes to the master configuration.

3. Log out of the IBM WebSphere Integrated Solutions Console for the OpenPages server.

Update the Java Messaging Ports on Workflow Server:

After updating the ports used by the Java Messaging Service on the OpenPages server, you must update the workflow server queue connection endpoints with the new OpenPages port number(s) set above.

Procedure

1. Open a browser window and navigate to the following address to launch IBM WebSphere Integrated Solutions Console for the workflow server, by default:

   `http://<server_name>:9061/ibm/console`

   Where:

   `<server_name>` is the name of the server where the IBM WebSphere Application Server is installed and `9061` is the default workflow server admin port.
2. Log on to the IBM WebSphere Integrated Solutions Console as a user with administrative privileges.
3. Update the workflow server topic connection endpoints with the new port number(s) set above.
   a. In the **Resources** > **JMS** tree in the left pane, click the **Topic Connection Factories** link.
   b. In the list on the **Topic connection factories** page, click the **OPTCF** link.
   c. Under General Properties, locate the **Provider endpoints** field in the **Connections** group.
   d. Update the port number in the **Provider endpoints** field to use the new SIB endpoint address value for the OpenPages server: `<host_name>:<SIB_ENDPOINT_ADDRESS>:BootstrapBasicMessaging`.
   e. Click **Apply**.
   f. In the **Messages** box that appears at the top of the page, click **Save** to commit the changes to the master configuration.
4. Update the workflow server activation specifications with the new port number(s) set above.
   a. In the **Resources** > **JMS** tree in the left pane, click the **Activation specifications** link.
   b. In the list on the **Activation Specifications** page, click **CacheSyncBridgeTopicAS** for the server which you changed the SIB port.
   c. Under General Properties, locate the **Provider endpoints** field in the **Destination** group.

d. Update the port number in the **Provider endpoints** field to the new OpenPages SIB port number:
`<server_name>:<SIB_ENDPOINT_ADDRESS>:BootstrapBasicMessaging`.

e. Click **Apply**.

f. In the **Messages** box that appears at the top of the page, click **Save** to commit the changes to the master configuration.

g. In the list on the **Activation Specifications** page, click **RepositoryTopicAS** for the server which you changed the SIB port.

h. Repeat the steps above to change the OpenPages SIB endpoint address:
`<server_name>:<SIB_ENDPOINT_ADDRESS>:BootstrapBasicMessaging`

i. In the **Messages** box that appears at the top of the page, click **Save** to commit the changes to the master configuration.

j. In the list on the **Activation Specifications** page, click **SiteGeneratorTopicAS** for the server which you changed the SIB port.

k. Repeat the steps above to change the OpenPages SIB endpoint address:
`<server_name>:<SIB_ENDPOINT_ADDRESS>:BootstrapBasicMessaging`

l. In the **Messages** box that appears at the top of the page, click **Save** to commit the changes to the master configuration.

Update Port Values in OpenPages Property Files

If you changed the OpenPages bootstrap port (`10101`), the OpenPages application port (`10108`), you must manually change the port values in the following properties files for the OpenPages application server for which you changed the ports: `aurora.properties`, `-sosa.properties`, and `-server.properties`.

Update Port Values in the Aurora Property File (aurora.properties):

Procedure

1. Log on to the OpenPages admin server associated with the application server for which you changed ports as a user with administrator privileges.
2. Open an AIX shell window and navigate to the `<OP_Home>|aurora|conf` directory.

   Where: `<OP_Home>` represents the installation location of the OpenPages application, by default:

   AIX
   `/opt/OpenPages`
3. Locate the `aurora.properties` file in the `conf` directory and open the file in a text editor of your choice.
   a. If you changed the OpenPages application port number (`10108`) update the port in the following property:
      `application.url.path=`
   b. If you changed the OpenPages bootstrap port number (`10101`) update the port in the following property:
      `url.service.port=`
   c. When finished, save and close the file.

Update Port Values in the OpenPages Sosa Property File (-sosa.properties):

Procedure

1. In the AIX shell window, remain in the `<OP_Home>|aurora|conf` directory.

2. Locate the -sosa.properties file for the application server for which you changed ports and make a backup copy of the file. File names have the following format:

   <server_name>-OPNode1Server<#>-sosa.properties

   Where:

   <server_name> is the name of the OpenPages application host server.

   <#> is the number of the server.
3. Open the selected -sosa.properties in a text editor of your choice and do the following:
   a. If you changed the OpenPages application port number (by default, 10108) update the port in the following property:

      application.url.path=

   b. If you changed the OpenPages bootstrap port number (by default, 10101) update the port in the following property:

      openpages.service.port=

   c. When finished, save and close the file.

Update Port Values in the OpenPages Server Property File (-server.properties):

Procedure

1. In the AIX shell window, remain in the <OP_Home>|aurora|conf directory.
2. Locate the -server.properties file for the application server for which you changed ports and make a backup copy of the file. File names have the following format:

   <server_name>-OPNode1Server<#>-server.properties

   Where:

   <server_name> is the name of the OpenPages application host server.

   <#> is the number of the server.
3. Open the selected application -server.properties file in a text editor of your choice and do the following:
   a. If you changed the OpenPages bootstrap port number (by default, 10101) update the following properties with the new OpenPages bootstrap port:

      ```
      url.service.rule=
      security.providerurl=
      url.service.port=
      url.service.workflow=
      jta.providerurl=
      url.service.security=
      jms.providerurl=
      url.service.repository=
      url.service.transformation=
      url.repositoryService=
      url.service.sitegenerator=
      service.client.providerurl=
      url.service.clientapi=
      ```

   b. If you changed the OpenPages application port number (by default, 10108) update the following properties with the new OpenPages application port:

      ```
      url.path.openpages=
      webclient.http.server.port=
      ```

   c. Save and close the file.

Update Port Values in the Workflow Server Properties Files (-server.properties):

If you changed the OpenPages bootstrap port, OpenPages application port, and/or workflow application port, you need to update the ports in the server properties file for which you changed the port(s).

Procedure

1. In the AIX shell window, remain in the <OP_Home>|aurora|conf directory.
2. Locate the -server.properties file for the selected workflow server and make a backup copy of the file. File names have the following format:

   <server_name>-IBPMNode<#>Server-server.properties

   Where:

   <server_name> is the name of the workflow host server.

   <#> is the number of the node or server.
3. Open the selected workflow -server.properties file in a text editor of your choice and do the following:
   a. If you changed the OpenPages bootstrap port (10101) update the following properties with the new OpenPages bootstrap port:

      ```
      url.service.rule=
      security.providerurl=
      url.service.port=
      url.service.workflow=
      url.service.security=
      url.service.repository=
      url.service.transformation=
      url.service.sitegenerator=
      url.repositoryService=
      service.client.providerurl=
      url.service.clientapi=
      ```

   b. If you changed the OpenPages application port (10108) update the following properties with the new OpenPages application port:

      ```
      url.path.openpages=
      webclient.http.server.port=
      ```

   c. If you changed the workflow server bootstrap port (20101) update the following properties with the new workflow bootstrap port:

      ```
      jta.providerurl=
      jms.providerurl=
      ```

   d. If you changed the workflow application port (20108) update the following property with the new workflow application port:

      ```
      url.path.workflow.admin=
      ```

   e. Save and close the file.

Update ObjectManager properties file (ObjectManager.properties):

If you changed the OpenPages bootstrap port (10101), you need to update the ports in the ObjectManager properties file for which you changed the port.

Procedure

1. In the AIX shell, navigate to the following directory:

   <OP_Home>/bin

2. Open the ObjectManager.properties file in a text editor of your choice and do the following:
   a. Update the following property with the new OpenPages bootstrap port:
      openpages.service.port=
   b. Save and close the file.

Update Port Values in RunTool.sh script (RunTool.sh)

Note: The information in this topic applies only to IBM WebSphere environments.

If you changed the OpenPages bootstrap port (10101), you need to update the ports used by the RunTool.sh script. The RunTool.sh script is used by multiple OpenPages background tasks.

Procedure

1. In the AIX shell, navigate to the following directory:
   <OP_Home>/bin
2. Open the RunTool.sh file in a text editor of your choice and do the following:
   a. If the launchClient.sh command contains the following parameters:
      -CCBootstrapHost=<server_name>
      -CCBootstrapPort=<openpages_bootstrap_port>

      Make sure the -CCBootstrapPort value is using the new OpenPages bootstrap port. If these parameters are not present, skip this task.

      Examples

      If the parameters are present:
      launchClient.sh -JVMOptions "$JVMOPTIONS" "$OPENPAGES_HOME/
      applications/opappstools.ear" -CCBootstrapHost=OPAdminServer
      -CCBootstrapPort=30101 -CCjar=opappstool-$TOOL_NAME.jar "$@"

      If the parameters are not present:
      launchClient.sh -JVMOptions "$JVMOPTIONS" "$OPENPAGES_HOME/
      applications/opappstools.ear"-CCjar=opappstool-$TOOL_NAME.jar "$@"
   b. Save and close the file.

Update Port Values in the Database

If you updated any of the default OpenPages ports, you must update the port value(s) in the REGISTRY_ENTRIES table in the OpenPages database as follows.

Procedure

1. Log on to a machine with SQL*Plus and access to the database server.
2. Run the following SQL commands to update the port number in the REGISTRY_ENTRIES table:

   ```
   update registryentries set value='<new_port_number>'
   where path='/OpenPages/Platform/Reporting Schema/Object URL
   Generator/Port';
   commit;
   ```

   where <new_port_number> is the new OpenPages application server port number.
3. When the commands are complete, log out of SQL*Plus.

Update Port Values on the Reporting Server

If you changed the OpenPages application port number (10108), you must update the associated CommandCenter instance with the new port number

Procedure

1. Log onto the reporting server as a user with administrator privileges.
2. Open an AIX shell window and navigate to the `<Cognos_Home>|configuration` directory.

   Where:

   `<Cognos_Home>` represents the installation location of the Cognos application. By default:

   AIX

   `/opt/OpenPages/Cognos/cognos/c8/configuration`
3. Locate the `OpenPagesSecurityProvider_OpenPagesSecurityRealm.properties` file and make a backup copy of the file.
4. Open the `OpenPagesSecurityProvider_OpenPagesSecurityRealm.properties` file in a text editor of your choice and do the following:
   a. Replace the existing OpenPages application port number (`10108`) update the following property with the new OpenPages application port number:

      `openpages.application.url=`
   b. When finished, save and close the file.

Change Port Numbers for the Workflow Server

Follow this procedure to change port numbers of the workflow server.

Before changing the port numbers, make sure that the new ports you are going to use are available. For details, see "Check Port Number Availability" on page 407.

Changing Workflow Ports for an Oracle WebLogic Server Environment

Important: If you have more than one cluster member on the same server, the workflow listen port for each cluster member must be different by 2.

For example, if you have 3 managed servers on the same server in which the default listen ports are 49951, 49953 and 49955 respectively:

Table 63. Original Port Assignments

Cluster Member	Listen Port	SSL Listen Port
<server_name>-InterstageBPMCS1	49951	49952
<server_name>-InterstageBPMCS2	49953	49954
<server_name>-InterstageBPMCS3	49955	49956

If you want to change the listen port of the <server_name>-InterstageBPMCS1 to 49991, you must change the SSL listen port of the same cluster member to 49992.

You must then change the listen port of the remaining cluster members.

Table 64. Changed Port Assignments

Cluster Member	Listen Port	SSL Listen Port
<server_name>-InterstageBPMCS1	49991	49992

Table 64. Changed Port Assignments (continued)

Cluster Member	Listen Port	SSL Listen Port
<server_name>-InterstageBPMCS2	49993	49994
<server_name>-InterstageBPMCS3	49995	49996

Stop the Workflow Application Server:

Before changing the ports, make sure that the workflow server you are working with is stopped. Only the IBM OpenPages admin and workflow admin servers must be running.

Important: DO NOT use the `stopAllServers` script, as the script will attempt to stop any other applications associated with OpenPages ports.

Update the Workflow Server Listen Port:

Change the port numbers for the workflow server listen port as follows:

Procedure

1. Open a browser window and log on to the Oracle WebLogic Server Administration Console for the workflow server as a user with administrative privileges.

   By default, the URL is `http://<server_name>:49901/console`

   Where:

   `<server_name>` is the name of the server where Oracle WebLogic Server is installed and `49901` is the default workflow server admin port.
2. In the **Change Center** pane of the Console, click **Lock & Edit** (if not already selected).
3. In the Console's **Domain Structure** pane, expand the **Environment** tree and click **Servers**.
4. On the **Summary of Servers** page, click the **Configuration** tab (if not already selected).
5. In the **Servers table** listing, click the name of the workflow server for which you want to change port numbers.

   For example: `<server_name>-InterstageBPMCS<#>`

   Where: `<server_name>` is the name of the workflow server, and `<#>` is the number of the server.
6. On the **Settings for <Server_Name>** page for the selected server, on the **General** tab, change the value in the following fields:
   - **Listen Port** - the port used by the workflow server. By default, this port is 49951.
   - **SSL Listen Port** - the SSL port used by the workflow server. By default, this port is 49952.
7. Click **Save**.

Update the Ports for the Messaging Bridge Between the Workflow Server and the OpenPages Application Server:

After changing the workflow application port number, you must update the port numbers for the messaging bridge on the workflow server, which allows the workflow server to send and receive JMS messages from the OpenPages server.

There are two listings in the table for each OpenPages instance. Each server bridge needs to be updated.

Example

The following two entries reference OpenPages instance 1 on server `server01`:

```
server01-InterstageBPMCS1-OP2IBPMBridge
server01-InterstageBPMCS1-OPInternalBridge
```

Procedure

1. In the **Domain Structure** pane, expand the **Services** tree then **Messaging** in the left pane and click **Bridges**.
2. In the **Bridges** table listing on the **Summary of Messaging Bridges** page, do the following:
   a. In the **Name** column, locate the server for which you need to change the port . In the **Source Bridge Destination** column, click the **OP2IBPMBridgeSource** entry for the application server you want to configure.

      `<server_name>-InterstageBPMCS<#>-OP2IBPMBridgeSource`
3. On the **Settings for <Server_Name>-OP2IBPMBridgeSource** page, change the port value in the **Connection URL** field to the workflow application port.
4. Click **Save**.
5. Return to the **Summary of Messaging Bridges** page.
6. In the **Source Bridge Destination** column, click the **OPInternalBridgeSource** entry for the application server you want to configure.

   `<server_name>-InterstageBPMCS<#>-OPInternalBridgeSource`
7. On the **Settings for <Server_Name>-OPInternalBridgeSource** page, change the port value in the Connection URL to the new workflow server port.
8. Click **Save**.
9. Return to the **Summary of Messaging Bridges** page.
10. In the **Target Bridge Destination** column, click the **OPInternalBridgeTarget** entry for the application server you want to configure.

    `<server_name>-InterstageBPMCS<#>-OPInternalBridgeTarget`
11. On the **Settings for <Server_Name>-OPInternalBridgeTarget** page, change the port value in the Connection URL to the new workflow server port.
12. Click **Save**.
13. Return to the **Summary of Messaging Bridges** page.
14. If you need to change the ports for any other OpenPages instance on this server, repeat these steps for each.
15. Click the **Activate Changes** button in the **Change Center** to implement the changes.

Update the Ports for the Messaging Bridge Between the OpenPages Application Server and the Workflow Server:

After changing the workflow application port number, you must update the port numbers for the messaging bridge on the OpenPages server, which allows the OpenPages server to send and receive JMS messages from the workflow server.

Procedure

1. Open a browser window and log on to the Oracle WebLogic Server Administration Console for the OpenPages server as a user with administrative privileges.

   By default, the URL is `http://<server_name>:7001/console`

   Where `<server_name>` is the name of the server where OpenPages server is installed and `7001` is the OpenPages admin port.
2. In the **Change Center** pane of the Console, click **Lock & Edit** (if not already selected).
3. In the **Domain Structure** pane, expand the **Services** tree then **Messaging** in the left pane and click **Bridges**.
4. In the Bridges table listing on the **Summary of Messaging Bridges** page, do the following:
   a. Locate the server for which you need to change the port in the **Name** column.
   b. In the **Target Bridge Destination** column, click the **OP2IBPMBridgeTarget** entry for the application server you want to configure.

      Example : `<server_name>-OpenPagesServer#-OP2IBPMBridgeTarget`
5. On the **Settings for <Server_Name>-OP2IBPMBridgeTarget** page, do the following:
   a. Change the port value in the **Connection URL** field to the new workflow server port.
   b. Click **Save**.
6. If you need to change the ports for any other workflow instance on this server, repeat these steps for each.
7. Click the **Activate Changes** button in the **Change Center** to implement the changes.

Changing Workflow Ports for an IBM WebSphere Application Server Environment

Because the OpenPages application on the IBM WebSphere Application Server uses port ranges, if you need to change one of the IBM OpenPages GRC Platform environment port numbers, we recommend that you change all of the OpenPages application and workflow (IBPM) server ports to a new range by following the instructions in this section.

By default, the workflow (IBPM) server uses the port range `20101-20120`.

Stop the Workflow Application Server:

Before changing the ports, make sure that the managed workflow server(s) you are working with is stopped. Only the workflow admin server must be running.

Important: DO NOT use the `stopAllServers` script, as the script will attempt to stop any other applications associated with OpenPages ports.

Procedure

1. Log on to the OpenPages the application server for which you changed ports as a user with administrator privileges.
2. To stop a workflow server, do the following:
   a. Open an AIX shell and navigate to the `<Workflow_Home>/profiles/<server_name>-IBPMNode<#>/bin` directory.

      Where: `<Workflow_Home>` represents the installation location of the workflow, by default: `/opt/Fujitsu/InterstageBPM`
   b. Enter the commands as follows to stop each workflow server for which you want to change the port numbers:

      `./stopServer.sh <server_name>-IBPMNode<#>Server`

      Where: `<#>` is the number of workflow application server.

Update the Port Numbers in the Admin Console:

Use the following steps to change the default port numbers on a workflow server in the IBM WebSphere Integrated Solutions Console.

Procedure

1. Open a browser window and navigate to the following address to launch IBM WebSphere Integrated Solutions Console for the workflow server, by default:

   `http://<server_name>:9061/ibm/console`

   Where:

   `<server_name>` is the name of the server where the IBM WebSphere Application Server is installed and `9061` is the default workflow application port.
2. Log on to the IBM WebSphere Integrated Solutions Console as a user with administrative privileges.
3. Expand **Servers** then **Server Types** in the left pane and click the **WebSphere application servers** link.
4. In the list on the **Application servers** page, click the name of the application server for which you want to change port numbers. For example:

   `<server_name>-IBPMNode<#>Server`

   Where:

   `<server_name>` is the name of the application server.

   `<#>` is the number of the node or server.
5. On the **Application servers** > **<IBPM-server-name>** page for the selected server, under the **Communications** heading, click the **Ports** link.
6. On the **Ports** page for the selected server, click the link to the port that you want to change.

   Note: When changing ports, we recommend you change all the ports shown on the **Ports** page for each server and maintain all ports in a specific range.
7. On the **<port type>** page for the selected port, do the following:
   a. Enter a new port number in the **Port** field.
   b. Click **Apply**.
   c. In the **Messages** box that appears at the top of the page, click **Save** to commit the changes to the master configuration.
8. If you changed the workflow application port (`WC defaulthost`, by default, `20108`) and/or workflow application SSL port (`WC defaulthost secure`, by

default, 20111), update the port numbers in the default workflow application virtual hosts created by the IBM WebSphere Application Server as follows:

a. In the left pane of the IBM WebSphere Integrated Solutions Console, expand **Environment** then click **Virtual Hosts**.
b. In the list on the **Virtual Hosts** page, click **default_host**.
c. On the **Virtual Hosts > default_host** page, under the **Additional Properties** heading, click **Host Aliases**.
d. On the **Host Aliases** page, click the appropriate * link to update the workflow application (WC_defaulthost) port you changed above. The port numbers listed are the previous port numbers for each port.

   For example, if the application port for the workflow instance you changed was 20108, click the * in the same row as 20108.
e. On the **Configuration** tab, enter the new port number in the **Port** field.
f. Click **Apply**.
g. In the **Messages** box that appears at the top of the page, click **Save** to commit the changes to the master configuration.
h. On the **Host Aliases** page, click * to select the workflow application (WC_defaulthost_secure) SSL port, by default 20111. The port numbers listed are the previous port numbers for each port.
i. On the **Configuration** tab, enter the new port number in the **Port** field.
j. Click **Apply**.
k. In the **Messages** box that appears at the top of the page, click **Save** to commit the changes to the master configuration.

Update the Java Messaging Ports on Workflow Admin Console:

If you changed the IBM WebSphere Service Integration Bus (SIB) messaging service endpoint port for the workflow server (by default, 20115), you need to change other settings within the OpenPages application server and the workflow server.

Procedure

1. Open a browser window and navigate to the following address to launch IBM WebSphere Integrated Solutions Console for the workflow server, by default:

   `http://<server_name>:9061/ibm/console`

   Where:

   <server_name> is the name of the server where the IBM WebSphere Application Server is installed and 9061 is the default workflow server admin port.
2. Log on to the IBM WebSphere Integrated Solutions Console as a user with administrative privileges.
3. Update the workflow server queue connection endpoints with the new port number(s) set above.
   a. In the **Resources** > **JMS** tree in the left pane, click the **Queue Connection Factories** link.
   b. In the list on the **Queue connection factories** page, click the **IAnalyticsConnectionFactory** link.
   c. Under General Properties, locate the **Provider endpoints** field in the **Connections** group.
   d. Update the port number in the **Provider endpoints** field to use the new workflow port number:
   <server_name>:<SIB_ENDPOINT_ADDRESS>:BootstrapBasicMessaging.

e. Click **Apply**.
f. In the **Messages** box that appears at the top of the page, click **Save** to commit the changes to the master configuration.

4. Update the workflow topic connection endpoints with the new port number(s) set above.
   a. In the **Resources** > **JMS** tree in the left pane, click the **Topic Connection Factories** link.
   b. In the list on the **Topic connection factories** page, click the **iFlowDistFactory** link.
   c. Under General Properties, locate the **Provider endpoints** field in the **Connections** group.
   d. Update the port number in the **Provider endpoints** field to the new SIB endpoint address value for the workflow server: `<server_name>:<SIB_ENDPOINT_ADDRESS>:BootstrapBasicMessaging`.
   e. In the **Messages** box that appears at the top of the page, click **Save** to commit the changes to the master configuration.
   f. In the list on the **Topic connection factories** page, click **iFlowFactory** for the server which you changed the SIB port.
   g. Repeat the steps above to change the workflow SIB endpoint address: `<server_name>:<SIB_ENDPOINT_ADDRESS>:BootstrapBasicMessaging`

Update Ports to the Java Messaging Service on the OpenPages Admin Console:

If you changed the IBM WebSphere Service Integration Bus (SIB) messaging service endpoint port for the workflow server (by default, `20115`), you need to change the following settings within the OpenPages admin console.

Procedure

On the IBM WebSphere Integrated Solutions Console for the OpenPages application (`http://<server_name>:9060/ibm/console`), update the workflow server activation specifications with the new port number(s) set above.

1. In the **Resources > JMS** tree in the left pane, click the **Activation specifications** link.
2. In the list on the **Activation Specifications** page, click **NotificationTopic** for the server which you changed the SIB port.
3. Under General Properties, locate the Provider endpoints field in the Destination group.
4. Update the port number in the Provider endpoints field to the new workflow SIB port number:
   `<server_name>:<SIB_ENDPOINT_ADDRESS>:BootstrapBasicMessaging`
5. Click **Apply**.
6. In the **Messages** box that appears at the top of the page, click **Save** to commit the changes to the master configuration.
7. In the list on the **Activation Specifications** page, click **SQNotificationTopic** for the server which you changed the SIB port.
8. Repeat the steps above to change the workflow SIB endpoint address:
   `<server_name>:<SIB_ENDPOINT_ADDRESS>:BootstrapBasicMessaging`
9. In the **Messages** box that appears at the top of the page, click Save to commit the changes to the master configuration.

Update Port Values in the Server Property Files

Note: The information in this topic applies to both Oracle WebLogic and IBM WebSphere environments.

If you changed the workflow bootstrap port (`49951/20101`), and/or the workflow server application port (`49951/20108`), you must manually change the port values in the following properties files for the workflow application server for which you changed the ports.

Note: Default port numbers in this section are listed in parenthesis in (**Windows** / **AIX**) format.

Update Port Values in the Workflow Server Properties Files (-server.properties):

If you changed the OpenPages bootstrap port, OpenPages application port, and/or workflow application port, you need to update the ports in the server properties file for which you changed the port(s).

Procedure

1. Log on to the OpenPages the application server for which you changed ports as a user with administrator privileges.
2. In the Command Prompt window or AIX shell window, remain in the `<OP_Home>|aurora|conf` directory.
3. Locate the `-server.properties` file for the selected workflow server and make a backup copy of the file. File names have the following format:

   Windows : `<server_name>-InterstageBPMCS<#>-server.properties`

   AIX : `<server_name>-IBPMNode<#>Server-server.properties`

   Where:

   `<server_name>` is the name of the workflow host server.

   `<#>` is the number of the node or server.
4. Open the selected workflow `-server.properties` file in a text editor of your choice and do the following:
   - **Windows**
     a. Update the following properties with the new workflow application port:

        ```
        jta.providerurl=
        jms.providerurl=
        url.path.workflow.admin=
        ```
   - **AIX**
     a. If you changed the workflow server bootstrap port (20101) update the following properties with the new workflow bootstrap port:

        ```
        jta.providerurl=
        jms.providerurl=
        ```

     b. If you changed the workflow application port (20108) update the following property with the new workflow application port:

        ```
        url.path.workflow.admin=
        ```
5. Save and close the file.

Update Port Values in the OpenPages Server Properties Files (`-server.properties`):

Procedure

1. Log on to the OpenPages the application server for which you changed ports as a user with administrator privileges.
2. In the Command Prompt window or AIX shell window, remain in the <OP_Home>|aurora|conf directory.
3. Locate the -server.properties file for the application server associated with the workflow server for which you changed ports and make a backup copy of the file. File names have the following format:

   Windows : <server_name>-OpenPagesServer<#>-server.properties

   AIX : <server_name>-OPNode1Server<#>-server.properties

   Where:

   <server_name> is the name of the workflow host server.

   <#> is the number of the node or server.
4. Open the selected application -server.properties file in a text editor of your choice.

   If you changed the workflow application port number (by default, 49951/20108) update the following property with the new workflow application port:

   url.path.workflow.admin=
5. Save and close the file.

Update Port Values in the iFlowClient Property Files (-iFlowClient.properties):

The Fujitsu Interstage i-Flow engine uses properties files. If you changed the workflow bootstrap port (49951/20108), update the ports in the iFlowClient.properties file and the server-specific iFlowClient.properties file.

Procedure

1. In the Command Prompt window or AIX shell, navigate to the following directory:

   <Workflow_Home>|client

   Where <Workflow_Home> is the directory where Fujitsu Interstage BPM is installed. By default,

   Windows:
   C:\Fujitsu\InterstageBPM

   AIX: /opt/Fujitsu/InterstageBPM
2. Locate the -iFlowClient.properties file for the workflow server for which you changed ports and make a backup copy of the file. File names have the following format:

   Windows <server_name>-InterstageBPMCS<#>-iFlowClient.properties

   AIX <server_name>-IBPMNode<#>Server-iFlowClient.properties

   Where:

   <server_name> is the name of the workflow host server.

   <#> is the number of the node and server.
3. Open the server-iFlowClient.properties file in a text editor of your choice and do the following:
   a. Update the following properties with the new workflow server bootstrap port:

      JMSNamingProviderURL=
      NamingProviderURL=

b. Save and close the file.

4. Open the iFlowClient.properties file in a text editor of your choice:
   a. If you changed the port number specified in these fields, update the port. If you did not change that specific port, do not update these fields.

      ```
      JMSNamingProviderURL=
      NamingProviderURL=
      ```

   b. Save and close the file.

   You may not have changed the port specified in the iFlowClient.properties in a server with multiple workflow server instances.

Update Port Values in the IBPM console configuration file (console.conf):

If you changed the workflow bootstrap port (49951/20101), you need to update the ports in the console.conf file for the server for which you changed the port.

Procedure

1. In the Command Prompt window or AIX shell, navigate to the following directory:

   Windows:

   ```
   <Workflow_Home>\console\ibpmconsole-<server_name>-InterstageBPMCS<#>\app\ibpmconsole
   ```

   AIX:

   ```
   <Workflow_Home>/profiles/<server_name>-IBPMNode<#>/installedApps/
    IBPMCell/fujitsu-console-ear.ear/ibpmconsole.war
   ```

2. Open the console.conf file in a text editor of your choice and do the following:
   a. Update the following property with the new workflow server bootstrap port:

      ```
      NamingProviderURL =
      ```

   b. Save and close the file.

3. For Oracle WebLogic Server environments, copy the updated console.conf to the stage folder, by default:<Workflow_Home>\IBPMDomain\servers\<server_name>-InterstageBPMCS<#>\stage\ibpmconsole-<server_name>-InterstageBPMCS<#>\ibpmconsole

Update the ibpm.properties File for Cluster Members:

If you changed the workflow bootstrap port (49951/20101) and/or the workflow application port (49951/20108), you need to update the ports in the ibpm.properties file for the server for which you changed the port(s).

Note: For AIX, this file contains the workflow bootstrap port (20101) and/or the workflow application port (20108), you need to change both, as appropriate.

Procedure

1. In the Command Prompt window or AIX shell, navigate to the following directory:

   Windows:

   ```
   <Workflow_Home>\server\deployment\WLS-Cluster<server_name>-InterstageBPMCS<#>
   ```

   AIX:

   ```
   <Workflow_Home>/server/deployment/WAS-Cluster<server_name>-IBPMNode<#>Server
   ```

   Where:

<Workflow_Home> is the directory where Fujitsu Interstage BPM is installed, by default:

Windows: c:\Fujitsu\InterstageBPM

AIX: /opt/Fujitsu/InterstageBPM

2. Open the ibpm.properties file in a text editor of your choice and do the following:
   - **Windows**
     a. Update the following properties with the new workflow server port (by default, it is 49951):

        ```
        NamingProviderURL=
        JMSNamingProviderURL=
        ServerBaseURL=
        ServerEmailBaseURL=
        ```

     b. Save and close the file.
   - **AIX**
     a. If you changed the workflow server bootstrap port (by default, it is 20101) update the following properties with the new workflow server bootstrap port:

        ```
        NamingProviderURL=
        JMSNamingProviderURL=
        ```

     b. If you changed the workflow server application port (by default, it is 20108) update the following properties with the new workflow server application port:

        ```
        ServerBaseURL=
        ServerEmailBaseURL=
        ```

     c. Save and close the file.
3. Execute the importProperties script with the updated parameter values:
   - **Windows**

     ```
     importProperties.bat <Workflow_Home>\server\deployment\
     WLS-Cluster<server_name>-InterstageBPMCS<server#>\
     ibpm.properties <opworkflow_DB_username> <opworkflow_DB_password>
     ```

   - **AIX**
     a. Open the setIBPMenv.sh file in the text editor
     b. Replace the masked password in the DATABASE_PASSWORD parameter with the workflow database password. The password has been automatically masked using asterisks (***) during the installation. You need to replace the mask with clear text.
     c. Save this file.

        Note: Note: Before executing importProperties.sh, make sure that the user performing the installation has the permission to execute the script. If the user does not have the permission to execute importProperties.sh, enter the following command:

        ```
        chmod 755 importProperties.sh
        ```

     d. Run ./importProperties.sh
     e. Mask the password in the DATABASE_PASSWORD parameter with asterisks. For example, DATABASE_PASSWORD=*****
     f. Save and close the file.

Restart Services

Note: The information in this topic applies to both Oracle WebLogic and IBM WebSphere environments.

After completing the port changes, restart the OpenPages and workflow services.

For details, see Chapter 16, “Starting and Stopping Servers,” on page 465.

Update the Reporting Schema and Framework

Note: The information in this topic applies to both Oracle WebLogic and IBM WebSphere environments.

After services are restarted, you must re-create the reporting schema and regenerate the Reporting Framework V6 so that the port change is reflected in any redirects of CommandCenter reports.

For more details, see “Creating or Re-creating the Reporting Schema” on page 60 and “Updating the Reporting Framework” on page 64.

Configuring Global Administration Security in IBM WebSphere

By default, security is not enabled for the IBM WebSphere . To restrict access to administrative functions on the IBM OpenPages and/or workflow application server, you can configure global administration security in the IBM WebSphere Integrated Solutions Console.

Note: If you add new vertical or horizontal servers, make sure that the correct administrator user name and password are specified for the installation scripts (`install.properties`).

Enabling Global Administration Security

The following procedure requires you to enable global security on the application and workflow servers, and then disable the transaction protocol messaging option between application server cells (disabling this option does not affect application messages or the security of the server).

With the exception of using different port numbers, the process of configuring global security in the IBM WebSphere Integrated Solutions Console is the same for both the IBM OpenPages application and the workflow server.

Procedure

1. Open a browser window and log on to the IBM WebSphere Integrated Solutions Console as a user with administrative privileges.

   By default, the URL is `http://<host_name>:<port>/ibm/console`

   Where:

   `<host_name>` is the name of the server where the IBM WebSphere is installed.

   `<port>` is the server port number. By default, the installation port numbers are:

   - `9060` for the IBM OpenPages server (`IBM OpenPages Cell`)
   - `9061` for the workflow server (`IBPMCell`)
2. Expand **Security** in the left pane and click **Global security**.

3. In the Global security pane, do the following:
   a. Under **Administrative security**, select the **Enable administrative security** option.
   b. Clear the following options (if selected):
      - Enable application security
      - Use Java 2 security to restrict application access to local resources
   c. When finished, click **Apply** and then **Save** to save the changes in your local configuration to the master configuration.
4. For each application and workflow server in your environment, do the following:
   a. In the left pane of the Console, expand **Severs** > **Server Types** and then click **WebSphere application servers**.
   b. In the right pane, click the name of a server from the list.

      Example

      `<server_name>OPNode1Server1` (if this is an application server) or `<server_name>IBPMNode1Server` (if this is a workflow server)
   c. In the right pane for the selected server, under the **Container Settings** heading, expand **Container Services** and then click **Transaction Service**.
   d. In the Transaction service pane, select the **Configuration** tab (if not already selected, and clear the **Enable transaction coordination authorization** check box.
   e. When finished, click **OK** and then **Save** to save the changes in your local configuration to the master configuration.
   f. Repeat Steps a-e for each application and workflow server in your environment.
5. In the left pane of the Console, expand **System administration** and click **Nodes**.
   a. In the Nodes pane, select the check box next to each node listed in the table.
   b. When all the nodes are selected, click **Synchronize**.
6. Restart the Deployment Manager (DMgr), Node Agent (NA), and all servers.

Changing the IBM WebSphere Administrator User Account Password

Once global security in the IBM WebSphere Integrated Solutions Console is configured, you can change the password for the administrative user account as follows.

Note: The IBM OpenPages application and workflow servers have the same administrator account.

Procedure

1. Open a shell window and navigate to the `<OP_Home>/aurora/conf` directory.

   Where: `<OP_Home>` is the installation location of the IBM OpenPages application. By default this is `/opt/OpenPages`.
2. In the `conf` directory, locate the `was-admin-users.properties` file and do the following:
   a. Open the file in a text editor of your choice.
   b. Locate the following code line in the file:

      ```
      <admin>=<password value>
      ```

Where:

`<admin>` is the user name of the administrator account. By default, the user name in the file is 'admin'.

`<password value>` is the password of the administrator account.

c. Change the value following the equal sign to the new password (the new password will be in clear text).

d. When finished, save the file.

3. Restart all servers to re-encrypt and enable the new password.

Results

Note: On occasion, IBM WebSphere displays user name and password prompt boxes for the IBM OpenPages and/or workflow servers. If this occurs, manually type the new user name and password that was set in the `was-admin-users.properties` file into the prompt boxes.

Administering SSL

Accessing the IBM OpenPages Application Using SSL

To access the OpenPages application using a secure SSL connection, follow these instructions.

Procedure

1. Open a browser window.
2. Point to the following URL (assuming the default settings were kept during the installation):

   `https://<server_name>:<port>/openpages`

Results

Where:

`<server_name>` is the name of the server machine hosting the IBM OpenPages application.

`<port>` is the port number associated with the application server.

Example

`https://server01.com:7010/openpages`

Note: You must have an SSL digital certificate to use SSL with the OpenPages application.

For additional information on SSL configuration, see the *IBM OpenPages GRC Platform Installation Guide* .

Enabling and Disabling Secure Session Cookies

A secure session cookie tells the browser to only send the session cookie back over an encrypted HTTPS connection. This ensures that the cookie identifier is secure and should only be used with OpenPages when using HTTPS connections. When this feature is enabled, session cookies over an HTTP connection no longer work.

Use the following instructions to enable or disable secure session cookies on Oracle WebLogic or IBM WebSphere application servers.

On the Oracle WebLogic Application Server

Procedure

1. Navigate to the weblogic.xml file in the \sosa\WEB-INF directory as follows:

   `<OP_HOME>\applications\op-apps\sosa\WEB-INF`

   Where: <OP_HOME> is the installation location of the OpenPages application.
2. Make a back up copy of the weblogic.xml file by copying it to a safe location.
3. Edit the weblogic.xml file as follows:
   a. Open the weblogic.xml file in a text editor of your choice.
   b. Do one of the following:

To do this...	Under the `<session-descriptor>` element, do this...
Enable secure session cookies	Add the following code
Disable secure session cookies	Remove the following code

```
<session-param>
     <param-name>CookieSecure</param-name>
     <param-value>true</param-value>
</session-param>

<session-param>
     <param-name>URLRewritingEnabled</param-name>
     <param-value>false</param-value>
 </session-param>
```

   c. Save and close the file.
4. Repeat Steps 2 and 3 for the weblogic.xml file located in the \openpages\WEB-INF directory as follows:

   `<OP_HOME>\applications\op-apps\openpages\WEB-INF`
5. If you have a clustered environment, repeat steps 1 through 4 on all application servers in your cluster.

On the IBM WebSphere Application Server

Procedure

1. Open a browser window and log on to the IBM WebSphere Integrated Solutions Console as a server administrator with the proper permissions.

   By default, the URL is http://<server_name>:<port>/ibm/console

   Where:

   <server_name> is the name of the application server

   <port> is the port number associated with the application server (for example, 9060).
2. In the left panel of the Integrated Solutions Console, do the following:
   a. Expand the tree for **Servers** | **Server Types**.
   b. Click the **WebSphere application servers** link in the list.
3. In the list on the Application servers page, click the name of the application server you want to configure.
4. On the **Application servers** *OpenPages -server-name* page, click the **Configuration** tab.
5. Under the **Container Settings** heading on the **Configuration** tab, click the **Session management** link.

6. On the **Application servers** *OpenPages -server-name* **Session management** page, do the following:
   a. Verify that the **Enable cookies** setting is selected. If not selected, select the check box to enable the link for the setting.
   b. Click the **Enable cookies** link.
   c. On the **Application servers** *OpenPages -server-name* **Session management** > **Cookies** page, configure the **Restrict cookies to HTTPS sessions** setting as follows:

To do this...	Then do this...
Enable secure session cookies	Select the **Restrict cookies to HTTPS sessions** check box.
Disable secure session cookies	Clear the **Restrict cookies to HTTPS sessions** check box.

7. When finished, click **Apply**.
8. Repeat Steps 5-8 for all available application servers.

Renewing SSL Certificates for IBM OpenPages

Periodically, SSL certificates need to be renewed and re-imported into your OpenPages environment.

In general, the process for renewing a certificate is similar to the process for installing new certificates. You create a new certificate request and import the signed certificate into the appropriate keystores. You do not need to repeat the steps for configuring SSL and changing property files for OpenPages, unless information contained in the certificate changes.

Certification Authorities provide instructions on how to submit renewal applications and import the signed certificates. Follow those instructions in conjunction with the following tasks.

See either:

- "Renewing SSL Certificates in an Oracle WebLogic Server Environment"
- "Renewing SSL Certificates in a IBM WebSphere Application Server Environment" on page 439

Renewing SSL Certificates in an Oracle WebLogic Server Environment

In order to renew an SSL certificate for an IBM OpenPages GRC Platform in an Oracle WebLogic Server environment, create a new certificate signing request, submit it to a CA, and import the signed server certificate.

If there is no change to the root certificate, you should not have to re-import the root certificate or import certificates into client browsers.

If you want to use the same alias for the certificate, you must delete the key pair in the keystore first. If you use a different alias for the certificate, you must configure Oracle WebLogic Server with this new alias.

Procedure

1. Log on to each IBM OpenPages server as a user with administrative privileges.

2. Create the Certificate Signing Request (CSR) by generating a keystore, key pair, and a Certificate Signing Request (CSR) file.

   For details on these tasks, see "Configuring OpenPages for SSL in an Oracle WebLogic Server Environment" in the *IBM OpenPages GRC Platform Installation Guide* .

3. Submit the request to the Certification Authority (CA).
   a. Submit the CSR to your Certification Authority (CA) to renew the certificate. Follow the instructions provided by your CA on how to submit the CSR.
   b. Download the approved root and CA certificates to a local directory. Make sure the certificates are named to distinguish the root from the CA certificate.
4. Import the certificate.

   Import the renewed server certificate into each application server by performing the following tasks:
   a. Log on to each OpenPages server as a user with administrative privileges.
   b. Launch a Command Prompt window (using the **Run as Administrator** option).
   c. Navigate to the `OpenPagesDomain` directory in `<OP_Home>`.

      By default, `C:\<OP_Home>\OpenPagesDomain`
   d. Use the **`Keytool`** command within the `OpenPagesDomain` directory to import the server certificate (`.cer`) or certificate chain (`.p7b`) using the following command:

      ```
      keytool -import -alias <certificate_name> -trustcacerts -file <file_name>
      -keystore <keystore_name>
      ```

      Where:

      - `import` imports the certificate.
      - `alias` is the name of the certificate.
      - `file` specifies the name of the file to store the certificate. The command may require the full path name.
      - `keystore` is the keystore associated with the certificate.
      - `trustcacerts` imports the certificate as a trusted certificate

      Example

      The example imports the `servercert` certificate into the `opkeystore` file.

      ```
      keytool -import -alias opkeystore -trustcacerts
      -file servercert.cer -keystore opkeystore.jks
      ```
   e. Enter the password for the keystore.
   f. Enter `Yes` to trust the certificate.
5. Update Oracle WebLogic server.

   If you changed the alias name, you must update the alias for the IBM OpenPages administrative server and workflow server using the Oracle WebLogic Server Administrative Console. For details on these tasks, see "Configuring OpenPages for SSL in an Oracle WebLogic Server Environment" in the *IBM OpenPages GRC Platform Installation Guide* .

Renewing SSL Certificates in a IBM WebSphere Application Server Environment

In order to renew an SSL system for an IBM OpenPages GRC Platform in an IBM WebSphere Application Server environment, create a new certificate signing request, submit it to a Certification Authority, and import the signed server certificate.

Procedure

1. Log on to cluster administrator server as a user with administrative privileges.
2. Create the certificate request.
   a. Navigate to the IBM WebSphere Integrated Solutions Console: `http://<server_name>:<port>/ibm/console`

      where `<server_name>` is the name of the application server and `<port>` is the IBM WebSphere Application Server port assigned during the IBM WebSphere Application Server installation (9060 by default).
   b. Log in to the IBM WebSphere Integrated Solutions Console as with an administrator account.
   c. Expand the tree for **Security | SSL certificate and key management** in the left panel.
   d. On the **SSL certificate and key management** page, click the **Keystores and certificates** link in the **Related Items** list.
   e. Click the keystore for your IBM OpenPages environment, by default `opkeystore`.
   f. Click **Personal certificate requests** in the **Additional Properties** list to create a certificate request.
   g. On the **Personal certificates requests** page, select the certificate request you want to renew and click **Extract**.
   h. Enter a name for the certificate request, for example `ServerCertificateRequest.cer`.
   i. Click **OK**.

   The certificate request file is created in `<OP_Home>/profiles/OpenPagesDmgr/etc`.
3. Submit the request to the Certification Authority (CA).
   a. Submit the Certificate Signing Request (CSR) to your Certification Authority (CA) to renew the certificate. Follow the instructions provided by your CA on how to submit the CSR.
   b. Download the approved root and CA certificates to the `<OP_Home>/profiles/OpenPagesDmgr/etc` directory. Make sure the certificates are named to distinguish the root from the CA certificate.
4. Import the certificate.

   Import the renewed server certificate into each application server by performing the following tasks:
   a. Log on to cluster administrator server as a user with administrative privileges.
   b. Navigate to the IBM WebSphere Integrated Solutions Console: `http://<server_name>:<port>/ibm/console`

      where `<server_name>` is the name of the application server and `<port>` is the IBM WebSphere Application Server port assigned during the IBM WebSphere Application Server installation (9060 by default).
   c. Log in to the IBM WebSphere Integrated Solutions Console as with an administrator account.

d. Expand the tree for **Security | SSL certificate and key management** in the left panel.
e. On the **SSL certificate and key management** page, click the **Keystores and certificates** link in the **Related Items** list.
f. Click the keystore for your OpenPages environment, by default `opkeystore`.
g. Click **Personal certificates** in the **Additional Properties** list.
h. On the **Personal certificates requests** page, click **Receive from a certificate authority**.
i. Enter the name (and file path) of the signed certificate and click **OK**.

5. Update IBM WebSphere Application server.

   If you changed the alias name, you must update the alias for the OpenPages admin server and workflow server using the IBM WebSphere Integrated Solutions Console. For details on these tasks, see "Configuring OpenPages for SSL on a IBM WebSphere Application Server" in the *IBM OpenPages GRC Platform Installation Guide* .

Renewing SSL Certificates for CommandCenter

Periodically, SSL certificates need to be renewed and re-imported into your CommandCenter environment.

In general, the process for renewing a certificate is similar to the process for installing new certificates. You create a new certificate request and import the signed certificate into the appropriate keystores. You do not need to repeat the steps for configuring SSL and changing property files for OpenPages, unless information contained in the certificate changes.

Certification Authorities provide instructions on how to submit renewal applications and import the signed certificates. Follow those instructions in conjunction with the following tasks.

See either:

- "Renewing Certificates for CommandCenter Environments on an IIS Web Server"
- "Renewing Certificates for CommandCenter Environments on an Apache Web Server" on page 442

Renewing Certificates for CommandCenter Environments on an IIS Web Server

Perform these steps for the web server on any reporting server that will handle external CommandCenter traffic.

About this task

The information in this topic applies only to Windows environments.

Procedure

1. Generate a key pair and request.
   a. Log on to the reporting server as a user with administrative privileges.
   b. Launch the Windows Internet Information Services Manager, by clicking the **Start** menu, then selecting **Administrative Tools | Internet Information Services Manager**.

c. In the left pane of the **Internet Information Services Manager**, select the application server you want to configure.
d. In the **Features** view, double-click **Server Certificates**.
e. In the **Actions** pane, click **Create Certificate Request** to launch the Request Certificate Wizard.
f. On the **Distinguished Name Properties** screen of the wizard:

In this text box...	Do this...
Common name	Type a name for the certificate.
Organization	Type the name of the organization in which the certificate will be used.
Organizational unit	Type the name of the organizational unit in the organization in which the certificate will be used.
City/locality	Type the unabbreviated name of the city or locality where your organization or organizational unit is located.
State/province	Type the unabbreviated name of the state or province where your organization or organizational unit is located.
Country/region	Type the name of the country or region where your organization or organizational unit is located.

g. Click **Next**.
h. On the **Cryptographic Service Provider Properties** screen, select a cryptographic service provider from the list:
   - Microsoft RSA SChannel Cryptographic Provider
   - Microsoft DH SChannel Cryptographic Provider

   By default, IIS 7 uses the Microsoft RSA SChannel Cryptographic Provider.
i. On the **Cryptographic Service Provider Properties** screen, select a bit length that can be used by the provider from the **Bit length** drop-down list.

   By default, the RSA SChannel provider uses a bit length of 1024. The DH SChannel provider uses a bit length of 512. A longer bit length is more secure, but it can affect performance.
j. Click **Next**.
k. On the **File Name** page, in the **Specify a file name for the certificate** request field, use the **Browse** button or type a name for the certificate file.
l. Click **Finish**.

2. Submit the Certificate Signing Request (CSR) to Certification Authority (CA) for approval.
   a. Submit the CSR to your CA to renew the certificate. Follow the instructions provided by your CA on how to submit the CSR.
   b. Download the approved root and CA certificates to a local directory. Make sure the certificates are named to distinguish the root from the CA certificate.
3. Install the signed certificate.

   Import the renewed server certificate into each reporting server by performing the following tasks:
   a. Log on to the reporting server as a user with administrative privileges.

b. Launch the Windows Internet Information Services Manager, by clicking the **Start** menu, then selecting **Administrative Tools | Internet Information Services Manager**.
c. In the left pane of the **Internet Information Services Manager**, select the application server you want to configure.
d. In the **Features** view, double-click Server Certificates.
e. In the **Actions** pane, click Complete Certificate Request.
f. On the **Complete Certificate Request** screen:
   - In the **File name that contains the certification authority's** response field, use the **Browse** button or type the path of the file that contains the signed certificate.
   - In the **Friendly name** field, type a recognizable name for the certificate.
   - Click **OK**.

Results

At this point, the IIS web server has been fully configured for IIS. Next, you must configure CommandCenter to use the IBM OpenPages HTTPS address and SSL port. For details, see "Edit OpenPages Properties Files — Windows and AIX" in the *IBM OpenPages GRC Platform Installation Guide* .

Renewing Certificates for CommandCenter Environments on an Apache Web Server

Perform these steps for the web server on any reporting server that will handle external CommandCenter traffic.

About this task

The information in this topic applies only to AIX and Windows environments.

Procedure

1. Log on to the reporting server as a user with administrative privileges.

   Note: Log in as a non-root user, such as the user you created for the IBM OpenPages installation, for example: `opuser`.
2. Perform the following tasks to renew your certificate(s):
   a. Generate a key pair and request.
   b. Submit CSR to CA for approval.
   c. Import the server certificate.

   For details on these tasks, see "Configuring an Apache Web Server for SSL — Windows and AIX" in the *IBM OpenPages GRC Platform Installation Guide* .

Troubleshooting Browser Issues

This section contains the following topics:

- "Setting the Cognos Application Firewall (CAF) for Browser Security" on page 447
- "Setting a Session Inactivity Timeout Value" on page 448

Windows Internet Explorer 8 Browser Issues

Browser Display Issues and Internet Explorer 8

Note: The information in this section applies to IBM OpenPages version 5.5.2.1 or later.

If you are using the Microsoft Windows Internet Explorer® 8 (IE8) browser to display the:

- IBM OpenPages application
- Interstage BPM Console

then, you must use IE8 in Compatibility View for the application to display properly.

By setting Compatibility View, the IE8 browser will display the IBM OpenPages application and the Interstage BPM Console correctly as viewed in Internet Explorer® 7 (IE7).

Compatibility View can be set for multiple computers in an enterprise environment or for a single machine. For more information on configuring and using Compatibility View, see the following Microsoft articles:

- http://support.microsoft.com/kb/956197
- http://support.microsoft.com/kb/960321
- http://www.microsoft.com/nz/windows/internet-explorer/features/enhanced-navigation.aspx

Internet Explorer 8 Security Issues and Running Reports

Depending on how Internet Explorer 8 browser security is configured on client machines, CommandCenter reports may not launch successfully from the IBM OpenPages application user interface.

If a client machine using the Internet Explorer 8 browser is unable to run CommandCenter reports from the IBM OpenPages application user interface, then do the following:

- Add each reporting server to the **Trusted sites** zone in Internet Explorer 8 on that machine.
- Clear the **Require server verification (https:) for all sites in this zone** checkbox.
- Modify the options of the **Trusted Sites** zone and set the **Enable XSS Filter** property to **Disable**
- Set the security level for the **Trusted sites** zone to **Low**.
- Click the **Custom level properties** for the **Trusted Sites** zone. Under **Downloads**, set **Automatic prompting for file downloads** and **File download** to **Enable**.
- Restart the browser

For information on adding trusted sites to the browser, use the Internet Explorer 8 Help.

CSV View Report Issues

If you selected the **View in CSV Format** option after running a CommandCenter report and receive browser error messages, use the following troubleshooting information to resolve the issue.

- If you are using Microsoft Windows IIS and the following browser message is displayed, *Page cannot be found - HTTP 400 - Bad Request*, then use the instructions in the following link to configure the IIS Web server:

  https://www-304.ibm.com/support/docview.wss?uid=swg21388375
- If you are using Internet Explorer® 7 (IE7), you must configure browser security to allow for file downloads as follows

Procedure

1. From the IE7 toolbar, click the **Tools** menu and select **Internet Options**.
2. Click the **Security** tab.
3. Select the **Local intranet** zone (if not already selected).
4. Click the **Custom level...** button.
5. In the Settings pane, under **Downloads**, ensure that the **Automatic prompting for file downloads** option is set to **Enable**. If not, select **Enable** for this setting.
6. Restart the browser.

Browser Locale Settings and Messaging Issues

If a user sets their Internet Explorer browser to an unsupported locale, logon and other IBM OpenPages GRC Platform application messages will be displayed only in English.

To ensure proper display of messages in the browser, users must set their browsers to a supported locale. For a list of supported locales, see Table 46 on page 235.

Browser Security Issues and Best Practices

The following sections contain a discussion of browser security issues relating to the HTTP referrer header and recommendations for improving security.

About Browser Security Environmental Issues and the HTTP Referrer Tag

The following security vulnerabilities may exist if a logged on user does any of the following from a valid OpenPages session in the same browser:

- Navigates to a different (non- IBM OpenPages) site and then returns to the IBM OpenPages application — the non- IBM OpenPages site could contain malicious code that might compromise secure information from the valid IBM OpenPages session.
- Navigates to a different (non- IBM OpenPages) site from a valid OpenPages session in the same browser, and then leaves the workstation unattended — any malicious user physically present in the same location could click the browser's Back button, or navigate to the IBM OpenPages session from the same browser.

Discussion

HTTP referrer tag is known to be the only means of identifying a web page or the resource (such as a PDF file or Mail client) that links to the current page. Referrer logging is commonly used to allow websites and web servers to identify where people are visiting them from, thus becoming a tool to combat cross-site request forgery http://en.wikipedia.org/wiki/HTTP_referrer - HTTP referrer at Wiki.

Some security issues associated with the referrer tag are as follows:

- The referrer tag is an optional HTTP request-header field, as noted in the W3C specification (http://www.w3.org/Protocols/HTTP/HTRQ_Headers.html#z14 - W3C specification). This means that browsers and other user agents can choose not to use or support this header in their implementation, be configured to not send the header, or can be behind a proxy or firewall that strips the header out. All of these limitations are noted in the official W3C working group note SVR3.
- Even if the referrer tag is enabled, various methods exist to combat its security mechanisms, one of which is referrer spoofing http://en.wikipedia.org/wiki/Referrer_spoofing - Referrer spoofing at Wiki. Therefore, it is never a completely secure mechanism.
- Internet Explorer 4.0 or later has a known issue where it will not send referrer headers in unsecured situations (http://support.microsoft.com/kb/178066 - IE Referrer known knowledge base (KB) issue). The referrer will also be empty if the page is accessed from either the bookmarks list or the address is typed directly into the address bar. Thus any security method using referrers can be completely inaccurate and can be modified from the client side. A common consensus among administrators, as a best practice, is to never use the referrer tag if security must work in all circumstances.
- Most security implementations (related to bank accounts, e-mail accounts) do not implement such a security mechanism. The most common method to enforce user account-level security is to use TIMEOUTs, which is a configurable option in the IBM OpenPages server platform.

HTTP referrer tag is known to be the only means of identifying a web page or the resource (such as a PDF file or Mail client) that links to the current page. Referrer logging is commonly used to allow websites and web servers to identify where people are visiting them from, thus becoming a tool to combat cross-site request forgery (http://en.wikipedia.org/wiki/HTTP_referrer - HTTP referrer at Wiki).

The referrer tag is an optional HTTP request-header field, as noted in the W3C specification. This means that browsers and other user agents can choose not to use or support this header in their implementation, be configured to not send the header, or can be behind a proxy or firewall that strips the header out. All of these limitations are noted in the official W3C working group note SVR3 (http://www.w3.org/Protocols/HTTP/HTRQ_Headers.html#z14 - W3C specification).

Even if the referrer tag is enabled, various methods exist to combat its security mechanisms, one of which is referrer spoofing. Therefore, it is never a completely secure mechanism (http://en.wikipedia.org/wiki/Referrer_spoofing - Referrer spoofing at Wiki).

Internet Explorer 4.0 or later has a known issue where it will not send referrer headers in unsecured situations. The referrer will also be empty if the page is accessed from either the bookmarks list or the address is typed directly into the address bar. Thus any security method using referrers can be completely inaccurate and can be modified from the client side. A common consensus among administrators, as a best practice, is to never use the referrer tag if security must work in all circumstances (http://support.microsoft.com/kb/178066 - IE Referrer known knowledge base issue).

Browser Best Practices

An IBM OpenPages browser session is active until one of the following occurs:

- The user logs out of the IBM OpenPages application

- The session expires
- The browser instance is closed

The following are some suggested best practices for enhancing browser security.

Users should be trained on the importance of always:

- Logging off an IBM OpenPages application session when they have finished their work and closing that browser window.

  Note: Closing the browser window ensures that no sensitive information has been stored in the browser's cache.
- Opening a new browser window to navigate to other web sites as follows.

For this version of Internet Explorer...	Open a new browser window as follows...
IE 7	Only from the Windows Start menu or a browser shortcut to navigate to other web sites.*
IE 8	Only from the browser File menu and clicking New Session to navigate to other web sites.*

  Note: * Browser windows opened by other methods will result in session sharing between Internet Explorer windows and/or tabs.
- Blocking their machines from external use when not physically present — either by keeping their machines on stand-by or by locking their accounts.
- Copying (not clicking) a link to the IBM OpenPages GRC Platform application from an e-mail and then pasting the link into the address bar of the browser window. After pasting the link, users should validate that the link they just pasted matches the link in the text of the e-mail message.
- Configuration of an inactivity timeout — administrators should set this to a desired security level based on commonly known levels of inactivity for their organization. For more information, see "Setting a Session Inactivity Timeout Value" on page 448.
- Configuration of the **Cross-site Scripting Filter** setting to check all HTTP `GET` requests sent to the OpenPages application server. For more information, see "Setting the Cross-site Scripting Filter" on page 280.

Optimizing Application Performance in the Internet Explorer Browser

To optimize the performance of the IBM OpenPages GRC Platform application in the Windows Internet Explorer browser, you can increase the disk space setting for temporary internet files to 200 MB on client machines.

Procedure

1. From the Internet Explorer toolbar, click the **Tools** menu and select **Internet Options.**
2. Click the **General** tab.
3. Under **Browsing history**, click **Settings**.
4. In the **Temporary Internet Files and History Settings** box, enter `200` in the disk space box.
5. When finished, click **OK**.

6. Restart the browser to effect the change.
   For additional information, see the Windows Internet Explorer Help.

Setting the Cognos Application Firewall (CAF) for Browser Security

To prevent URL redirection attacks in Cognos, we recommend that you use the following steps to enable CAF and configure a host list in Cognos Configuration.

The `backURL` parameter is a standard (and optional) Cognos URL parameter. This parameter, shown in the following example, can be modified to redirect a user to any site. Therefore, the potential exists for an attacker to also use this parameter to redirect a user to a malicious site where sensitive information could be exposed, such as the user's cookie.

```
https://test.my-company.com/cognos841/cgi-bin/cognos.cgi?b_action=xts.run
&m=portal/launch.xts&ui.tool=CognosViewer&ui.action=run&encoding=UTF8
&method=newQuery&backURL=http%3a%2f%2fwww.google.com&m=qs%2fqs.xts
&cafcontextid=&obj=%2fcontent%2fpackage%5b%40name%3d%27OpenPages%27%5d
```

The IBM Cognos 8 Business Intelligence version 8.4.1 *Installation and Configuration Guide*, Chapter 11: Configuration Options, section "Configure IBM Cognos 8 Components to Use IBM Cognos Application Firewall" indicates that the standard method for performing positive validation of URL input parameters and data is to use the CAF (Cognos Application Firewall) setting in the Cognos Configuration tool. If the data does not match a CAF rule, it is rejected.

The IBM OpenPages GRC Platform Installer for CommandCenter enables the Cognos Application Firewall (CAF) by default.

CAF can be configured with a list of host names, including port numbers and domains that a user can access through the `backURL` parameter. If a `backURL` parameter contains a host or a domain name that does not appear in the list, the request will be rejected. An error message, similar to the following, will be displayed to users who try to access invalid domains or hosts through the `backURL` parameter:

```
DPR-ERR-2079 Firewall Security Rejection. Your request was rejected by the
security firewall.
```

The CAF setting has a known issue where enabling the firewall sometimes obscures useful error messages. For example, if a report author developed a report and that report had a logic flaw, a generic firewall error message (as shown above) would be displayed rather than a more useful message containing information about the cause of the actual problem.

Although generic firewall messages are considered a safe way to protect information, this type of nondescript CAF error message would make troubleshooting of report authoring/development and certain kinds of configuration issues more difficult.

Procedure

1. Log on to the reporting server as a user with administrative privileges.
2. Start IBM Cognos Configuration:

a. Launch a Command Prompt window (using the Run as Administrator option) or AIX shell.
b. Navigate to the <COGNOS_HOME>|bin64 or <COGNOS_HOME>|bin directory.

   Where: <COGNOS_HOME> is the installation location of the Cognos application. By default, this is:

   Windows:
   C:\OpenPages\Cognos\cognos\c8

   AIX: /opt/OpenPages/Cognos/cognos/cognos8
c. Execute the following command:

   Windows:
   cogconfig.bat

   AIX: ./cogconfig.sh

3. In the **Explorer** window, under **Security**, click **IBM Cognos Application Firewall**.
4. In the **Properties** window, for the **Enable CAF validation** property, set the appropriate values.

   By default, IBM Cognos Application Firewall is enabled.
5. Add host and domain names to the IBM Cognos list of valid names.
6. Save the configuration.

Setting a Session Inactivity Timeout Value

The IBM OpenPages system will time out an IBM OpenPages user session after a set period of browser inactivity.

By default, Oracle WebLogic has a 90-minute time-out period, and IBM WebSphere a 30-minute time-out period.

If wanted, you can modify the value of the inactivity time-out period (in minutes) as follows.

Setting a Session Inactivity Timeout Values in an Oracle WebLogic Environment

Procedure

1. Log on to the IBM OpenPages application server as a user with administrative permissions.
2. Stop all IBM OpenPages services (see "About Stopping IBM OpenPages Application Servers" on page 470).
3. Navigate to the <OP_Home>\applications\op-apps\sosa\WEB-INF directory.

   Where:

   <OP_Home> is the installation location of the IBM OpenPages application. By default, this is
   c:\OpenPages
4. In a text editor of your choice, open the web.xml file and look for the following code lines:

   ```
   <!-- Set the default session timeout (in minutes) -->
   <session-config>
   <session-timeout>90</session-timeout>
   </session-config>
   ```
5. Set the <session-timeout> parameter to the value (in minutes) that you want.
6. When finished, save the file and exit the editor.

7. If this is a load-balanced environment, repeat Steps 1-6 for each application server in the load-balanced environment until all are updated.
8. When finished, restart all IBM OpenPages services (see "Starting and Stopping OpenPages Application Servers" on page 465) to effect the change.

Setting a Session Inactivity Timeout Values in an IBM WebSphere Environment

Procedure

1. Open a browser window and log on to the IBM WebSphere Integrated Solutions Console as a server administrator with the proper permissions.

   By default, the URL is http://<server_name>:<port>/ibm/console

   Where:

   <server_name> is the name of the application server

   <port> is the port number associated with the application server (for example, 9060).
2. In the left panel of the Integrated Solutions Console, do the following:
   a. Expand the tree for **Applications** | **Application Types**.
   b. Click the **WebSphere enterprise applications** link in the list.
3. In the list on the Enterprise applications page, click the name of the resource you want to configure (for example, `op-apps`).
4. On the **Enterprise Applications** ***IBM OpenPages -resource-name*** page, click the **Configuration** tab (if not already selected).
5. Under the **Web Module Properties** heading on the **Configuration** tab, click the **Session management** link.
6. On the **Enterprise servers** ***IBM OpenPages -resource-name*** **Session management** page, do the following:
   a. Under **General Properties** find the Session timeout pane.
   b. In the pane, select the **Set timeout** option, if not already selected.
   c. In the **Set timeout** box, type a timeout value (in minutes). For example, 90 (by default, the value is set for 30 minutes).
   d. When finished, click **Apply**.

Configuring HTTP Compression in OpenPages

HTTP compression is a technique used to reduce the network bandwidth that is used to transfer files from the server to the client by compressing web content. Compliant web browsers automatically decompress the content before displaying it to users.

For IBM OpenPages application servers, HTTP compression is installed during the IBM OpenPages installation process.

By default, HTTP compression is disabled on IBM OpenPages application servers to reduce processor usage and improve performance over a local area network (LAN). On systems that use a router or switch to compresses data, you may also want to disable HTTP compression on both the IBM OpenPages application and/or CommandCenter servers in your environment to avoid double compression.

In situations where clients are primarily accessing the servers using a narrow network bandwidth (such as modems), we recommend enabling HTTP compression on both application and CommandCenter servers.

Note: Files that are already compressed, such as image files, PDF, and ZIP files will not be compressed to improve performance.

This section contains information on:

- "Enabling or Disabling HTTP Compression on IBM OpenPages Application Servers"
- "Enabling or Disabling HTTP Compression on the CommandCenter Server"

For information on installing and configuring HTTP Compression for Microsoft Windows IIS 7 only, see Appendix B, "Installing and Configuring HTTP Compression," on page 611

Enabling or Disabling HTTP Compression on IBM OpenPages Application Servers

Note: These steps apply to all IBM OpenPages application servers in a clustered environment.

Follow these steps to enable or disable HTTP compression on IBM OpenPages application servers via settings in the application user interface.

Procedure

1. Log on to the IBM OpenPages application user interface as a user with administrative permissions.
2. Access the Settings page (see "Accessing the Settings Page" on page 268).
3. Set the value in the **Show Hidden Settings** setting to `true` (for details, see "Showing Hidden Settings" on page 273).
4. Expand the **OpenPages | Applications | Common | Configuration | HTTP Compression** folder hierarchy.
5. Click the **Compression Enabled** setting to open its detail page.
6. In the **Value** box, type one of the following values. If the value is set to:
   - `true` – HTTP compression is enabled.
   - `false` - HTTP compression is not enabled.
7. When finished, click **Save**.

   The change will take effect immediately.

Enabling or Disabling HTTP Compression on the CommandCenter Server

This section contains HTTP compression information for the CommandCenter server running in a Windows or AIX environment.

Enabling or Disabling Compression on the CommandCenter Server Using Windows IIS

Note: The information in this topic applies only to a CommandCenter server running IIS 7 on Windows Server 2008.

Note: Before you can enable HTTP compression on a CommandCenter server running Windows, HTTP compression must first be installed and configured. To verify and/or configure static or dynamic compression on CommandCenter servers, see Appendix B, "Installing and Configuring HTTP Compression," on page 611.

Procedure

1. From the Windows **Start** menu on the CommandCenter server, select **Control Panel**.
2. Open Administrative Tools as follows:
   a. Do one of the following:

For Windows Server...	Do this...
2008	Click **System and Maintenance**.
2008 R2	Click **System and Security**.

   b. Click the **Administrative Tools** link.
3. Administrative Tools window, double-click **Internet Information Services (IIS) Manager**.
4. In the Connections pane:
   a. Expand Sites > Default Web Site.
   b. Select the name of the Cognos folder (for example, `cognos8`).
5. In Features View, under 'IIS':
   a. Double-click **Compression**.
   b. For the following check boxes, do one of the following:
      - To enable compression, select both 'Enable dynamic content compression' and 'Enable static content compression'.
      - To disable compression, clear both 'Enable dynamic content compression' and 'Enable static content compression'.
   c. In the Actions pane, click **Apply** when finished.

Enabling Compression on the CommandCenter Server Using Apache Web Server

Note: The information in this topic applies to Windows and AIX environments.

HTTP compression can be enabled or disabled on the Apache Web Server for Windows and AIX environments. The Apache source package includes the `mod_deflate` module, which provides for the compression of web content. By default, this module is not enabled.

Procedure

1. On the CommandCenter server, navigate to the `<Apache_Home>|conf` directory.
   Where: `<Apache_Home>` is the installation location of the Apache Web Server.
   Example

   Windows `C:\Program Files (x86)\Apache2.2`
   AIX `/opt/pware/`

2. Navigate to the `httpd.conf` file and do the following:
   a. Make a backup copy of the file before modifying it.
   b. Open the `httpd.conf` file in a text editor of your choice.
3. In the `httpd.conf` file, load the `mod_deflate` module as follows.
   a. Verify that the following statement is present at the beginning of the file:
   `LoadModule deflate_module modules/mod_deflate.so`

b. If the mod_deflate module statement in Step 3a is commented out (has a # (number sign) at the beginning of the line), then remove the # (number sign) so the compression module will be loaded.

4. At the bottom of the httpd.conf file, add the following block of configuration code to enable compression:

```
<IfModule deflate_module>
SetOutputFilter DEFLATE
<IfModule setenvif_module>
# Netscape 4.x has some problems
BrowserMatch ^Mozilla/4 gzip-only-text/html
# Netscape 4.06-4.08 have some more problems
BrowserMatch ^Mozilla/4\.0[678] no-gzip
# MSIE masquerades as Netscape, but it is fine
BrowserMatch \bMSI[E] !no-gzip !gzip-only-text/html
# Don't compress already-compressed files
SetEnvIfNoCase Request_URI \.(?:gif|jpe?g|png)$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \.pdf$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \.(?:exe|t?gz|zip|bz2|sit|rar)$ no-gzip dont-vary
# Make sure proxies don't deliver the wrong content
Header append Vary User-Agent env=!dont-vary
</IfModule>
</IfModule>
```

5. When finished, save the file.
6. Depending on your environment, do one of the following to restart the Apache Web Server.
   - For Windows:
     - Click the Windows **Start** menu and select **All Programs**.
     - From the **Administrative Tools** list, select **Services**.
     - Right-click the Apache2.2 service and select **Restart**.
   - For AIX:
     - Log on to the CommandCenter server as the root user.
     - Navigate to the <Apache_Home>/bin directory.
     - Enter the following command to stop the server:

       ```
       ./apachectl stop
       ```

     - Once the server is stopped, enter the following command to start the server:

       ```
       ./apachectl start
       ```

Disabling Compression on the CommandCenter Server Using Apache Web Server

Note: The information in this topic applies to Windows and AIX environments.

Procedure

1. On the CommandCenter server, navigate to the <Apache_Home>|conf directory.

   Where: <Apache_Home> is the installation location of the Apache Web Server.

   Example

   Windows C:\Program Files (x86)\Apache2.2
   AIX /opt/pware/

2. Navigate to the httpd.conf file and do the following:
   a. Make a backup copy of the file before modifying it.
   b. Open the httpd.conf file in a text editor of your choice.

3. From the bottom of the `httpd.conf` file, remove the following block of configuration code to disable compression:

```
<IfModule deflate_module>
SetOutputFilter DEFLATE
<IfModule setenvif_module>
# Netscape 4.x has some problems
BrowserMatch ^Mozilla/4 gzip-only-text/html
# Netscape 4.06-4.08 have some more problems
BrowserMatch ^Mozilla/4\.0[678] no-gzip
# MSIE masquerades as Netscape, but it is fine
BrowserMatch \bMSI[E] !no-gzip !gzip-only-text/html
# Don't compress already-compressed files
SetEnvIfNoCase Request_URI \.(?:gif|jpe?g|png)$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \.pdf$ no-gzip dont-vary
SetEnvIfNoCase Request_URI \.(?:exe|t?gz|zip|bz2|sit|rar)$ no-gzip dont-vary
# Make sure proxies don't deliver the wrong content
Header append Vary User-Agent env=!dont-vary
</IfModule>
</IfModule>
```

4. When finished, save the file.
5. Depending on your environment, do one of the following to restart the Apache Web Server.
   - For Windows:
     - Click the Windows **Start** menu and select **All Programs**.
     - From the **Administrative Tools** list, select **Services**.
     - Right-click the `Apache2.2` service and select **Restart**.
   - For AIX:
     - Log on to the CommandCenter server as the root user.
     - Navigate to the `<Apache_Home>/bin` directory.
     - Enter the following command to stop the server:

       ```
       ./apachectl stop
       ```

     - Once the server is stopped, enter the following command to start the server:

       ```
       ./apachectl start
       ```

Using Log Files

The IBM OpenPages application writes error and other messaging information to a standard set of log files. You can use these log files to troubleshoot reporting, workflow, and general user errors that may occur.

This section contains the following topics:

Configuring Application Thread-Dump Logs for Cluster Members

About Application Thread-Dump Logs for Cluster Members

Note: By default, application thread-dump logs are disabled. Use the instruction that follow to configure service thread-dump logs for cluster members.

Log folder location: <OP_Home>|aurora|logs

Where: <OP_Home> represents the installation location of the IBM OpenPages GRC Platform application. By default, this is:	
Windows	C:\OpenPages
AIX	/opt/OpenPages

Log file names are as follows:

Windows/Oracle WebLogic OpenPagesServer<#>-thread.dump.<time_stamp>.txt

Example

OpenPagesServer1-thread.dump.20101102.123348.243.txt

AIX/IBM WebSphere OPNode<#>Server<#>-javacore.<time_stamp>.txt

Example

OPNode1Server1-javacore.20101102.122628.7836.0001.txt

Configuring Service Thread-Dump Logs for Cluster Members

You can enable or disable thread-dump logs by changing the value of the periodic thread dump setting in the aurora.properties file as follows.

Procedure

1. Log on to the IBM OpenPages application server as a user with administrative privileges.
2. Open a command or shell window and navigate to the <OP_Home>|aurora|conf directory.
3. Locate the aurora.properties file in the conf directory and do the following:
   a. Open the aurora.properties file in a text editor of your choice.
   b. Search the file for the property 'periodic.thread.dump.enabled'.
   c. Change the property value following the equal sign as follows:

If the value is set to...	**Then...**
true	Thread-dumps are enabled.
false	Thread-dumps are disabled. This value is set by default.

   d. Save your changes and exit the editor.
4. Repeat Steps 1-4 for each cluster member for which you want to enable thread dumps.

Results

Note: You do not have to restart IBM OpenPages servers after changing the value of this property as the IBM OpenPages application monitors this property for changes.

Configuring Extended Access Logging

If you want to capture additional information for troubleshooting performance and other issues for a managed server, you will have to configure some additional access logging parameters in the Web server console.

This section includes instructions for both Oracle WebLogic and IBM WebSphere . Follow the instructions that correspond to your particular environment.

Oracle WebLogic - Configuring Extended Access Logging

Note: The information in this topic applies only to Oracle WebLogic environments.

Procedure

1. Start the IBM OpenPages application services (if not already started).
2. Open a browser window and log on to the Oracle WebLogic Server Administration Console as a user with administrative privileges.

   By default, the URL is `http://<host_name>:<port>/console`

   Where:

   `<host_name>` is the name of the server where Oracle WebLogic is installed.

   `<port>` is the server port number. By default, the installation port number is `7001` for the IBM OpenPages server (`IBM OpenPages Domain`).
3. In the Change Center pane of the Console, click **Lock & Edit** (if not already selected).
4. On the Home page, in the Domain Configurations pane, under the heading **Environment**, click the **Servers** link.
5. On the Summary of Servers page, click the name of the IBM OpenPages managed server you want from the **Servers** table listing.

   The format of the managed server name will look similar to this:

   `<host_name>-OpenPagesServer<#>`

   Where:

   `<host_name>` is the machine name of the managed server.

   `<#>` is the number of managed nodes on that particular server.
6. On the Settings for <managed-server-name> page, do the following:
   a. Click the **Logging** tab.
   b. On the **Logging** tab, click the **HTTP** tab.
   c. Scroll to the bottom of the page and click the **Advanced** link.
   d. In the **Extended Logging Format Fields** box, type the following value:

      `date time cs-method cs-uri-stem cs-uri-query sc-status time-taken`
   e. When finished, click **Save**.
   f. In the Change Center pane, click **Release Configuration** and log out.
7. To configure additional logging for another managed server, repeat Steps 3 - 6.
8. When finished, log out of the Console.

Results

Once configured, the `access.log` file will provide additional information. The log file is located in the following directory:

`OpenPages\OpenPagesDomain\servers\<servername>-OpenPagesServer<#>\logs`

IBM WebSphere - Configuring Extended Access Logging

Note: The information in this topic applies only to IBM WebSphere environments.

1. Start the IBM OpenPages application services (if not already started).
2. Open a browser window and log on to the IBM WebSphere Integrated Solutions Console as a user with administrative privileges.

   By default, if WAS global security is not enabled, the URL is: http://<host_name>:9060/ibm/console

   Where:

   `<host_name>` is the name of the server where IBM WebSphere is installed.
3. Expand **Servers** then **Server Types** in the left pane and click the **WebSphere application servers** link.
4. In the list on the Application servers page, click the name of the IBM OpenPages managed server you want from the list. For example:

   `<host_name>-OPNode<#>Server<#>`

   Where:

   `<host_name>` is the machine name of the managed server.

   `<#>` is the number of the node and server.
5. On the Application servers > <managed-server-name> page for the selected server, do the following:
   a. Click the **Configuration** tab (if not already selected).
   b. Under the **Troubleshooting** section of the page, click the link for **NCSA access and HTTP error logging**.
6. On the **Application servers > <managed-server-name>** > **NCSA access and HTTP error logging** page, under **General Properties**, do the following:
   a. Select the **Enable logging service at server start-up** setting.
   b. Make sure that the Enable access logging setting is selected. If not, select it.
   c. For the **NCSA access log format** setting, select one of the following:
      - **Common** - contains basic information, such as IP address, date/time stamp, request URI, and so forth.
      - **Combined** - contains the basic information plus additional referral, user agent, and cookie information.
   d. When finished, click **Apply** to apply the change and save it to master configuration.
7. Return to the On the Application servers page, and do the following:
   a. Under the **Select** column in the Application Server table, select the box next to the managed server you just updated.
   b. Click **Restart**.
8. To configure additional logging for another managed server, repeat Steps 3 - 6.

When the selected server is fully restarted, by default, a new log file named `http_access.log` will be created under `${SERVER_LOG_ROOT}`.

The exact value of SERVER_LOG_ROOT can be found by expanding Environment in the left pane of the Console and clicking the WebSphere variables link.

The path to the http_access.log file will be similar to this:
<OP_Home>/profiles/<host_name>-OPNode<#>/logs/<host_name>-OPNode<#>Server<#>

Where:

<OP_Home> is the installation location of the OpenPages application. By default, this is

/opt/OpenPages.

<host_name> is the name of the OpenPages application server.

<#> is the number of the node or server within that node (for example, OPNode1Server1).

IBM OpenPages Standard Application Server Log Files

Standard IBM OpenPages application log files are located as follows.

Log folder location: <OP_Home>|aurora|logs

Where: <OP_Home> represents the installation location of the IBM OpenPages GRC Platform application. By default, this is:	
Windows	C:\OpenPages
AIX	/opt/OpenPages

File names vary depending on your environment as follows.

Log File Names on Oracle WebLogic

Note: The information in this topic applies only to Windows environments.

Where:

<host_name> is the name of the IBM OpenPages application host.

Table 65. Windows/Oracle WebLogic Application Server Log Files

This log file...	**Contains this type of information...**
<host_name>-OpenPagesServer1-startup.log	Messages written during initialization of the IBM OpenPages application caches on the IBM OpenPages server.
<host_name>-OpenPagesServer1-aurora.log	Errors, exceptions, and informational messages written during IBM OpenPages application in use.

Log File Names on AIX/IBM WebSphere Application Server

Where:

<host_name> is the name of the IBM OpenPages application host.

<#> represents the number of the node and the number of the server within that node (for example, OPNode1Server1).

Table 66. AIX/IBM WebSphere Application Server Log Files

This log file...	Contains this type of information...
<host_name>-OPNode<#>Server<#>-startup.log	Messages written during initialization of the IBM OpenPages application caches on the IBM OpenPages server.
<host_name>-OPNode<#>Server<#>-aurora.log	Errors, exceptions, and informational messages written during IBM OpenPages application usage.

Oracle WebLogic Administrative Server and Cluster Member Log Files

Note: The information in this topic applies only to Windows environments.

Administrative Server Logs

Log folder location: <OP_Home>\OpenpagesDomain\servers\OpenpagesAdminServer\logs

Where:

<OP_Home> is the installation location of the OpenPages application. By default, this is c:\OpenPages.

This log file...	Contains this type of information...
access.log	Web server page access messages for the default 7001 or 7002 ports
OpenpagesAdminServer.log	Debugging and/or warning messages for the IBM OpenPages cluster administrative server.
OpenpagesDomain.log	• Debugging, warning, and/or error deployment messages for the OpenPagesAdminServer service • Memory usage messages for the OpenPagesAdminServer service

Application Cluster Member Logs

Log folder location: <OP_Home>\OpenpagesDomain\servers\<host_name>OpenPagesServer<#>\logs

Where:

<OP_Home> is the installation location of the OpenPages application. By default, this is c:\OpenPages.

<host_name> is the name of the IBM OpenPages managed server cluster member.

<#> is the number of the server.

This log file...	Contains this type of information...
access.log	Web server page access messages for the default 7009 or 7010 ports
<host_name>-OpenPagesServer<#>.log	• Debugging, warning, and/or error deployment messages for the OpenPagesAppServer service • Memory usage messages for the OpenPagesAppServer service

AIX/WAS DMGR Server, Node Agent, and Cluster Member Log Files

Deployment Manager (DMGR) Server Logs

Log folder location: <OP_Home>/profiles/OpenPagesDmgr/logs/dmgr

Where:

<OP_Home> is the installation location of the OpenPages application. By default, this is
/opt/OpenPages.

This log file...	Contains this type of information...
startServer.log	Log entries that monitor the status of starting the various application server components.
stopServer.log	Log entries that monitor the status of stopping the various application server components.
SystemErr.log	Error log entries written by the underlying IBM WebSphere application server.
SystemOut.log	Log entries written by the underlying IBM WebSphere application server about the status of various J2EE resources being used.

Node Agent Logs

Log folder location: <OP_Home>/profiles/<host_name>-Node1/logs/nodeagent

Where:

<host_name> is the name of the IBM OpenPages application server.

This log file...	Contains this type of information...
startServer.log	Log entries that monitor the status of starting administrative agents.
stopServer.log	Log entries that monitor the status of stopping administrative agents.
SystemErr.log	Error log entries written by the underlying IBM WebSphere application server.
SystemOut.log	Log entries written by the underlying IBM WebSphere application server about the status of various J2EE resources being used.

Application Cluster Member Logs

Log folder location:

<OP_Home>/profiles/<host_name>-OPNode<#>/logs/<host_name>-OPNode<#>Server<#>

Where:

<host_name> is the name of the IBM OpenPages application server.

<#> is the number of the node or server within that node (for example, OPNode1Server1).

This log file...	Contains this type of information...
startServer.log	Log entries that monitor the status of starting the cluster member.
stopServer.log	Log entries that monitor the status of stopping the cluster member.
SystemErr.log	Error log entries written by the underlying IBM WebSphere application server.
SystemOut.log	Log entries written by the underlying IBM WebSphere application server about the status of various J2EE resources being used.

Workflow Log Files

Standard workflow log files are located under various directories as described in this section. File names vary depending on your environment as follows.

Oracle WebLogic-specific Workflow Log Files

Note: The information in this topic applies only to Windows environments.

Where:

<Workflow_Home> represents the installation location of the Fujitsu Interstage BPM server.
By default, this is: c:\Fujitsu\InterstageBPM

<OP_Home> represents the installation location of the IBM OpenPages application.
By default, this is: C:\OpenPages

<host_name> is the name of the host machine.

<#> is the number of the server.

Table 67. Oracle WebLogic-specific Workflow Server Log Files

This log file...	Contains this type of information...
Log folder location: <Workflow_Home>|server|instance|default|logs	
<host_name>-InterstageBPMCS<#>.log	Records all runtime errors and exceptions logged by the Interstage BPM server application.
Log folder location: <Workflow_Home>|IBPMDomain|servers|<host-name>-serverName|logs	
<host_name>-InterstageBPMCS<#>.log	Log entries written by the underlying Oracle WebLogic application server about the status of various J2EE resources being used.
Log folder location: <OP_Home>|aurora|logs	
<host_name>-InterstageBPMCS<#>-startup.log	Messages written during initialization of the IBM OpenPages application caches on the Interstage BPM workflow server.
<host_name>-InterstageBPMCS<#>-aurora.log	Messages written by the IBM OpenPages integration code that runs on the Interstage BPM server.

AIX/WAS-specific Workflow Log Files

Where:

<Workflow_Home> represents the installation location of the Fujitsu Interstage BPM server.
By default, this is: /opt/Fujitsu/InterstageBPM

<OP_Home> represents the installation location of the IBM OpenPages application.
By default, this is: /opt/OpenPages

<host_name> is the name of the host machine.

<#> represents the number of the node.

Table 68. AIX/IBM WebSphere Workflow Server Log Files

This log file...	Contains this type of information...
Log folder location: <Workflow_Home>|server|instance|default|logs	
<host_name>-IBPMNode<#>Server.log	Records all runtime errors and exceptions logged by the Interstage BPM server application.
Log folder location: <Workflow_Home>|profiles|<host_name>-IBPMNode<#>|logs|<host_name>-IBPMNode<#>Server	
startServer.log	Log entries that monitor the status of starting the workflow server on the cluster member.
stopServer.log	Log entries that monitor the status of stopping the workflow server on the cluster member.
SystemOut.log	Log entries written by the underlying IBM WebSphere application server about the status of various J2EE resources being used.

Table 68. AIX/IBM WebSphere Workflow Server Log Files (continued)

This log file...	Contains this type of information...
SystemErr.log	Error log entries written by the underlying IBM WebSphere application server.
Log folder location: <OP_Home>|aurora|logs	
<host_name>-IBPMNode<#>Server-startup.log	Messages written during initialization of the IBM OpenPages application caches on the Interstage BPM workflow server.
<host_name>-IBPMNode<#>Server-aurora.log	Messages written by the IBM OpenPages integration code that runs on the Interstage BPM server.

Deployment Manager (DMGR) Workflow Logs:

Log folder location: <Workflow_Home>/profiles/IBPMDmgr/logs/dmgr

Where:

<Workflow_Home> represents the installation location of the Fujitsu Interstage BPM server.
By default, this is: /opt/Fujitsu/InterstageBPM.

This log file...	Contains this type of information...
startServer.log	Log entries that monitor the status of starting the various workflow server components.
stopServer.log	Log entries that monitor the status of stopping the various workflow server components.
SystemErr.log	Error log entries written by the underlying IBM WebSphere application server.
SystemOut.log	Log entries written by the underlying IBM WebSphere application server about the status of various J2EE resources being used.

Node Agent Workflow Logs:

Log folder location: <Workflow_Home>/profiles/<host_name>-IBPMNode<#>/logs/nodeagent

Where:

<host_name> is the name of the IBM OpenPages application server.

<#> is the number of the node.

This log file...	Contains this type of information...
startServer.log	Log entries that monitor the status of starting administrative agents.
stopServer.log	Log entries that monitor the status of stopping administrative agents.

This log file...	Contains this type of information...
SystemErr.log	Error log entries written by the underlying IBM WebSphere application server.
SystemOut.log	Log entries written by the underlying IBM WebSphere application server about the status of various J2EE resources being used.

Chapter 16. Starting and Stopping Servers

This chapter contains the following topics:

Starting and Stopping OpenPages Application Servers

About Services and Scripts Used by the OpenPages Application

The OpenPages application runs only if all of the services are started and all of the services for all supporting applications are running.

About Using Windows Services

Note: The information in this topic applies only to Windows environments.

The following table lists Windows services associated with the OpenPages application and workflow servers.

Table 69. OpenPages and Fujitsu Interstage BPM Services on Windows

Service Name	Description
OpenPagesAdminServer	Starts or stops the OpenPages Admin service. **Note:** In a horizontal-cluster environment, cluster members do not have an OpenPages Admin service.
OpenPagesServer#	Starts or stops an OpenPages managed server. **Where:** # represents the number of the managed server. In a cluster environment, the number for each managed server increments by one.
InterstageBPMAdminServer	Starts or stops the Fujitsu Interstage BPM Deployment Manager service.
InterstageBPMCS#	Starts or stops the Fujitsu Interstage BPM application server. **Where:** # represents the number of the managed server. In a cluster environment, the number for each managed server increments by one.

About Using AIX Scripts

Note: The information in this topic applies only to AIX environments.

In the AIX environment, OpenPages includes a number of scripts to initiate and launch the OpenPages application environment.

Note: These scripts can be run individually or you can use wrapper scripts to start and stop OpenPages .

The following table lists the scripts required to start and stop the OpenPages application.

Table 70. OpenPages and Fujitsu Interstage BPM Scripts on AIX

Script Name	Description
Fujitsu Interstage BPM:	
startManager.sh	Starts the Fujitsu Interstage BPM Deployment Manager.
startNode.sh	Starts the Fujitsu Interstage BPM node agent.
startServer.sh	Starts the Fujitsu Interstage BPM application server.
stopManager.sh	Stops the Fujitsu Interstage BPM Deployment Manager.
stopNode.sh	Stops the Fujitsu Interstage BPM node agent.
stopServer.sh	Stops the Fujitsu Interstage BPM application server.
OpenPages Application:	
startManager.sh	Starts the OpenPages Deployment Manager.
startNode.sh	Starts the OpenPages node agent.
startServer.sh	Starts the OpenPages application server.
stopManager.sh	Stops the OpenPages Deployment Manager.
stopNode.sh	Stops the OpenPages node agent.
stopServer.sh	Stops the OpenPages application server.
Scripts for Both Applications:	
startAllServers.sh	Starts all OpenPages and Fujitsu Interstage BPM services in the correct sequence.
stopAllServers.sh	Stops all OpenPages and Fujitsu Interstage BPM services in the correct sequence.

About Starting Application Servers

This section describes how to start the OpenPages application in both a Windows and AIX environment.

In a Windows environment, the services required to start the OpenPages application servers can be configured to start automatically.

In an AIX environment, you need to manually run scripts to start the OpenPages application servers.

Important: :

- You must start the OpenPagesAdminServer service (Windows) or run the OpenPages startManager script (AIX) first and then the other services/scripts as described in the following procedures.
- If you are running OpenPages in a load-balanced environment, you must start the server on the cluster administrator first before starting any cluster members.

About First Time Start Up

The first time you start the OpenPages server, it must precompile all of the included JSPs. This initialization process of the environment can take up to several minutes to complete. This only applies to the very first time OpenPages starts after installation. Future startups take much less time.

Determining Application Readiness

To determine whether the application is ready to be accessed after starting up servers, do the following.

Procedure

1. Open the log file specified in the following table.

If this...	Navigate to this folder...	View this log file...
Windows	<OP_Home>\ OpenPagesDomain\servers\ <host_name>- OpenPagesServer1\logs	<host_name>- OpenPagesServer<#>.log
AIX	<OP_Home>/profiles/ OpenPagesDmgr/logs/dmgr	startServer.log

   Where:

   <OP_Home> represents the installation location of the OpenPages application.

   <host_name> is the name of the server.

   <#> is the number of the server.

2. Scroll to the bottom of the log file and look for a message stating that the web application server is "running in Production Mode". If this line appears, the server is running in production mode and the application is ready to be accessed.

Starting OpenPages in a Windows Environment

In a Windows environment, all OpenPages and Fujitsu Interstage BPM services can be configured to start automatically or you can start the services manually, as described in this section.

If you need to start or restart the OpenPages application, you must start the services or scripts in the proper sequence using one of the following three methods.

Automatically Starting OpenPages Application Servers

Note: The information in this topic applies only to Windows environments.

By default, all OpenPages and Fujitsu Interstage BPM services are configured as Manual, (will not start upon reboot).

You can configure all OpenPages and Fujitsu Interstage BPM services to Automatic through Windows Services to start upon booting, or use scripts on each server to start the services upon reboot.

When you reboot the server, all OpenPages and Fujitsu Interstage BPM services will start.

Starting All OpenPages Application Services Using a Script

Note: The information in this topic applies only to Windows environments.

The StartAllServers.cmd script included with OpenPages will start all OpenPages and Fujitsu Interstage BPM services in the proper sequence.

Procedure

1. Log on to the OpenPages application server as a user with administrative privileges.
2. Open a Command Prompt window (using the **Run as Administrator** option) and do the following:
   a. Navigate to the <OP_Home>\bin directory.

      Where: <OP_Home> is the installation location of the OpenPages application. By default, this is: c:\OpenPages.
   b. Run the following command to start the OpenPages and Fujitsu Interstage BPM services:

      ```
      StartAllServers.cmd
      ```

      When all services have been started, the Command Prompt window closes.

Starting OpenPages Application Services Individually Using Windows Services

Note: The information in this topic applies only to Windows environments.

In the Windows environment you start the OpenPages application by starting the required OpenPages and Fujitsu Interstage BPM services.

Procedure

1. Log on to the OpenPages application server as a user with administrative privileges.
2. Click the Windows **Start** menu and select **All Programs**.
3. From the **Administrative Tools** list, select **Services**.
4. Start the OpenPagesAdminServer service, if present.

   Note: A cluster member does not run the OpenPagesAdminServer service.
5. Start the OpenPagesServer# service.
   Where: # represents the number of the managed server.

   Note: If there is more than one managed server on the current system, you must start the service (OpenPagesServer#) for each managed server in sequence before proceeding to the Fujitsu Interstage BPM services.
6. Start the InterstageBPMAdminServer service, if present.

   Note: A cluster member does not run the InterstageBPMAdminServer service.

7. Start the InterstageBPMCS# service.
   Where: # represents the number of the managed server.

   As services are starting, Windows Services may indicate that the services have started, but background OpenPages processes may still be running. It may take a few minutes for the OpenPages service to be operational.

Starting OpenPages in an AIX Environment

In AIX, all OpenPages and Fujitsu Interstage BPM services can be started using a single script or you can start the services manually, as described in this section.

Starting All OpenPages Application Servers Using a Script

Note: The information in this topic applies only to AIX environments.

The `startAllServers.sh` script included with OpenPages will start all OpenPages and Fujitsu Interstage BPM services in the proper sequence.

Procedure

1. Log on to the OpenPages application server as a user with administrative privileges.
2. Open an AIX shell window and do the following:
   a. Navigate to the <OP_Home>/bin directory.

      Where: `<OP_Home>` is the installation location of the OpenPages application. By default, this is: `/opt/OpenPages`.
   b. Run the following script to start the OpenPages and Fujitsu Interstage BPM services:

      ```
      ./startAllServers.sh
      ```

Starting OpenPages Application Servers Individually Using Scripts

Note: The information in this topic applies only to AIX environments.

Use the following steps to start the OpenPages and Fujitsu Interstage BPM services manually. In the AIX environment, you run a set of scripts to start the OpenPages application.

Procedure

1. Log on to the OpenPages application server as a user with administrative privileges.
2. Use an AIX shell to navigate to the <OP_Home>/profiles/OpenPagesDmgr/bin directory.
3. Enter the following command to launch a script that starts the OpenPages Deployment Manager:

   ```
   ./startManager.sh
   ```
4. After the script completes successfully, navigate to the <OP_Home>/profiles/OpenPagesNode1/bin directory.
5. Enter the following commands, in the order specified, to launch scripts that start the OpenPages Node Agent and the OpenPages application server:

   ```
   ./startNode.sh
   ./startServer.sh OPNode#Server#
   ```

   Where: `OPNode#` is the node that the current server is in and `Server#` is the number of the server within that node. **Example**: `OPNode1Server1`.

Note: If there is more than one managed server on the current system, you must run the start script (./startServer.sh OPNode#Server#) for each managed server in sequence before proceeding to the Fujitsu Interstage BPM scripts.

6. After the script completes successfully, navigate to the {app_server_root}/Profiles/IBPMDmgr/bin directory.
7. Enter the following command to launch a script that starts the IBPM Deployment Manager:

   ```
   ./startManager.sh
   ```

8. After the script completes successfully, navigate to the {app_server_root}/profiles/IBPMNode1/bin directory.
9. Enter the following commands, in the order specified, to launch scripts that start the IBPM Node Agent and the IBPM application server:

   ```
   ./startNode.sh
   ```

   ```
   ./startServer.sh IBPMNode#server
   ```

   Where: `IBPMNode#` is the node that the current server is in. Do not specify a server number as only one server should exist for each Fujitsu Interstage BPM node. **Example**: `IBPMNode1server`.

   When the scripts complete successfully, the OpenPages application is properly started.

About Stopping IBM OpenPages Application Servers

This section describes how to stop the OpenPages application server in both the Windows and AIX environment.

Stopping the application server prevents the OpenPages application from being accessed.

Important:

- You must stop the InterstageBPMCS# service(s) (Windows) or run the Fujitsu Interstage BPM stopServer.sh script (AIX) first and then the other services or scripts as described in the following procedures. Otherwise, you risk losing data or corrupting the installation.
- If you are running OpenPages in a load-balanced environment, you must stop the server on each cluster member first before stopping the cluster administrator.

Stopping OpenPages in a Windows Environment

In a Windows environment, all OpenPages and Fujitsu Interstage BPM services can be configured to stop automatically or you can stop the services manually, using one of the following three methods.

Automatically Stopping OpenPages Application Servers

Note: The information in this topic applies only to Windows environments.

Windows automatically and gracefully stops the OpenPages application when a server shuts down.

Stopping All OpenPages Application Services Using a Script

Note: The information in this topic applies only to Windows environments.

The `StopAllServers.cmd` script included with OpenPages will stop all OpenPages and Fujitsu Interstage BPM services in the proper sequence.

Procedure

1. Log on to the OpenPages application server as a user with administrative privileges.
2. Launch a Command Prompt window (using the **Run as Administrator** option).
3. Navigate to the <OpenPages_Home>/bin directory.
4. Enter the following command to launch a script that stops the OpenPages and Fujitsu Interstage BPM services:

   ```
   StopAllServers.cmd
   ```

   When all services have been stopped, the Command Prompt window closes.

Stopping OpenPages Application Services Individually Using Windows Services

Note: The information in this topic applies only to Windows environments.

You can stop the OpenPages application without shutting down or rebooting the machine. Use the following steps to stop OpenPages services manually.

Important: Stopping the OpenPages Admin service before stopping each managed server will cause the OpenPages application to stop on all servers. This could result in the loss of data and other problems.

In the Windows environment, you stop the OpenPages application by stopping the required OpenPages and Fujitsu Interstage BPM services.

Procedure

1. Log on to the OpenPages application server as a user with administrative privileges.
2. Click the Windows **Start** menu and select **All Programs**.
3. From the **Administrative Tools** list, select **Services**.
4. Stop the InterstageBPMCS# service.
   Where: # represents the number of the managed server.
5. Stop the InterstageBPMAdminServer service, if present.

   Note: A cluster member machine does not run the InterstageBPMAdminServer service.
6. Stop the OpenPagesServer# service.
   Where: # represents the number of the managed server.

   Note: If there is more than one managed server on the current system, you must stop the service (OpenPagesServer#) for each managed server before stopping the OpenPagesAdminServer service. The managed servers can be stopped in any order.
7. Stop the OpenPagesAdminServer service, if present.

   Note: A cluster member machine does not run the OpenPagesAdminServer service.

   When the services are stopped successfully, the OpenPages application is properly shut down.

Stopping OpenPages in an AIX Environment

In an AIX environment, all OpenPages and Fujitsu Interstage BPM services can be stopped using a single script or you can stop the services manually, as described in this section.

Stopping All OpenPages Application Servers Using a Script

Note: The information in this topic applies only to AIX environments.

The `stopAllServers.sh` script included with OpenPages will stop all OpenPages and Fujitsu Interstage BPM services in the proper sequence.

Procedure

1. Log on to the OpenPages application server as a user with administrative privileges.
2. Use an AIX shell to navigate to the <OpenPages_Home>/bin directory.
3. Enter the following command to launch a script that starts the OpenPages and Fujitsu Interstage BPM services:

   ./stopAllServers.sh

Stopping OpenPages Application Servers Individually Using Scripts

Note: The information in this topic applies only to AIX environments.

In the AIX environment, you run a set of scripts to stop the OpenPages application.

Procedure

1. Log on to the OpenPages application server as a user with administrative privileges.
2. Navigate to the {app_server_root}/profiles/IBPMNode1/bin directory.
3. Enter the following commands, in the order specified, to launch scripts that stop the IBPM application server and the IBPM Node Agent.

   ./stopServer.sh IBPMNode#Server

   ./stopNode.sh

   Where: # is the node number that the current server is in. A server number is not required as only one server should exist for each Fujitsu Interstage BPM node.
4. After the scripts complete successfully, navigate to the {app_server_root}/profiles/IBPMDmgr/bin directory.
5. Enter the following command to launch a script that stops the IBPM Deployment Manager:

   ./stopManager.sh
6. After the script completes successfully, navigate to the <OpenPages_Home>/profiles/OpenPagesNode1/bin directory.
7. Enter the following commands, in the order specified, to launch a script that stops the OpenPages application server and the OpenPages Node Agent.

   ./stopServer.sh OPNode#server#

   ./stopNode.sh

Where: OPNode# is the node that the current server is in and Server# is the number of the server within that node. **Example**: OPNode1Server1.

If there is more than one managed server on the current system, you must run the stop server script (./stopServer.sh OPNode#server#) for each managed server before running the stop node agent script (./stopNode.sh). The managed servers can be stopped in any order.

8. After the scripts complete successfully, navigate to the <OpenPages_Home>/profiles/OpenPagesDmgr/bin directory.
9. Enter the following command to launch a script that stops the OpenPages Deployment Manager:

   ./stopManager.sh

   When the script completes successfully, the OpenPages application is properly shut down.

Starting and Stopping the Database Server

This section describes how to stop, start or restart the database server in both the Windows and AIX environment.

Starting and Stopping the Database Server in a Windows Environment

Note: The information in this topic applies only to Windows environments.

The following table lists Windows services associated with the OpenPages Oracle database instance.

Table 71. OpenPages Oracle Services on Windows

Service Name	Description
OracleOPXRepos_server112_se_x64TNS ListenerOPX600011GEMx64se	Runs the Oracle Database listener service, which connects the user to the Oracle Database instance.
OracleService<SID>	Used to start and stop the Oracle Database instance. **Where:** <SID> represents the database instance identifier.

Use the following steps to start or stop database services using Windows Services.

Procedure

1. Log on to the database server as a user with administrative privileges.
2. Click the Windows **Start** menu and select **All Programs**.
3. From the **Administrative Tools** list, select **Services**.
4. For each database service listed in the above table, do the following:

If you want to...	Then do this...
Start the server	Right-click the service name and select **Start**.
Stop the server	Right-click the service name and select **Stop.**

Starting and Stopping the Database Server in an AIX Environment

Note: The information in this topic applies only to AIX environments.

Procedure

1. Log on to the database server as a user with administrative privileges.
2. In a shell window, navigate to the following directory:

   `<Oracle_Home>/openpages_data/repository/server112_se_x64/software`

   Where:

   `<Oracle_Home>` is the installation location of the Oracle database directory. By default, this is `/opt/oracle`.
3. Execute the following command:

   ```
   ./oprepository.sh <tnsalias_name> <listener_name> <sysdba_password>
    <argument_value>
   ```

   Where:

   `<tnsalias_name>` is the TNS alias of the database service.

   `<listener_name>` is the listener service.

   `<sysdba_password>` is the password for the database `sys` user.

   `<argument_value>` is the argument value that is passed to the database server.

   Valid argument values are:

   - start
   - shutdown
   - abort
   - restart

   Example

   The following example starts the database server.

   ```
   ./oprepository.sh AIX61 OPX61GEM openpages start
   ```

Starting and Stopping the CommandCenter Server

This section describes how to start or stop the CommandCenter server and the OpenPages Framework Model Generator service in both the Windows and AIX environments. Use any of the following methods.

Note that the IBM Cognos Configuration tool will display the status of the start-up, which can be helpful with troubleshooting, if necessary.

Starting and Stopping the CommandCenter Server

Use one of the following procedures, as appropriate, to start or stop the CommandCenter server.

Using the IBM Cognos Configuration Tool to Start and Stop the CommandCenter Server

Note: The information in this topic applies to Windows and AIX environments.

Procedure

1. Log on to the reporting server as a user with administrative privileges.
2. Start the IBM Cognos Configuration tool as follows:
   a. Open a Command Prompt window (using the **Run as Administrator** option) or AIX shell and navigate to the `<Cognos_Home>|bin64` or `<Cognos_Home>|bin` directory.

Where: `<Cognos_Home>` represents the installation location of the Cognos application. By default, this is:	
Windows	`C:\OpenPages\Cognos\cognos\c8`
AIX	`/opt/OpenPages/Cognos/cognos/cognos8`

   b. Execute one of the following commands to open the tool:

Windows `cogconfig.bat`
AIX `./cogconfig.sh`

3. Do one of the following:

To do this...	Then...
Start the server	Click **Actions** | **Start.** (It may take several minutes for the service to start the first time.) If the **Start** option is not available, the server has already started. **Note:** The start-up may pause if you have not configured a mail server. Click **OK** in the dialog box that displays, then click **Continue**.
Stop the server	Click **Actions** | **Stop.**

Using the Windows Operating System to Start and Stop CommandCenter

Note: The information in this topic applies only to Windows environments.

Use the following steps to start or stop the CommandCenter service in a Windows environment using Windows Services.

Procedure

1. Log on to the reporting server as a user with administrative privileges.
2. Click the Windows **Start** menu and select **All Programs**.
3. From the **Administrative Tools** list, select **Services**.
4. Do one of the following:

To do this...	Then...
Start the server	Right-click the `CommandCenter` service and select **Start**.
Stop the server	Right-click the `CommandCenter` service and select **Stop.**

Using the AIX Operating System to Start and Stop CommandCenter

Note: The information in this topic applies only to AIX environments.

Use the following steps to start or stop the CommandCenter server in an AIX environment using command-line scripts.

Procedure

1. Log on to the reporting server as a non-root user with administrative privileges.
2. Launch an AIX shell and navigate to the `bin` directory as follows:
   `<Cognos_Home>/bin`

   Where:
   `<Cognos_Home>` is the installation location of the Cognos application. By default, this is: /opt/OpenPages/Cognos/cognos/cognos8/configuration
3. Do one of the following:

To do this...	Then...
Start the server	Enter the following command: `./startup.sh`
Stop the server	Enter the following command: `./shutdown.sh`

Starting and Stopping the OpenPages Framework Model Generator Service

Use one of the following procedures, as appropriate for your operating system, to start or stop the OpenPages Framework Model Generator Service.

Using the Windows Operating System to Start and Stop the Framework Model Generator

Note: The information in this topic applies only to Windows environments.

Use the following steps to start or stop the Framework Model Generator Service in a Windows environment using Windows Services.

Procedure

1. Log on to the reporting server as a user with administrative privileges.
2. Click the Windows **Start** menu and select **All Programs**.
3. From the **Administrative Tools** list, select **Services**.
4. Do one of the following:

To do this...	Then...
Start the server	Right-click the `OpenPages Framework Model Generator` service and select **Start**.
Stop the server	Right-click the `OpenPages Framework Model Generator` service and select **Stop.**

Using the AIX Operating System to Start and Stop the Framework Model Generator

Note: The information in this topic applies only to AIX environments.

Use the following steps to start or stop the Framework Model Generator Service in an AIX environment using command-line scripts.

Procedure

1. Log on to the reporting server as a non-root user with administrative privileges.
2. Open an AIX shell as a user with administrative privileges and navigate to the following directory:

   `<CommandCenter_Home>/apache-tomcat-6.0.26/bin -- or --`
   `<CommandCenter_Home>/apache-tomcat/bin`

   Where `<CommandCenter_Home>` is the installation location of the CommandCenter. By default, this is: `/opt/OpenPages/CommandCenter`.
3. Do one of the following:

To do this...	Then...
Start the server	Enter the following command: `./startup.sh`
Stop the server	Enter the following command: `./shutdown.sh`

Starting the IBM Cognos 8 Go! Dashboard Service

Use the following steps to manually start the Go! Dashboard service on a CommandCenter machine.

Windows

On a Windows system, the `IBM Cognos 8 Go! Dashboard` service is configured, by default, to start automatically when Windows starts. If the service is stopped, you can use Windows Services to restart the service as follows.

Procedure

1. Log on to the reporting server as a user with administrative privileges.
2. Click the Windows **Start** menu and select **All Programs**.
3. From the **Administrative Tools** list, select **Services**.
4. Do one of the following:

To do this...	Then...
Start the service	Right-click the `IBM Cognos 8 Go! Dashboard` service and select **Start**.
Stop the service	Right-click the `IBM Cognos 8 Go! Dashboard` service and select **Stop.**

AIX

For an AIX environment, use the following steps.

Procedure

1. Log on to the reporting server as a non-root user with administrative privileges.

2. Open an AIX shell and navigate to:
   `<go_dashboard_location>/dashboard/bin`
3. Run the following script to start the Go! Dashboard service:
   `./startup.sh`

Chapter 17. Migrating IBM OpenPages Environments

If your organization has multiple IBM OpenPages environments, you can use IBM OpenPages environment migration to move both configuration and metadata from one environment to another through the IBM OpenPages application, without needing physical access to either environment. Migration means exporting from a source environment and importing into a target environment.

Note: You can also use ObjectManager, a command line interface (CLI) tool, to migrate configuration changes. For more information, see "Importing Configuration Changes" on page 533.

About Migrating IBM OpenPages Environments

An IBM OpenPages environment is a set of IBM OpenPages servers that target a single database instance, inclusive of that database instance.

Many organizations use different IBM OpenPages environments for specific purposes. For example, one company may use the following environments:

- Development environment - A specific set of servers where changes are made to the IBM OpenPages metadata.
- Test environment - A specific set of servers where configuration changes from the development environment are tested.
- UAT environment - A specific set of servers where configuration changes from the test environment are reviewed by end users before being released to the production environment.
- Production environment - A specific set of servers where tested and reviewed metadata changes are made available to the end users.

Other organizations may combine development and testing into a single environment for generating and testing metadata changes, and use a second environment for production.

The environment from which you want to export data is referred to as the source and the environment into which you want to import data is referred to as the target.

Settings That Apply to Environment Migration

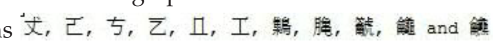
The environment migration settings are found in the **OpenPages | Applications | GRCM | Environment Migration** folder hierarchy.

For instructions on accessing the settings page, see "Accessing the Settings Page" on page 268.

Table 72. Environment Migration Settings

Setting	Definition
Asynchronous Timeout	The timeout value (in seconds) for AJAX calls on environment migration pages. The default is 120.

Table 72. Environment Migration Settings (continued)

Setting	Definition
Export File Name Prefix	Prefix to be added to the environment migration export JAR file name. The default prefix `openpages` is used if no value is given. Prefix length is limited to 15 characters. If the prefix is longer than 15 characters, it is truncated. **Important:** • The following characters cannot be used in the prefix: `\ / | * : { } [ ] " ?` • Do not use the special characters as defined in CJK Compatibility Ideographs Unicode Block Name and the four-byte characters as defined in the CJK Unified Ideographs EXTENSION-B Unicode Block Name (such as ) in the Export File Name Prefix.
Process Log Report Page Spec	The location of the Process Log Report Page Spec. This value was previously fixed and can now be set. The default is `/_cw_channels/Reporting/Hidden Reports/CommandCenter/Administrative Reports/Environment Migration/Process Log Report.pagespec`
Special Character Validation	Specifies whether or not special characters are checked while validating names of metadata. The default is **true**. Set to **false** to preserve legacy special character rules.

The **ImportConfiguration** and **ExportConfiguration** Application Permissions are required to allows members of user groups to access the environment migration tool for import and export. For details on these permissions, see " IBM OpenPages Application Permissions" on page 20.

For an overview of Environment Migration, see Chapter 17, "Migrating IBM OpenPages Environments," on page 479.

Supported Migration Items

In any scenario, you can use the environment migration capability to move any of the following metadata items between any two compatible IBM OpenPages environments:

- Object Profiles
- Object Types
- Field Groups
- Fields
- Application Text
- Object Text
- Error Text
- Filter Definitions
- Field Dependencies
- Dependency Picklists
- Object Type Relationships
- Rulesets
- Settings (excludes machine specific settings in the OPX Repository)
- Object Type Dimensions

- Recursive Object Levels
- Date Dimension Types
- Date Dimension Type Associations

Important: You must use the ObjectManager tool rather than the configuration migration export and import capability in the user interface when migrating field groups that contain four-byte characters as defined in the CJK Unified Ideographs EXTENSION-B Unicode Block Name (such as [illegible] and [illegible]). For information on ObjectManager, see Chapter 19, "Using the ObjectManager Tool," on page 517

The environment migration process creates a file in the Java ARchive (JAR) format (referred to in this document as a migration file) that is automatically saved to the repository.

The exported migration file is named in the `<export file name prefix>-env-mig-<MMddYYkkmmss>` format; where:

- the <export file name prefix> is the export file name prefix setting (see "Settings That Apply to Environment Migration" on page 326), truncated if the prefix exceeds 15 characters;
- the timestamp portion of the file name represents the month (MM), the day (dd), the year (YY), hour (kk), minute (mm), and seconds (ss) when the export was started.

For example, `openpages-env-mig-011712031416`.

About Exporting Dependencies

When exporting configuration items, the export process automatically determines if there are any dependencies required by the configuration items and adds those dependencies to the migration file.

The dependencies that will be exported for each type of item are listed in the following table.

Table 73. Dependent Items Exported

This item...	Exports this dependency...
Object profile	• views • object types (including all object type dependencies) • field groups (including all field group dependencies) • view labels
Object type	• field groups (including any underlying fields) • dependencies • dependent picklists • filters • root folders • object type images • corresponding settings and object strings • object type relationships • file types (if the object type is file-upload based)
Field group	Any underlying fields

Table 73. Dependent Items Exported (continued)

This item...	Exports this dependency...
Application strings	Any corresponding string keys
Object type dimensions	Any recursive object levels, if associated
Date dimension type associations	Any corresponding date dimension types

About Import Validation

The environment migration import process automatically validates all migrated configuration items as the first step of an import, verifying that:

- The XML is well-formed, according to the DTD.
- The metadata attributes are valid, according to IBM OpenPages validation rules.
- All dependent items that a particular item requires are present in either in the migration file or in the target system.
- Special characters are validated if the special character validation setting is true (see "Settings That Apply to Environment Migration" on page 326).

For example, if a particular profile is selected for import, validation will check for any missing object types, fields, or field groups, allowing you to take corrective actions before the profile is loaded into the target environment.

Additionally, you can manually run the validation process separate from the import.

Note: We strongly recommend that you manually validate all data before importing the configuration items into the target environment.

The validation process provides feedback through a detailed CommandCenter-style report on the current status, the number of correctly validated items, and any inconsistencies or failed validations.

Items Not Migrated

The following items are not exported by the environment migration. These items will not be available for import into a target environment and the validation process will not identify these as missing.

If any of the items you plan to migrate has a dependency on one or more of these items, you will need to manually move the dependent item or items prior to using environment migration. For help determining if any dependencies will not be migrated and how to manually move those dependencies, contact IBM OpenPages Customer Support.

Configuration Settings Not Migrated

The configuration settings listed in Table 74 on page 483, are not migrated by environment migration.

Important: Do not attempt to change the security model with the **OpenPages | Common | Security | Model** setting on the source system if there is instance data in the target system. If you do, the configuration settings import will fail.

Note: The hidden settings will not be migrated if the **Show Hidden Settings** setting is set to false. For details, see "Showing Hidden Settings" on page 273. To allow the migration of the hidden settings, set the **Show Hidden Settings** setting to true.

Table 74. Configuration Settings Not Exported

Setting description	Location
Mail server name	**OpenPages | Applications | Common | Email | Mail Server**
Guest password on server	**OpenPages | Platform | Application Server Guest Password**
JMS listener urls for all paired servers	**OpenPages | Platform | Global Caches | JMS | Listener Urls**
Default OpenPages e-mail sender address	**OpenPages | Platform | Publishing | Mail | From Address**
Default OpenPages e-mail server	**OpenPages | Platform | Publishing | Mail | Host**
Default OpenPages e-mail username	**OpenPages | Platform | Publishing | Mail | Username**
OpenPages detail page name for reference by CommandCenter	**OpenPages | Platform | Reporting Schema | Object URL Generator | Detail Page**
OpenPages server name for reference by CommandCenter	**OpenPages | Platform | Reporting Schema | Object URL Generator | Host**
OpenPages server port for reference by CommandCenter	**OpenPages | Platform | Reporting Schema | Object URL Generator | Port**
OpenPages application protocol for reference by CommandCenter	**OpenPages | Platform | Reporting Schema | Object URL Generator | Protocol**
Default workflow e-mail sender address	**OpenPages | Platform | Workflow | Email | Mail From**
Default workflow e-mail server	**OpenPages | Platform | Workflow | Email | Mail Server**
Export File Name Prefix	**OpenPages | Applications | GRCM | Environment Migration | Export File Name Prefix**

Metadata Items Not Migrated

The following metadata items are not migrated by environment migration. If any of these items is not in the target environment, you need to manually move the items.

- triggers
- workflows
- custom query subjects
- JSPs
- Role Templates
- instance data

User Security Not Migrated

User security is not migrated by the environment migration.

If there are profiles in the system containing user fields that have been scoped to specific security domain groups, verify that the same security domain groups are in place in the target environment. If not, configure the target environment to match the source.

The import validation process will stop the import if any required security domain group is not present in the target environment. An error in the following format will appear in the validation Log Details report:

```
<line#> Processing 'displayTypePropertyValue', Attribute: 'name', Value:
'<group Name>' is not defined in the migration package or in the target
system!: Group Missing!
```

User fields can have a scope defined that filters the amount of returned search data. This scope definition is based on security domain groups in the IBM OpenPages environment. However, these security groups are not migrated by the environment migration.

If a user field has a scope defined in the source environment, but that configuration does not exist in the target environment, the import will be stopped.

For more information on setting the scope definitions, see "Configuring User and Group Selector Display Types for Simple Strings" on page 224.

CommandCenter Reports Not Migrated

CommandCenter reports are not migrated by the environment migration.

If a profile contains an embedded report that is not available in the target environment, a user with that profile will see a message in the IBM OpenPages interface that the report is missing.

Important: If you want a user to access an embedded report that is not present in the target environment, you must manually move the report from the source environment to the target environment **before** migrating the environment.

Item Dependencies Not Migrated by Default

Environment migration automatically determines if there are any dependencies required by the exported items and adds those dependencies to the migration file.

However, some items that can be exported for migration are not included automatically as dependencies.

The following metadata item is not exported as a dependency:

- **Namespaces**. If a profile includes a computed field that relies on a namespace, and that namespace does not exist (or is defined differently) in the target environment, the profile will pass import validation. However, a user will not be able to access the computed field in the target environment.

  To avoid this scenario, make sure that all namespaces upon which computed fields have a dependency are included in the export JAR.

Environment Migration Best Practices

When using environment migration to move metadata and configuration items from one environment to another, use the following best practice guidelines to help ensure a smooth transition of information:

- Settings cannot be imported if the target system does not have the dependencies specified in the settings values. To migrate the settings, first migrate the dependencies (such as Object Types, Field Groups and Recursive Object Levels) without the settings. Then, migrate the settings using a separate JAR.
- Import configuration items during planned downtime, when end users are not accessing that environment. Issues could arise if an end user is working with an item while that item is being imported.
- Replicate the metadata on your production environment to the development and/or test environment where you will be making and testing configuration changes.

  Using the same configuration data in all environments ensures that:

  – All environments will operate on the same baseline set of IBM OpenPages metadata as a starting point.
  – Any test configurations or items in a test or development environment will be removed, preventing those items from being migrated inadvertently to production.

  For more information on replicating environments, see Using the OpenPages Backup Utility.
- Make modifications and additions to configuration items in a test and/or development environment. Once the items are fully tested, then migrate the items to the production environment.
- Before importing configuration items, validate the data using the IBM OpenPages migration capabilities described in "Validating the Migration File" on page 488.
- If a background import, export, or validate configuration process is currently running on the system, you must wait until processing is complete before submitting another configuration job.

About the Environment Migration Process

From a single client system, you can use the IBM OpenPages application to select and export changed configuration items from one IBM OpenPages environment, then import the items into a second environment. The environment migration import process automatically validates the imported items to ensure they will work properly in the new environment.

Table 75 outlines the process for exporting changed configuration items from a source environment and importing those changed items into a target environment using environment migration.

Table 75. Tasks for Migrating Data Items Using Environment Migration

Use this environment...	To do this task...
Source	Export the configuration items into a JAR file. See "Exporting Configuration Items from the Source Environment" on page 486.
Target	Verify that all the configuration items are valid in the target environment. See "Validating the Migration File" on page 488.

Table 75. Tasks for Migrating Data Items Using Environment Migration (continued)

Use this environment...	To do this task...
Target	Import the configuration items into the current environment. See "Importing Configuration Items to the Target Environment" on page 487.

Exporting Configuration Items from the Source Environment

You can create a new migration file each time you perform an export or you can add additional items to an existing migration file. The migration file is automatically saved to the repository and can optionally be saved to a local client.

Important:

- If a background import, export, or validate configuration process is currently running on the system, you must wait until processing is complete before submitting another configuration job.
- You cannot export while in System Administration Mode (SAM). For details, see "Enabling and Disabling System Admin Mode" on page 58.

Before you begin

Only an IBM OpenPages Super Administrator or a user with ExportConfiguration permission can access the **Export Configuration** menu item. For information about assigning application permission to a user, see "Configuring Application Permissions" on page 18.

Procedure

1. Log on to the source IBM OpenPages application as a user with the **Export Configuration** permission.
2. Disable System Administration Mode, if enabled. For details, see "Enabling and Disabling System Admin Mode" on page 58.
3. From the menu bar, select **Administration** and click **Export Configuration**.
4. On the **Export Options** tab, do one of the following:
   a. Under **Create a new migration package**, select **Export local configuration** to create a new migration file and click **Submit**.
   b. Under **Create new export based on a previously saved migration package (JAR)** select either **Local disk** or **Server repository**. Click the **Browse** button to locate the migration file to use, then click **Submit**.

      Note: If you selected the wrong package, reload the **Export Configuration** page or click the browser's **Back** button.
5. In the **Choose items to export** tab, select the type of item to export from the **Choose type** drop-down list.
6. In the **Select items** pane, use the list or the tree structure to select specific items to export or click **All** to select all the items of that type. Click **None** to clear the list of selected items. The **Review items** pane displays the current count of each type.
7. Repeat Steps 5 and 6 for each type of item you want to export.
8. Optionally, to review the details of the selected items, click the links in the **Review selected items** pane. All items of that type selected for export are displayed in the **Selected item details** pane.

9. Click the **Clear** button to remove the items from the display. Clearing the list will not remove the items from the file.

   To remove an item from the migration file, select the type of item to remove from the **Choose type** drop-down list. Locate the item(s) in the list or the tree structure and clear the check box.

10. When you have selected the objects to export, click the **Save migration file** button.

    The **Export History** pane shows the progress of the export.

    View a detailed status by clicking the **View Log** icon to launch the Log Summary report. This report shows the number of items that have been logged in the Process Log Report, under the **Full system detail log** link. See "About Migration Reports" on page 491.

11. Click the **Refresh** button in the **Export History** pane to update the progress on screen in real-time. When the export is complete, the **Export History** pane will display a message indicating if the export completed successfully or with errors. If successful, the migration file is saved to the OpenPages repository. If the `Completed With Errors` message appears, you can use the migration reports to determine the nature of the error. See "About Migration Reports" on page 491,.

    The **Export Configuration** page returns to the initial state, allowing you to perform additional exports, as needed.

Importing Configuration Items to the Target Environment

You can load the migration file into the target environment by downloading the file from the IBM OpenPages repository or importing a saved file from the local client.

The import process automatically validates the configuration items before performing the import to ensure that the items are complete and any object dependencies are in the migration file or in the target environment before the items are imported (see "About Import Validation" on page 482). If there are any validation errors, the import process will be stopped. You can launch a validation report to view details on the errors.

To avoid validation errors, review the information on dependent items that must be manually created and/or moved to the target environment. For details, see "Items Not Migrated" on page 482.

Only an IBM OpenPages Super Administrator or a user with the ImportConfiguration permission can access the **Import Configuration** menu item. For information about assigning application permission to a user, see "Configuring Application Permissions" on page 18.

Important: The environment migration import process may periodically enable System Administration Mode (SAM), preventing users from making and saving changes (see "Enabling and Disabling System Admin Mode" on page 58). To avoid errors in the imported data and other issues, the migration should be performed during off-hours or when the target environment is not being used.

Configuring Environment Migration to Allow Special Characters

The environment migration import process checks for any special characters in the name of the items being imported. By default, if any item has a name with a special character, the import will stop.

Before you begin

In order to import metadata items that use special characters in the name, you must disable this validation.

Procedure

1. Access the **Settings** page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages** | **Application** | **GRCM** | **Environment Migration** folder hierarchy.
3. Click the **Special Character Validation** setting to open its detail page.
4. In the **Value** box, type one of the following values:

If the value is set to...	Then...
true	The import will check for special characters in the name of metadata items being imported. This value is set by default.
false	The import will allow metadata items with special characters in the name to be imported.

5. Click **Save**.

Validating the Migration File

This task is optional, but we recommend that you validate the data so you can remedy issues before running the import process.

Important: If a background import, export, or validate configuration process is currently running on the system, you must wait until processing is complete before submitting another configuration job.

Procedure

1. Log on to the target IBM OpenPages application as a user with the **Import Configuration** permission.
2. From the menu bar, select **Administration** and click **Import Configuration**.
3. On the **Import Options** tab, select one of the following based on where the migration file is located:
   a. **Local Disk** to import a file from the local machine. The migration files are in the JAR format.
   b. **Server repository** to import a migration file from the IBM OpenPages repository.
4. Click the **Browse** button to locate the migration file to import.
5. Click the **Submit** button.

6. To review the details of the selected items, click the links in the **Review items in the migration package** pane. All items of that type selected for import are displayed in the **Selected item details** pane.

   Click the **Clear** button to remove the items from the display. Clearing the list will not remove the items from the file.

   Note: If you selected the wrong migration file, reload the **Import Configuration** page or click the browser's **Back** button.
7. Click **Validate** to begin the validation process. The **Import History** pane shows the progress of the validation. You can view a detailed status by clicking the **View Log** icon.
8. Click the **Refresh** button in the **Import History** pane to update the progress on screen. When the validation is complete, the **Import History** pane will display a message indicating if the validation completed successfully or with errors.

Results

If the `Completed With Errors` message appears, you can use the migration reports to determine the nature of the error. See "About Migration Reports" on page 491. If there are any validation errors, these errors will need to be addressed before importing.

If there are warnings in the migration reports, these can be safely ignored, and you can continue with the import.

Performing the Import for Environment Migration

Use the following instructions to import configuration changes.

Important: Do not manually make changes to the application configuration during the import. This can corrupt the data or result in errors. In either case, you would need to re-export the data before attempting the import again.

Important: If a background import, export, or validate configuration process is currently running on the system, you must wait until processing is complete before submitting another configuration job.

Before you begin

- If the profiles that are being exported have home page report tabs, or report listings in the classic tab configured, then those reports have to be manually imported into the target system first, since environment migration does not support reports.
- On the target system, check the value of the **OpenPages | Applications | GRCM | Home Page | Maximum Reports Listing** setting. This setting must have a value that is equal to, or greater than, the value for this setting in the source system. For instructions on accessing the settings page, see "Accessing the Settings Page" on page 268.

Procedure

1. Log on to the target IBM OpenPages application as a user with the **Import Configuration** permission.
2. From the menu bar, select **Administration** and click **Import Configuration**.
3. On the **Import Options** tab, select one of the following, based on where the migration file is located:

a. **Local Disk**to import a file from the local machine. The migration files are in the JAR format.
b. **Server repository** to import a file from the IBM OpenPages repository.

4. Click the **Browse** button to locate the migration file to import.
5. Click the **Submit** button.
6. To review the details of the selected items, click the links in the **Review items in migration package** pane. All items of that type selected for import are displayed in the **Selected item details** pane.

   Click the **Clear** button to remove the items from the display. Clearing the list will not remove the items from the file.

   Note: If you selected the wrong migration file, reload the **Import Configuration** page or click the browser's **Back** button.
7. When you are satisfied with the data to import, click the **Import** button. The environment migration process automatically validates the data before importing.

   The process will either:

   - Import the data, if there are no validation errors;
   - Stop the import if there are validation errors. If there are errors that need to be corrected, see "Environment Migration Best Practices" on page 485.

   The **Import History** pane shows the progress of the import. You can view a detailed status, by clicking the **View Log** icon.
8. Click the **Refresh** button in the **Import History** pane to update the progress on screen. When the import is complete, the **Import History** pane will display a message indicating if the import completed successfully or with errors. If the `Completed With Errors` message appears, you can use the migration reports to determine the nature of the error. See "About Migration Reports" on page 491. The **Import Configuration** page returns to the initial state, allowing you to perform additional imports, as needed.

Results

- After a successful import, you can optionally view detailed feedback, click the **View Log** icon to download a CommandCenter report with feedback on the current status, number of correctly validated items, and any inconsistencies or failed validations.

  Note: After importing a migration file, the repository will list the imported file using the end time of the import in the `<export file name prefix>-<YYYY_MM_dd_kk_mm>` format. If you need to import the migration file into another system, you should select the exported migration file.

  For example, if the **Import History** window indicates that the migration file `migration-100311120839` was imported, then after that file was imported, the repository shows that `migration-100411031232.jar` was created. If you need to import this package of changes into another system, you would select the `migration-100311120839.jar` file. (The name indicates that the Export File Name Prefix is `migration`.)
- If, as part of the Configuration Migration import operation, updates are made to the **OpenPages | Platform | Reporting Framework V6 | Configuration | Supported Triangle Relationships** setting, you must update the Reporting Schema with the new triangle views. For instructions, see "About Updating the Reporting Schema" on page 60.

About Migration Reports

You can view reports that provide details on the migration process (export, validation or import) run on the system.

Log Summary Migration Report

To view a summary report, click the **View Log** icon next to any ongoing or complete migration processes in the **History** pane. The Log Summary report is a CommandCenter report that lists the status of the items in the process.

For exports, only the **Full System Detail Log** is generated.

The report contains the following status fields:

- **Successes**. The number of items that were validated or imported without error. Click the link to view further details on the successfully processed items.
- **Warnings**. The number of items that resulted in a warning. Click the link to view further details on the warnings. If there are warnings, these can be safely ignored. They will not affect the processing.
- **Failures**. The number of items that resulted in some error. Click the link to view further details on the items that failed during the validation.
- **Overall Items Processed**. The total number of items validated or imported.
- **Full System Detail Log**. The number of items recorded in the Log Details report.

When a validation or an import encounters warnings and/or failures, the description of the message usually indicates how to correct the problem.

For example, if an attribute is missing or an item is missing a parent dependency, you would need to correct the issue on the source system and export the file again. Or, you can contact IBM OpenPages Customer Support for assistance.

Log Details Migration Report

During or after an export, validation, or import process has been run, click the **Full System Detail Log** link in the Log Summary report to view full details on the process. The information in the report depends upon the process being performed:

- **Export**. When exporting, the Log Details report lists the items exported and an overview of the number and type of items exported.
- **Validation**. When validating, the Log Details report lists the items being validated and whether the item is valid or there is an error.
- **Import**. When importing, the Log Details report first provides information about the validation process, listing the items being validated and whether the item is valid or there is an error. If the validation succeeds, the report provides information on the import process, listing the items imported and an overview of the number and types of items imported.

Chapter 18. Working With Cluster Members

This chapter contains the following topics:

- "Adding Members to a Vertical Cluster"
- Adding Members to a Horizontal Cluster

Adding Members to a Vertical Cluster

This section describes how to add an OpenPages application and workflow managed server to an existing cluster in the following environments:

- "Adding Vertical Cluster Members to an Existing Installation in an Oracle WebLogic Environment"
- "Adding Vertical Cluster Members to an Existing Installation in an IBM WebSphere Environment" on page 506
- "Adding Members to a Horizontal Cluster" on page 515

Adding Vertical Cluster Members to an Existing Installation in an Oracle WebLogic Environment

This section describes how to add an OpenPages application and workflow managed server to an existing IBM OpenPages GRC Platform installation running in an Oracle WebLogic environment.

Prerequisite

Before you begin the tasks described in this section, it is assumed that the `temp` directory created during the installation still exists as the scripts in that directory are mandatory.

Task Overview

The following tasks outline the process for adding a vertical cluster member:

- "Update Values in the OpenPages Property Files" on page 495
- "Update the Oracle WebLogic Administrator Password Value in the OpenPages Script Files" on page 496
- "Create the OpenPages Application Managed Server Instance" on page 497
- "Mask Passwords in the OpenPages Script Files" on page 498
- "Configure the IBPM Workflow Console" on page 498
- "Update Values in the Workflow Properties Files" on page 499
- "Update the Oracle WebLogic Administrator Password Value in the Workflow Script Files" on page 502
- "Create the Workflow Managed Server Instance" on page 503
- "Mask Passwords in the Workflow Script Files" on page 504
- "Update the Start/Stop Server Command Files" on page 504
- "Update the Unregister Services Command File and Restart Services" on page 506

Important: You must perform all of the tasks in this section for **each** managed server instance (OpenPages application/workflow server pair) that you want to add.

About Using Parameters in Tasks

The tasks described in this section require that you supply values for certain common parameters. You must enter these parameter values consistently across all of the tasks.

Example

Let's say a property or code statement requires the name of the machine on which you are adding the cluster member. That value is represented by the `<server_name>` parameter. If the name of the machine on which you are adding the cluster member is `OPHost`, then you must enter `OPHost` whenever you are asked to provide the value for `<server_name>`.

Important: The name of the server should **not** contain underscores (for example: OP_Host). Issues with connectivity between the Oracle Enterprise Manager and the Oracle WebLogic Server can occur.

These parameters are summarized in the following table.

Table 76. Parameters for Adding Cluster Members in Oracle WebLogic

Property	Description
`<drive>:<Workflow_Home_Path>`	The drive letter and installation path of the Fujitsu Interstage BPM server. **Default:** `C:\Fujitsu\InterstageBPM`
<admin_host_name>	The host name of the administrative server.
`<server_name>`	The host name of the machine on which you are adding the managed server instance. **Example** : `OPHost` **Important:** The name of the server should **not** contain underscores (for example: OP_Host). Issues with connectivity between the Oracle Enterprise Manager and the Oracle WebLogic Server can occur.
<server#>	The number of the managed server you are adding to the cluster. **Example** : If you currently have one managed server on `OP_Host`, this parameter value would be `2`.
<op_admin_port#>	The HTTP port number of the IBM OpenPages administrative server. **Example** : 7001 (Windows/ Oracle WebLogic), 9060 (AIX/IBM WebSphere).
<ibpm_admin_port#>	The HTTP port number of the workflow administrative server. **Example** : 49901 (Windows/Oracle WebLogic), 9061 (AIX/IBM WebSphere).
<new_OpenPages_http_port#>	The HTTP port number of the managed application server you are adding to the cluster. **Example** : If you currently have one managed application server on `OP_Host` with port number 7009, this parameter value would be `7011`.

Table 76. Parameters for Adding Cluster Members in Oracle WebLogic (continued)

Property	Description
<new_OpenPages_https_port#>	The HTTP secure port number of the managed application server you are adding to the cluster. **Example** : If you currently have one managed application server on `OP_Host` with secure port number 7010, this parameter value would be `7012`.
<new_IBPM_http_port#>	The HTTP port number of the managed workflow server you are adding to the cluster. **Example** : If you currently have one managed workflow server on `OP_Host` with port number 49951, this parameter value would be `49953`.
<new_IBPM_https_port#>	The HTTP secure port number of the managed workflow server you are adding to the cluster. **Example** : If you currently have one managed workflow server on `OP_Host` with secure port number 49952, this parameter value would be `49954`.
`<opworkflow_DB_username>`	The IBM OpenPages workflow user name for accessing the workflow database.
`<opworkflow_DB_password>`	The IBM OpenPages workflow password for accessing the workflow database.

Update Values in the OpenPages Property Files

Use the following instructions to modify and update values in these property files: `server.properties` and `sosa.properties` files.

Note: `<OP_Home>` in the file path represents the installation location of the OpenPages application. The default path for a Windows installation is `c:\OpenPages`.

Modify Values in the OpenPages Server Properties File (`server.properties`):

Update values in the `server.properties` file to specify the new server name and port.

Procedure

1. Log on to the application server where you are adding the new server as a user with administrative privileges. 2. Launch a Command Prompt window (using the Run as Administrator option).
2. Launch a Command Prompt window (using the **Run as Administrator** option).
3. Navigate to the `<OP_Home>\aurora\conf` directory and do the following.
   a. Create a copy of the following property file:
      `<server_name>`**- OpenPagesServer1-server.properties**
   b. Rename the copy of the file to:
      `<server_name>`**- OpenPagesServer** `<server#>` **-server.properties**
4. Open the renamed file in a text editor and do the following:
   a. Verify that the correct value for `<server_name>` is used throughout the file.
   b. Change all occurrences of port number 7009 to the HTTP port number of the OpenPages managed application server you are adding.

The port number for the new server should be two ports above the highest port value assigned to an IBM OpenPages server. For example, if OpenPagesServer2 is using port 7011, you should assign 7013 to the new server.

c. Update the parameter values for the following properties, where the new port number should be two ports above the highest port value assigned to the workflow server:
   - **workflow.client.props.path=** <drive>\:\\<Workflow_Home_Path>\\client\\server_name>-InterstageBPMCS<server#>-iFlowClient.properties
   - **url.path.workflow.admin=** http\://<server_name>\:<new_IBPM_http_port#>/ibpmconsole
   - **jms.topic.CacheTopic=** <server_name>-OpenPagesServer<server#>-CacheSyncPubTopic

d. When finished, save the file.

Modify Values in the Sosa Property File (sosa.properties):

Update values in the sosa.properties file to specify the new server name and port.

Procedure

1. In the <OP_Home>\aurora\conf directory, do the following:
   a. Create a copy of the following property file:
      <server_name> **-OpenPagesServer1-sosa.properties**
   b. Rename the copy of the file to:
      <server_name> **-OpenPagesServer** <server#> **-sosa.properties**
2. Open the renamed file in a text editor and update the parameter values for the following property:
   application.url.path= http\://<server_name>\:<new_OpenPages_http_port#>/openpages
3. When finished, save the file.

Update the Oracle WebLogic Administrator Password Value in the OpenPages Script Files

Use the following instructions to update the Oracle WebLogic password value in these script files: create_managed_server.bat, create_op_internal_jms_bridge.bat, and create_op_ibpm_jms_bridges_op.bat files.

Note:

- <OP_Home> in the file path represents the installation location of the OpenPages application. The default path for a Windows installation is c:\OpenPages.
- The password values that you type will be in plain text. After the member has been added to the cluster, you will have to manually mask these values with asterisks (***). For details, see "Mask Passwords in the OpenPages Script Files" on page 498.

Modify the Password Value in the create_managed_server.bat File:

Procedure

1. Navigate to the <OP_Home>\temp\scripts directory.
2. Open the create_managed_server.bat file in a text editor of your choice.

3. Update the Oracle WebLogic administrator password for the following line in the script:

   ```
   java weblogic.WLST <OP_Home>\temp\scripts\create_managed_server.py
   %ADMIN_SERVER_HOSTNAME%:<op_admin_port#>
   <weblogic_admin_username> <weblogic_admin_password> %SERVER_INSTANCE%
   <admin_host_name> %SERVER_INSTANCE_PORT% %SERVER_INSTANCE_SECURE_PORT%
   ```

   Where:

   <weblogic_admin_password> is the password of the Oracle WebLogic administrator account.

4. When finished, save the file.

Modify the Password Value in the create_op_internal_jms_bridge.bat File:

Procedure

1. In the <OP_Home>\temp\scripts directory, open the create_op_internal_jms_bridge.bat file in a text editor of your choice.
2. Update the Oracle WebLogic administrator password for the following line in the script:

   ```
   call <OP_Home>\temp\scripts\WLST.bat <OP_Home>\temp\scripts\
   create_internal_jms_bridge.py %ADMIN_SERVER_HOSTNAME%:<op_admin_port#>
   <weblogic_admin_username> <weblogic_admin_password> %SERVER_INSTANCE%
   <admin_host_name>
   %SERVER_INSTANCE_PORT%
   ```

   Where:

   <weblogic_admin_password> is the password of the Oracle WebLogic administrator account.

3. When finished, save the file.

Modify the Password Value in the create_op_ibpm_jms_bridges_op.batFile:

Procedure

1. In the <OP_Home>\temp\scripts directory, open the create_op_ibpm_jms_bridges_op.bat file in a text editor of your choice.
2. Update the Oracle WebLogic administrator password for the following line in the script:

   ```
   call <OP_Home>\temp\scripts\WLST.bat <OP_Home>\temp\scripts\
   create_op_ibpm_bridge.py
   %ADMIN_SERVER_HOSTNAME%:<op_admin_port#> <weblogic_admin_username>
   <weblogic_admin_password> %SERVER_INSTANCE% <admin_host_name>
   %SERVER_INSTANCE_PORT% %IBPM_INSTANCE_PORT%
   ```

   Where:

   <weblogic_admin_password> is the password of the Oracle WebLogic administrator account.

3. When finished, save the file.

Create the OpenPages Application Managed Server Instance

To create the new OpenPages application managed server instance, use the following steps.

Note: <OP_Home> in the file path represents the installation location of the OpenPages application. The default path for a Windows installation is c:\OpenPages.

Procedure

1. Start the OpenPagesAdminServer service.
2. At a Windows command prompt, navigate to the following directory:
   <OP_Home>\temp\scripts
3. From the \scripts directory, run the following .bat files with the updated values:
   a. **create_managed_server.bat** <server_name> **-OpenPagesServer** <server#> <new_OpenPages_http_port#> <new_OpenPages_https_port#>
   b. **create_op_internal_jms_bridge.bat** <server_name> **-OpenPagesServer** <server#> <new_OpenPages_http_port#> <new_OpenPages_https_port#>
   c. **create_op_ibpm_jms_bridges_op.bat** <server_name> **-OpenPagesServer** <server#> <new_OpenPages_http_port#> <new_OpenPages_https_port#> <new_IBPM_http_port#>
4. Navigate to the <OP_Home>\bin directory.
5. From the \bin directory, run the following command file to register the OpenPages services:
   RegisterOPWindowsServices.cmd <server_name> **-OpenPagesServer** <server#> **OpenPagesServer** <server#> **http://** <server_name>:<op_admin_port#>

Mask Passwords in the OpenPages Script Files

For security purposes, use the following steps to manually mask the plain text <weblogic_admin_password> that you entered in the OpenPages script files in "Update the Oracle WebLogic Administrator Password Value in the OpenPages Script Files" on page 496.

Note: <OP_Home> in the file path represents the installation location of the OpenPages application. The default path for an AIX installation is /opt/OpenPages.

Procedure

1. Navigate to the <OP_Home>\temp\scripts directory.
2. Open the following .bat files in a text editor:
   - create_managed_server.bat
   - create_op_internal_jms_bridge.bat
   - create_op_ibpm_jms_bridges_op.bat
3. For each .bat file, do the following.
   a. Locate the plain text password value for the <weblogic_admin_password> parameter in the file.
   b. Use asterisks (***) to overwrite the plain text password value for the <weblogic_admin_password> parameter.
   c. When finished, save the file.

Configure the IBPM Workflow Console

The create_ibpm_dirs.bat file creates the ibpmconsole directory under the <OP_Home> directory and extracts the contents of ibpmconsole.war into the ibpmconsole directory.

To update and run the .bat file, use the following steps.

Note: <Workflow_Home> in the file path represents the installation location of the Fujitsu Interstage BPM server. The default path for a Windows installation is c:\Fujitsu\InterstageBPM.

Procedure

1. Create the ibpmconsole directory within <OP_Home> as follows:
   a. Navigate to the <Workflow_Home>\server\deployment directory.
   b. Extract the contents of ibpmconsole.war to the <OP_Home>\ibpmconsole directory.
2. Navigate to the <OP_Home>\temp\scripts directory.
3. Open the create_ibpm_dirs.bat file in a text editor of your choice.
4. Modify the following '**set**' parameters in the file:
   a. Before changing the parameters, record the current values of the set count and set srvnum parameters.
   b. Change the current values to the following values:
      - **set count=** 1
      - **set srvnum=** <server#> (for example, set srvnum=2)
5. Save the changes to the file.
6. Run the create_ibpm_dirs.bat file.
7. Edit the create_ibpm_dirs.bat file to revert the changes made in step 6 to the original values, and save the file.

Update Values in the Workflow Properties Files

To update the ibpm.properties, iFlowClient.properties, console.conf, and server.properties files, use the following steps.

The create_ibpm_dirs.bat file creates a new deployment directory for the additional server, <Workflow_Home>\server\deployment\WLS-Cluster<server_name>-InterstageBPMCS<server#>.

Note: <Workflow_Home> in the file path represents the installation location of the Fujitsu Interstage BPM server. The default path for a Windows installation is c:\Fujitsu\InterstageBPM.

Copy the Required Files to New Directory:

The create_ibpm_dirs.bat file creates a deployment directory for the additional server under <Workflow_Home>.

Procedure

1. Navigate to the following directory: <Workflow_Home>\server\deployment\WLS-Cluster<server_name>-InterstageBPMCS1
2. Copy the following files to the new deployment directory:
   - ibpm.properties
   - importProperties.bat
   - setIBPMEnv.cmd

Modify Values in the IBPM Property File (ibpm.properties):

Update the ibpm.properties file in the new deployment directory with the name and port of the new workflow server instance.

Procedure

1. Navigate to the following directory:

<Workflow_Home>\server\deployment\WLS-Cluster<server_name>-InterstageBPMCS1

2. Copy the ibpm.properties file to:
   <Workflow_Home>\server\deployment\WLS-Cluster<server_name>-InterstageBPMCS<server#>
3. Open the copied file in a text editor and do the following:
   a. Update the parameter values for the following properties:
      - **ServerLogFile=** <drive>\:/<Workflow_Home_Path>/server/instance/default/logs/<server_name>-InterstageBPMCS<server#>.log
      - **NamingProviderURL=** t3\://<server_name>\:<new_IBPM_http_port#>
      - **ServerName=** <server_name>-InterstageBPMCS<server#>
      - **ServerBaseURL=** http\://<server_name>\:<new_IBPM_http_port#>/ibpmconsole/
      - **JMSNamingProviderURL=** t3\://<server_name>\:<new_IBPM_http_port#>
      - **ServerEmailBaseURL=** http\://<server_name>\:<new_IBPM_http_port#>/ibpmconsole/System/
   b. When finished, save the file.

Modify the Import Properties Batch File:

Procedure

1. Navigate to the following directory:
   <Workflow_Home>\server\deployment\WLS-Cluster<server_name>-InterstageBPMCS1
2. Copy the following files:
   - importProperties.bat
   - setIBPMEnv.cmd files

   into this directory:
   <Workflow_Home>\server\deployment\WLS-Cluster<server_name>-InterstageBPMCS<server#>
3. Open the copied setIBPMEnv.cmd file in a text editor and do the following:
   a. Update the parameter values for the following property:
      set SERVERNAME= <server_name> **-InterstageBPMCS** <server#>
   b. When finished, save the file.
4. Open the copied importProperties.bat file in a text editor and do the following:
   a. Update the parameter values on the following code line:
      call <Workflow_Home> **\server\deployment\WLS-Cluster** <server_name> **-InterstageBPMCS** <server#> **\setIBPMEnv.cmd**
   b. When finished, save the file.

Modify Values in the iFlow Client Property File (iFlowClient.properties):

Procedure

1. Navigate to the <Workflow_Home>\client directory and do the following:
   a. Create a copy of the following property file:
      <server_name> **-InterstageBPMCS1-iFlowClient.properties**
   b. Rename the copy of the file to:

<server_name> **-InterstageBPMCS** <server#> **-iFlowClient.properties**

2. Open the renamed file in a text editor and do the following:
   a. Update the parameter values for the following properties:
      - **JMSNamingProviderURL=** t3\://<server_name>\ :<new_IBPM_http_port#>
      - **NamingProviderURL=** t3\://<server_name>\:<new_IBPM_http_port#>
   b. When finished, save the file.

Modify Values in the IBPM Console Configuration File (`console.conf`):

Update the `console.conf` file in the new deployment directory with the name and port of the new workflow server instance.

Procedure

1. Navigate to the following directory:
   <Workflow_Home>\console_src\<server_name>-InterstageBPMCS1\ibpmconsole
2. Copy the `console.conf` file to:
   <Workflow_Home>\console_src\<server_name>-
   InterstageBPMCS<server#>\ibpmconsole
3. Open the `console.conf` file in a text editor and update the parameter value for the following property:
   NamingProviderURL= t3://<server_name>:<new_IBPM_http_port#>
4. When finished, save the file.

Modify Values in the Workflow IBPM Server Property File (`server.properties`):

Update the `server.properties` file..

Procedure

1. Navigate to the <OP_Home>\aurora\conf directory and do the following:
   a. Create a copy of the following property file:
      <server_name> **-InterstageBPMCS1-server.properties**
   b. Rename the copy of the file to:
      <server_name> **-InterstageBPMCS** <server#> **-server.properties**
2. Open the renamed file in a text editor and do the following:
   a. Update the parameter values for the following properties:
      - **workflow.client.props.path=** <drive>\:\\<Workflow_Home_Path>\\ InterstageBPM\\client\\ <server_name>-InterstageBPMCS<server#>-iFlowClient.properties
      - **jms.topic.CacheTopic=** <server_name>-InterstageBPMCS<server#>-CacheSyncPubTopic
   b. Change all occurrences of the following port numbers:
      - Replace 7009 with <new_OpenPages_http_port#>
      - Replace 49951 with <new_IBPM_http_port#>
   c. When finished, save the file.

Update the Oracle WebLogic Administrator Password Value in the Workflow Script Files

Use the following instructions to update the Oracle WebLogic password value in these script files: `create_ibpm_managed_server.bat`, `deploy_ibpm_console.bat`, `create_ibpm_internal_jms_bridge.bat`, and `create_op_ibpm_jms_bridges_ibpm.bat` files.

Note:

- `<OP_Home>` in the file path represents the installation location of the OpenPages application. The default path for a Windows installation is `c:\OpenPages`.
- The password values that you type will be in plain text. After the member has been added to the cluster, you will have to manually mask these values with asterisks (***). For details, see "Mask Passwords in the Workflow Script Files" on page 504.

Modify the Password Value in the `create_ibpm_managed_server.bat` File:

Procedure

1. Navigate to the `<OP_Home>\temp\scripts` directory.
2. Open the `create_ibpm_managed_server.bat` file in a text editor of your choice.
3. Update the Oracle WebLogic administrator password for the following line in the script:

   ```
   call <OP_Home>\temp\scripts\WLST.bat <OP_Home>\temp\scripts\
   create_ibpm_managed_server.py %SERVER_INSTANCE% %SERVER_INSTANCE_PORT%
   <Workflow_Home>\IBPMDomain IBPMDomain <weblogic_admin_username>
   <weblogic_admin_password> %ADMIN_SERVER_HOSTNAME% <ibpm_admin_port#> 1
   %SERVER_INSTANCE_SECURE_PORT%
   ```

   Where:

   `<weblogic_admin_password>` is the password of the Oracle WebLogic administrator account.
4. When finished, save the file.

Modify the Password Value in the `deploy_ibpm_console.bat` File:

Procedure

1. In the `<OP_Home>\temp\scripts` directory, open the `deploy_ibpm_console.bat` file in a text editor of your choice.
2. Update the Oracle WebLogic administrator password for the following line in the script:

   ```
   call <OP_Home>\temp\scripts\WLST.bat <OP_Home>\temp\scripts\
   deploy_ibpm_console_war.py %ADMIN_SERVER_HOSTNAME%:<ibpm_admin_port#>
   <weblogic_admin_username> <weblogic_admin_password> <Workflow_Home>
   %SERVER_INSTANCE%
   ```

   Where:

   `<weblogic_admin_password>` is the password of the Oracle WebLogic administrator account.
3. When finished, save the file.

Modify the Password Value in the `create_ibpm_internal_jms_bridge.bat` File:

Procedure

1. In the <OP_Home>\temp\scripts directory, open the create_ibpm_internal_jms_bridge.bat file in a text editor of your choice.
2. Update the Oracle WebLogic administrator password for the following line in the script:

   ```
   call <OP_Home>\temp\scripts\WLST.bat <OP_Home>\temp\scripts\
   create_internal_jms_bridge.py %ADMIN_SERVER_HOSTNAME%:<ibpm_admin_port#>
   <weblogic_admin_username> <weblogic_admin_password> %SERVER_INSTANCE%
   <server_name> %SERVER_INSTANCE_PORT%
   ```

   Where:

   <weblogic_admin_password> is the password of the Oracle WebLogic administrator account.
3. When finished, save the file.

Modify the Password Value in the create_op_ibpm_jms_bridges_ibpm.bat File:

Procedure

1. In the <OP_Home>\temp\scripts directory, open the create_op_ibpm_jms_bridges_ibpm.bat file in a text editor of your choice.
2. Update the Oracle WebLogic administrator password for the following line in the script:

   ```
   call <OP_Home>\temp\scripts\WLST.bat <OP_Home>\temp\scripts\
   create_op_ibpm_bridge.py %ADMIN_SERVER_HOSTNAME%:<ibpm_admin_port#>
   <weblogic_admin_username> <weblogic_admin_password> %SERVER_INSTANCE%
   <server_name> %SERVER_INSTANCE_PORT% %OP_INSTANCE_PORT%
   ```

   Where:

   <weblogic_admin_password> is the password of the Oracle WebLogic administrator account.
3. When finished, save the file.

Create the Workflow Managed Server Instance

To create the new workflow managed server instance, use the following steps.

Note:

- <OP_Home> in the file path represents the installation location of the OpenPages application. The default path for a Windows installation is c:\OpenPages.
- <Workflow_Home> in the file path represents the installation location of the Fujitsu Interstage BPM server. The default path for a Windows installation is c:\Fujitsu\InterstageBPM.

Procedure

1. Start the InterstageBPMAdminServer service.
2. At a Windows command prompt, navigate to the following directory:

   <OP_Home>\temp\scripts
3. From the \scripts directory, run the following .bat files with the updated values as follows:
   a. create_ibpm_managed_server.bat <server_name>-InterstageBPMCS<server#> <new_IBPM_http_port#> <new_IBPM_https_port#>
   b. deploy_ibpm_console.bat <server_name>-InterstageBPMCS<server#>
   c. create_ibpm_internal_jms_bridge.bat <server_name>-InterstageBPMCS<server#> <new_IBPM_http_port#> <new_IBPM_https_port#>

d. create_op_ibpm_jms_bridges_ibpm.bat <server_name>-InterstageBPMCS<server#> <new_IBPM_http_port#> <new_IBPM_https_port#> <new_OpenPages_http_port#>

4. Navigate to the <OP_Home>\bin directory.
5. From the \bin directory, run the following command file to register workflow services:

   RegisterIBPMWindowsServices.cmd <server_name>-InterstageBPMCS<server#> InterstageBPMCS<server#> http://<admin_host_name>:<ibpm_admin_port#>

6. Navigate to the <Workflow_Home>\server\deployment\WLS-Cluster<server_name>-InterstageBPMCS<server#> directory and run the following command file with the updated parameter values:

   importProperties.bat <Workflow_Home>\server\deployment\WLS-Cluster<server_name>-InterstageBPMCS<server#>\ibpm.properties <opworkflow_DB_username> <opworkflow_DB_password>

Mask Passwords in the Workflow Script Files

For security purposes, use the following steps to manually mask the plain text <weblogic_admin_password> that you entered in the workflow script files in "Update the Oracle WebLogic Administrator Password Value in the Workflow Script Files" on page 502.

Note: <OP_Home> in the file path represents the installation location of the OpenPages application. The default path for an AIX installation is /opt/OpenPages.

Procedure

1. Navigate to the <OP_Home>\temp\scripts directory.
2. Open the following .bat files in a text editor:
   - create_ibpm_managed_server.bat
   - deploy_ibpm_console.bat
   - create_ibpm_internal_jms_bridge.bat
   - create_op_ibpm_jms_bridges_ibpm.bat
3. For each .bat file, do the following.
   a. Locate the plain text password value for the <weblogic_admin_password> parameter in the file.
   b. Use asterisks (***) to overwrite the plain text password value for the <weblogic_admin_password> parameter.
4. When finished, save the file.

Update the Start/Stop Server Command Files

To add information about the new managed server instance to the start and stop server command files, use the following steps.

Modify the Start Server Command File:

Add the new IBM OpenPages and workflow servers to the start servers script.

Procedure

1. Navigate to the <OP_Home>\bin directory.
2. Open the StartAllServers.cmd file in a text editor.
3. After the block of start server code for the highest numbered OpenPagesServer# managed server instance in the file, do the following.
   a. Add the following lines of code:

```
sc start "OpenPagesServer<server#>"
call pauseForServerToStart.cmd %HOST_NAME% %OP_ADMIN_PORT%
<server_name>-OpenPagesServer<server#> %SERVER_CHECK_MAX_WAIT_COUNT%
if "%ERRORLEVEL%" NEQ "0" (
echo.
echo Unable to connect to OpenPages Managed server.
echo.
)
```

b. Update the parameter values in the lines that you added.

4. After the block of start server code for the highest numbered InterstageBPMCSServer# managed server instance in the file, do the following.
   a. Add the following lines of code:

```
sc start "InterstageBPMCS<server#>"
call pauseForServerToStart.cmd %HOST_NAME% %IBPM_ADMIN_PORT%
<server_name>-InterstageBPMCS<server#> %SERVER_CHECK_MAX_WAIT_COUNT%
if "%ERRORLEVEL%" NEQ "0" (
echo.
echo Unable to connect to IBPM Managed server.
echo.
)
```

   b. Update the parameter values in the lines that you added.
5. When finished, save the file.

Modify the Stop Server Command File:

Add the new IBM OpenOpenPages and workflow servers to the stop servers script.

Procedure

1. In the <OP_Home>\bin directory, open the StopAllServers.cmd file in a text editor.
2. Before the block of stop server code for the highest numbered OpenPagesServer# managed server instance in the file, do the following.
   a. Add the following lines of code:

```
sc stop "OpenPagesServer<server#>"
call pauseForServerToStop.cmd %HOST_NAME% %OP_ADMIN_PORT%
<server_name>-OpenPagesServer<server#> %SERVER_CHECK_MAX_WAIT_COUNT%
if "%ERRORLEVEL%" NEQ "0" (
echo.
echo Unable to shutdown OpenPages Managed server.
echo.
)
```

   b. Update the parameter values in the lines that you added.
3. Before the block of stop code for the highest numbered InterstageBPMCSServer# managed server instance in the file, do the following.
   a. Add the following lines of code:

```
sc stop "InterstageBPMCS<server#>"
call pauseForServerToStop.cmd %HOST_NAME% %IBPM_ADMIN_PORT%
<server_name>-InterstageBPMCS<server#> %SERVER_CHECK_MAX_WAIT_COUNT%
if "%ERRORLEVEL%" NEQ "0" (
echo.
```

```
echo Unable to shutdown IBPM Managed server.
echo.
)
```

b. Update the parameter values in the lines that you added.

4. When finished, save the file.

Update the Unregister Services Command File and Restart Services

To add information about the new managed server instance to the unregister Windows services command file, use the following steps.

Procedure

1. In the <OP_Home>\bin directory, open the UnRegisterAllServices.cmd file in a text editor.
2. Add the following line after the unregister code line for the highest numbered OpenPagesServer# managed server instance in the file:

   call UnRegisterOPWindowsServices.cmd "OpenPagesServer <server#> **"**

   Update the parameter in the line that you added.
3. Add the following line after the unregister code line for the highest numbered InterstageBPMCSServer# managed server instance in the file:

   call UnRegisterOPWindowsServices.cmd "InterstageBPMCS <server#> **"**

   Update the parameter in the line that you added.
4. Depending upon how many server instances simultaneously access the database, after adding a new server instance, you may need to increase the minimum number of connections to the Oracle database.

   Without enough database connections, you may receive errors, similar to:

   ```
   Listener refused the connection with the following error: ORA-12518,
   TNS:listener could not hand off client connection
   ```
5. Restart all services.

More Info: For details on starting services, see "Starting and Stopping OpenPages Application Servers" on page 465.

Adding Vertical Cluster Members to an Existing Installation in an IBM WebSphere Environment

This section describes how to add an OpenPages application and workflow managed server to an existing IBM OpenPages GRC Platform installation running in an IBM WebSphere environment.

Important: The IBM OpenPages GRC Platform requires a dedicated AIX LPAR and IBM WebSphere environment. Sharing the OpenPages LPAR with other applications and IBM WebSphere environments is not supported.

Prerequisite

Before you begin the tasks described in this section, it is assumed that the temp directory created during the installation still exists as the scripts in that directory are mandatory.

Task Overview

The following tasks outline the process for adding a vertical cluster member:

- "Create the OpenPages Application and Workflow Managed Server Instances" on page 508
- "Modify and Run the Workflow Scripts" on page 509
- "Update Values in Property Files" on page 510
- "Update the Start/Stop Server Scripts" on page 513
- "Mask Passwords in the Install Property File and Restart Services" on page 514

Important:

- You must perform all of the tasks in this section for **each** managed server instance (OpenPages application/workflow server pair) that you want to add.
- You must log on as the `opuser` to perform these tasks.

About Using Parameters in Tasks

The tasks described in this section require that you supply values for certain common parameters. You must enter these parameter values consistently across all of the tasks.

Example

Let's say a property or code statement requires the name of the machine on which you are adding the cluster member. That value is represented by the `<server_name>` parameter. If the name of the machine on which you are adding the cluster member is `aix_OP_Host`, then you must enter `aix_OP_Host` whenever you are asked to provide the value for `<server_name>`.

These parameters are summarized in the table below.

Table 77. Parameters for Adding Cluster Members in IBM WebSphere

Parameter	Description
<Workflow_Home>	The directory where Fujitsu Interstage BPM is installed. **Default**: `/opt/Fujitsu/InterstageBPM`
`<server_name>`	The host name of the machine on which you are adding the managed server instance. **Example**: `aix_OP_Host`
<server#>	The number of the managed server you are adding to the cluster. **Example**: If you currently have one managed server on `aix_OP_Host`, this parameter value would be 2.
<OpenPages_bootstrap_port#>	The value of the `BOOTSTRAP_ADDRESS` setting in the following property file: `<OP_Home>/temp/wasconfig/OpenPagesCell.<server_name>-OPNode1Server<server#>.config.props` **Example**: 10101

Table 77. Parameters for Adding Cluster Members in IBM WebSphere (continued)

Parameter	Description
<OpenPages_default_server_port#>	The value of the `WC_defaulthost` setting in the following property file: `<OP_Home>/temp/wasconfig/OpenPagesCell.<server_name>-OPNode1Server<server#>.config.props` **Example**: 10108
<IBPM_bootstrap_port#>	The value of the `BOOTSTRAP_ADDRESS` setting in the following property file: `<OP_Home>/temp/wasconfig/IBPMCell.<server_name>-IBPMNode<server#>Server.config.props` **Example**: 20101
<IBPM_default_server_port#>	The value of the `WC_defaulthost` setting in the following property file: `<OP_Home>/temp/wasconfig/IBPMCell.<server_name>-IBPMNode<server#>Server.config.props` **Example**: 20111
`<opadmin_WAS_username>`	If IBM WebSphere global security is configured, the IBM OpenPages administrator user name for accessing the IBM WebSphere Integrated Solutions Console.
`<opadmin_WAS_password>`	If IBM WebSphere global security is configured, the IBM OpenPages administrator password for accessing the IBM WebSphere Integrated Solutions Console. **Default:** `openpages`
`<opworkflow_DB_username>`	The IBM OpenPages workflow user name for accessing the workflow database.
`<opworkflow_DB_password>`	The IBM OpenPages workflow password for accessing the workflow database.

Create the OpenPages Application and Workflow Managed Server Instances

To create the new OpenPages application and workflow managed server instances, use the following steps.

Note: `<OP_Home>` in the file path represents the installation location of the OpenPages application. The default path for an AIX installation is `/opt/OpenPages`.

Procedure

1. Make sure that the following services are running:
   - `OpenPagesDmgr`
   - `OPNode1`
   - `IBPMDmgr`
2. Navigate to the `<OP_Home>/temp/perlinstall` directory.
3. Open the `install.properties` file in a text editor, and do the following.
   a. Type the password values for the following properties:

Note: The password values that you type will be in plain text. After all tasks are complete and the member has been added to the cluster, you will have to manually mask these values with asterisks (***). For details, see "Mask Passwords in the Install Property File and Restart Services" on page 514.

- **ADMIN_USERNAME=** <opadmin_WAS_username>

  Note: If IBM WebSphere global security is enabled, update accordingly. Otherwise, leave blank.
- **ADMIN_PASSWORD=** <opadmin_WAS_password>

  Note: If IBM WebSphere global security is enabled, update accordingly. Otherwise, leave blank.
- **OP_JDBC_PASSWORD=** <OpenPages_DB_User_Password>
- **IBPM_JDBC_PASSWORD=** <Workflow_DB_User_Password>

b. When finished, save the file.

4. At a shell prompt, run the following perl scripts in sequence with the updated values for these parameters:
   a. **perl addOPServer.pl** <server_name> **-OPNode1** <server_name>**- OPNode1Server** <server#>
   b. **perl createIBPMNode.pl** <server_name> **-IBPMNode** <server#>
   c. **perl addIBPMServer.pl** <server_name> **-IBPMNode** <server#> <server_name>**- IBPMNode** <server#> **Server** <server_name> **-OPNode1Server** <server#>
   d. **perl createIBPMJmsResourcesInOP.pl** <server_name>**- OPNode1Server** <server#> <server_name> **-IBPMNode** <server#> **Server**

Modify and Run the Workflow Scripts

This task provides instructions for modifying and running the createIBPMDirectories.sh and createIBPMPropertyFiles.sh scripts.

Note: <OP_Home> in the file path represents the installation location of the OpenPages application. The default path for an AIX installation is /opt/OpenPages.

Procedure

1. In the <OP_Home>/temp/perlinstall directory, open the following script files in a text editor of your choice:
   - createIBPMDirectories.sh
   - createIBPMPropertyFiles.sh
2. For each script file, make the following changes:
   a. Comment out the following while loop statements using the # sign, as shown:

      ```
      #while [ $COUNT -lt $NO_OF_SERVERS ]
      #do
      #done
      ```

   b. Change the expression count from +1 to the number of the member you are adding to the cluster:

      from this: **COUNT='expr $COUNT** + 1 **'**

      to this: **COUNT='expr** <server#> **'**
3. When finished, save the two script files.
4. At a shell prompt, run each script as follows:

a. `sh createIBPMDirectories.sh`
b. `sh createIBPMPropertyFiles.sh`

5. Edit the two scripts to revert the changes made in the second step to their original state and save the files.

Update Values in Property Files

Use the following instructions to modify and update values in these files: `server.properties`, `sosa.properties`, `ibpm.properties`, `iFlowClient.properties`, and `console.conf` files.

Note: `<OP_Home>` in the file path represents the installation location of the OpenPages application. The default path for an AIX installation is `/opt/OpenPages`.

Modify Values in the OpenPages Server Properties File (`server.properties`):

Procedure

1. Navigate to the `<OP_Home>/aurora/conf` directory and do the following.
   a. Create a copy of the following property file:
      `<server_name>` **-OPNode1Server1-server.properties**
   b. Rename the copy of the file to:
      `<server_name>` **-OPNode1Server** `<server#>` **-server.properties**
2. Open the renamed file in a text editor and do the following:
   a. Verify that the correct value for `<server_name>` is used throughout the file.
   b. Change all occurrences of the bootstrap port number for `OPNode1Server1` to the `<OpenPages_bootstrap_port#>` value of the new cluster member.

      Note: Bootstrap port numbers can be found in the following file:
      `<OP_Home>/temp/wasconfig/OpenPagesCell.<server_name>`
      `-OPNode1Server<server#>.config.props`
   c. Update the parameter values for the following properties:
      - **workflow.client.props.path=** `<Workflow_Home>/client/<server_name>-IBPMNode<server#>Server-iFlowClient.properties`
      - **url.path.openpages=** `http\://<server_name>\:<OpenPages_default_server_port#>/openpages`
      - **url.path.workflow.admin=** `http\://<server_name>\:<IBPM_default_server_port#>/ibpmconsole`
      - **webclient.http.server.port=** `<OpenPages_default_server_port#>`
   d. When finished, save the file.

Modify Values in the Sosa Property File (`sosa.properties`):

Procedure

1. In the `<OP_Home>/aurora/conf` directory, do the following:
   a. Create a copy of the following property file:
      `<server_name>` **-OPNode1Server1-sosa.properties**
   b. Rename the copy of the file to:
      `<server_name>` **-OPNode1Server** `<server#>` **-sosa.properties**
2. Open the renamed file in a text editor and update the parameter values for the following properties:
   - **openpages.service.port=** `<OpenPages_bootstrap_port#>`

- **application.url.path=** http\://<server_name>\
  :<OpenPages_default_server_port#>/openpages

3. When finished, save the file.

Modify Values in the Workflow IBPM Server Property File (server.properties):

Procedure

1. In the <OP_Home>/aurora/conf directory, do the following:
   a. Create a copy of the following property file:
      <server_name>**-IBPMNode1Server-server.properties**
   b. Rename the copy of the file to:
      <server_name>**-IBPMNode**<server#>**Server-server.properties**
2. Open the renamed file in a text editor and do the following:
   a. Change all occurrences of the workflow bootstrap port number for IBPMNode1Server to the <IBPM_bootstrap_port#> value of the new cluster member.

      Note: Bootstrap port numbers can be found in the following file:
      <OP_Home>/temp/wasconfig/IBPMCell.<server_name>
      -IBPMNode<server#>Server.config.props
   b. Update the parameter values for the following properties:
      - **jta.providerurl=** iiop\://<server_name>\:<IBPM_bootstrap_port#>
      - **jms.providerurl=** iiop\://<server_name>\:<IBPM_bootstrap_port#>
      - **workflow.client.props.path=** <Workflow_Home>/client/<server_name>
        -IBPMNode<server#>Server-iFlowClient.properties
      - **url.path.workflow.admin=** http\://<server_name>\
        :<IBPM_default_server_port#>/ibpmconsole
      - **url.path.openpages=** http\://<server_name>\
        :<OpenPages_default_server_port#>/openpages
      - **webclient.http.server.port=** <OpenPages_default_server_port#>
3. When finished, save the file.

Modify Values in the iFlow Client Property File (iFlowClient.properties):

Procedure

1. Navigate to the <Workflow_Home>/client directory and do the following:
   a. Create a copy of the following property file:
      <server_name>-IBPMNode1Server-iFlowClient.properties file
   b. Rename the copy of the file to:
      <server_name>-IBPMNode<server#>Server-iFlowClient.properties
2. Open the renamed file in a text editor and do the following:
   a. Change all occurrences of the workflow bootstrap port number for IBPMNode1Server to the <IBPM_bootstrap_port#> value of the new cluster member.

      Note: Bootstrap port numbers can be found in the following file:
      <OP_Home>/temp/wasconfig/IBPMCell.<server_name>
      -IBPMNode<server#>Server.config.props
   b. When finished, save the file.

Modify Values in the IBPM Console Configuration File (`console.conf`):

Procedure

1. Navigate to the following directory:
   ```
   <Workflow_Home>/profiles/<server_name>-IBPMNode1/installedApps/
   IBPMCell/fujitsu-console-ear.ear/ibpmconsole.war
   ```
2. Copy the `console.conf` file to the following directory:
   ```
   <Workflow_Home>/profiles/<server_name>-IBPMNode<server#>/installedApps/
   IBPMCell/fujitsu-console-ear.ear/ibpmconsole.war
   ```
3. Open the copied file in a text editor and update the parameter value for the following property:

   NamingProviderURL= `iiop://<server_name>:<IBPM_bootstrap_port#>`
4. When finished, save the file.

Modify Values in the IBPM Property File (`ibpm.properties`) and Run the Import Properties Script:

Procedure

1. Navigate to the following directory:
   ```
   <Workflow_Home>/server/deployment/WAS-Cluster<server_name>
   -IBPMNode<server#>Server
   ```
2. Open the `ibpm.properties` file in a text editor and do the following.
   a. Update the parameter values for the following properties:
      - **NamingProviderURL=** `iiop\://<server_name>\:<IBPM_bootstrap_port#>`
      - **JMSNamingProviderURL**`=iiop\://<server_name>\ :<IBPM_bootstrap_port#>`
      - **ServerHost**`=<server_name>`
      - **ServerLogFile**`=<Workflow_Home>/server/instance/default/logs/ <server_name>-IBPMNode<server#>Server.log`
      - **ServerInCluster**`=true`
      - **ServerBaseURL**`=http\://<server_name>\ :<IBPM_default_server_port#>/ibpmconsole/`
      - **ServerEmailBaseURL**`=http\://<server_name>\ :<IBPM_default_server_port#>/ibpmconsole/System/`

   b. If the following **ServerName** property:
      - Does not exist in the file, then add it to the end of the file.
      - Exists in the file, then update the parameter values.

        ServerName`=<server_name>-IBPMNode<server#>Server`

   c. When finished, save and close the file.
3. In the same directory, run the `importProperties.sh` script as follows:
   a. Open the `setIBPMenv.sh` file in a text editor.
   b. Replace the masked password in the `DATABASE_PASSWORD` parameter with the workflow database password.

      You need to replace the mask with clear text. The password has been automatically masked using asterisks (***) during the installation.
   c. Save the file.

Note: Before executing `importProperties.sh`, make sure that the user performing the installation has the permission to execute the script. If the user does not have the permission to execute `importProperties.sh`, enter the following command:

```
chmod 755 importProperties.sh
```

d. Run `./importProperties.sh`

e. Mask the password in the `DATABASE_PASSWORD` parameter with asterisks. For example, `DATABASE_PASSWORD=*****`

f. Save and close the `setIBPMenv.sh` file.

Note: If an error message for `logging.properties` displays while the script is running, it is not significant and can be ignored.

Run Patch Scripts to Update Server Configuration:

To update the new cluster member with the updated configuration on the OpenPages and workflow servers, run the `updateOPPatch.pl` and `updateIBPMPatch.pl` perl scripts as follows.

Procedure

1. Navigate to the following directory:

   `<OP_Home>/temp/perlinstall`
2. In the `<OP_Home>/bin` directory, open the `updateOPPatch.pl` script in a text editor.
3. Change the `$DMGR_HOST= value` to the name of the application server.

   Example: `$DMGR_HOST="aix_OP_Host"`
4. Save and close the file.
5. At a shell prompt, run the `updateOPPatch.pl` perl script on a single line to update the OpenPages server as follows:

   ```
   perl updateOPPatch.pl <server_name>-OPNode1
   <server_name>-OPNode1Server<server#>
   ```
6. Open the `updateIBPMPatch.pl` script in a text editor.
7. Change the `$DMGR_HOST= value` to the name of the application server.
8. Save and close the file.
9. At a shell prompt, run the `updateIBPMPatch.pl` script on a single line to update the workflow server as follows:

   ```
   perl updateIBPMPatch.pl <server_name>-IBPMNode<server#>
   <server_name>-IBPMNode<server#>Server
   ```

Update the Start/Stop Server Scripts

To add information about the new managed server instance to the start and stop server scripts, use the following steps.

Modify the Start Server Script:

Procedure

1. Navigate to the `<OP_Home>/bin` directory.
2. Open the `startAllServers.sh` script in a text editor.
3. After the line of `startServer.sh` code for the highest numbered OPNode1Server# managed server instance in the file, do the following.

   a. Add the following line of code:

```
$WAS_HOME/bin/startServer.sh <server_name>-OPNode1Server<server#>
```

b. Update the parameter values in the line that you added.

4. After the block of start server code for the highest numbered IBPMNode# managed server instance in the file, do the following.
   a. Add the following lines of code:

```
. $IBPM_PROFILES_HOME/<server_name>-
IBPMNode<server#>/bin/setupCmdLine.sh
# Starting the node
$WAS_HOME/bin/startNode.sh
# Starting all the server specified
$WAS_HOME/bin/startServer.sh <server_name>-IBPMNode<server#>Server
```

   b. Update the parameter values in the lines that you added.
5. When finished, save the file.

Modify the Stop Server Script:

Procedure

1. In the <OP_Home>/bin directory, open the stopAllServers.sh script in a text editor.
2. Before the line of stopServer.sh code for the highest numbered OPNode1Server# managed server instance in the file, do the following.
   a. Add the following line of code:

```
$WAS_HOME/bin/stopServer.sh <server_name>-OPNode1Server<server#>
```

   b. Update the parameter values in the line that you added.
3. Before the block of stop server code for the highest numbered IBPMNode# managed server instance in the file, do the following.
   a. Add the following lines of code:

```
. $IBPM_PROFILES_HOME/<server_name>-
IBPMNode<server#>/bin/setupCmdLine.sh
# Stopping the node
$WAS_HOME/bin/stopNode.sh
# Stopping all the server specified
$WAS_HOME/bin/stopServer.sh <server_name>-IBPMNode<server#>Server
```

   b. Update the parameter values in the lines that you added.
4. When finished, save the file.

Mask Passwords in the Install Property File and Restart Services

For security purposes, use the following steps to manually mask the plain text passwords that you entered in the install.properties files from task "Create the OpenPages Application and Workflow Managed Server Instances" on page 508.

Note: <OP_Home> in the file path represents the installation location of the OpenPages application. The default path for an AIX installation is /opt/OpenPages.

Procedure

1. Navigate to the <OP_Home>/temp/perlinstall directory.
2. Open the install.properties file in a text editor, and do the following.
   a. Use asterisks (***) to overwrite the plain text password values for the following properties. The overwritten password values will look similar to the following:
      - **ADMIN_PASSWORD=** *****

- **OP_JDBC_PASSWORD= *****
- **IBPM_JDBC_PASSWORD= *****

b. When finished, save the file.

3. Depending upon how many server instances need to simultaneously access the database, you may need to increase the minimum number of connections to the database. If you do not have enough database connections, you will receive errors when starting the servers.
4. Restart all services.

More Info: For details on starting services, see "Starting and Stopping OpenPages Application Servers" on page 465.

Adding Members to a Horizontal Cluster

This section describes how to add a new OpenPages application and workflow non-administrative managed server to an existing IBM OpenPages GRC Platform installation in a horizontal clustered environment.

Important: If installing onto a Windows server, the name of the server should not contain underscores (for example: OpenPages_Application). Issues with connectivity between the Oracle Enterprise Manager and the Oracle WebLogic Server can occur.

Procedure

1. Install IBM OpenPages GRC Platform on the machine you want to add as a member to your horizontal cluster.
2. If you are adding the non-administrative server for the first time, make sure you configure the domain account and share the network OpenPages storage directory.

   Important: The installation path must be the same on the admin server and on all managed servers.

   Example:

   Windows: `c:\OpenPages`

   AIX: `/opt/OpenPages`
3. Depending on your environment, follow the instructions in one of the following topics to add a non-administrative server to a second or third machine in your horizontal clustered environment:
   - "Adding Vertical Cluster Members to an Existing Installation in an Oracle WebLogic Environment" on page 493
   - "Adding Vertical Cluster Members to an Existing Installation in an IBM WebSphere Environment" on page 506

More Info

For more information on configuring domain accounts and the IBM OpenPages storage directory, see the section on "Configuring a Clustered OpenPages Environment" in the *IBM OpenPages GRC Platform Installation Guide* .

Chapter 19. Using the ObjectManager Tool

This chapter highlights the most commonly used features of the ObjectManager tool. For information about ObjectManager usage not covered in this chapter, contact your IBM representative for details.

This chapter contains the following topics:

About the ObjectManager Tool

The ObjectManager tool provides a command line interface (CLI) - rather than the application graphical user interface - to load data into the IBM OpenPages repository. With the ObjectManager tool, you can:

- Import (load) data into the IBM OpenPages repository, such as object and/or configuration data.
- Export (dump) filtered or unfiltered data from the IBM OpenPages repository. You can use exported data, for example, to migrate environments and data from one machine to another in a multi-deployment environment.
- Batch load multiple loader files in a single session.

Working With Loader Files

Understanding Loader File Naming Conventions

The ObjectManager tool uses XML loader files to load (import) or dump (export or extract) data into IBM OpenPages . The loader file name consists of a prefix, which is defined by the user, and a standard string that has the following format:

`<loader-file-prefix>-op-config.xml`

Where:

`<loader-file-prefix>` is the user-defined portion of the loader file name.

`-op-config.xml` is the standard string that follows the prefix and identifies the file as a loader file to the ObjectManager tool. Do not change this portion of the file name.

Note:

- When you pass a loader file parameter to the ObjectManager tool, you only pass the prefix portion of the loader file name.

- If no prefix is provided, the ObjectManager tool will attempt to load from or write to the file `op-config.xml`.

Import Example

If you want to load (import) data into the IBM OpenPages repository, you could, for example, create a loader file with the name 'mydata`-op-config.xml'` (prefix + standard string). When you pass the prefix '`mydata`' to the ObjectManager tool, the ObjectManager tool would automatically look for a loader file named 'mydata`-op-config.xml'`.

Export Example

If you want to extract (dump) data from IBM OpenPages , you could, for example, pass the prefix 'myconfig' to the ObjectManager tool. The ObjectManager tool would automatically create an export (dump) file named myconfig`-op-config.xml`.

Creating a Data Loader File

A data loader file is an XML file that contains the data you want to import or load through the ObjectManager into your system. You can use any XML or text editor of your choice to create a data loader file.

After you create the data loader file, you would save it using the file naming convention described in "Understanding Loader File Naming Conventions" on page 517.

All element tags in a data loader file are nested within the root element <openpagesConfiguration xmlFormatVersion="1.30"> and </openpagesConfiguration> tags.

An ObjectManager data loader file has the following structure:

```
<?xml version="1.0" encoding="UTF-8"?>
<openpagesConfiguration xmlFormatVersion="1.30">
      <parent-element>
          <child-element/>
          <child-element/>
      </parent-element>
</openpagesConfiguration>
```

Where:

`parent-element` is a tag identifying the type of information to be loaded.

`child-element` is a nested tag within a given information type that usually contains attributes and/or text content.

Example:

The following code example shows the structure of an XML data loader file that, when loaded through the ObjectManager tool, would update the currency exchange rates for the Canadian dollar (CAD), Mexican peso (MXN), and Hong Kong (HKD) dollar.

The exchangeRates element contains the exchangeRate child-element, which has attributes for the 3-letter country ISO code and the updated exchange rate for that currency.

```
<?xml version="1.0" encoding="UTF-8"?>
<openpagesConfiguration xmlFormatVersion="1.30">
   <exchangeRates>
      <exchangeRate isoCode="CAD"
                    rate="0.8636"/>
      <exchangeRate isoCode="MXN"
                    rate="0.0951"/>
      <exchangeRate isoCode="HKD"
                    rate="0.1289"/>
   </exchangeRates>
</openpagesConfiguration>
```

Running ObjectManager Commands

About the ObjectManager Command File

The ObjectManager command file is named as follows:

Windows `ObjectManager.cmd`
AIX `ObjectManager.sh`

The file is located in the `<OP_Home>|bin` directory of your IBM OpenPages installation.

Where: `<OP_Home>` represents the installation location of the IBM OpenPages GRC Platform application. By default, this is:	
Windows	`C:\OpenPages`
AIX	`/opt/OpenPages`

The ObjectManager command line must be:

- Run from the `bin` folder
- Typed on a single line (no line breaks) in a command window.

Important: When using the ObjectManager tool, make sure that the IBM OpenPages GRC Platform application services are running.

ObjectManager Command Line Parameters

Table 78 lists the various commands and parameters you can use with the ObjectManager tool.

Table 78. ObjectManager Command Line Parameters

Parameter	Value	Description
`<command>`	Can be one of the following:	Required.
	• `dump` or `d`	Dumps or exports data.
	• `load` or `l`	Loads or imports data from a single loader file.
	• `verify` or `v`	Verifies or compares data.
`<batch-mode>`	`batch` or `b`	Places ObjectManager in batch processing mode loads multiple loader files in a single session.

Table 78. ObjectManager Command Line Parameters (continued)

Parameter	Value	Description
<user>		Required. A user account. Some actions may require a Super Administrator account.
<password>		Required. User account password.
<loader-file-path>	By default, this is the current directory if no file path is specified.	Optional. The file path to a single XML loader file.
<batch-loader-dir>		Optional. The directory path to the XML loader files that are listed in the <batch-loader-list-file>. Can be a top-level directory if loader files are in multiple sub-folders under that directory.
<loader-file-prefix>	By default, the ObjectManager tool will attempt to load from or write to the file op-config.xml. if no prefix is specified.	Optional. The user-defined portion of the loader file name.
<batch-loader-list-file>		Required. The fully qualified file path and name of a text document containing a list of loader files for batch processing.

Interactive Command Line Loader File Syntax

The ObjectManager tool uses the following syntax for a loader file. See Table 78 on page 519 for a description of the various commands and parameters.

Note: Make sure to run the command on a single line in the Command Prompt window.

```
ObjectManager <command> config|c <user> <password>
<loader-file-path> <loader-file-prefix>
```

Load Command Example

The instructions in the following Windows-based example show how to use a loader file named 'data1-op-config.xml' that resides in the c:\import folder to load or import data into IBM OpenPages . This example uses the Super Administrator account, 'OpenPagesAdministrator'.

Procedure

1. Open a Command Prompt window.
2. Navigate to the bin installation directory, such as:
   ```
   cd C:\OpenPages\bin
   ```
3. Run the following command on a single line to load the data1-op-config.xml loader file:

Results

```
ObjectManager l c OpenPagesAdministrator OpenPagesAdministrator c:\import data1
```

Dump Command Example

The instructions in the following Windows-based example show how to export or dump data from IBM OpenPages to a file with the prefix 'config1' that resides in

the c:\export folder. If the folder does not already exist, the ObjectManager tool will create it. This example uses the Super Administrator account, 'OpenPagesAdministrator'.

Procedure

1. Open a Command Prompt window.
2. Navigate to the bin installation directory, such as:
   ```
   cd C:\OpenPages\bin
   ```
3. Run the following command on a single line to export data from IBM OpenPages into the 'config1-op-config.xml' loader file:

Results

```
ObjectManager d c OpenPagesAdministrator OpenPagesAdministrator c:\export config1
```

The file named 'config1-op-config.xml'will automatically be created in the c:\export folder.

Batch Mode Loader File Syntax

The ObjectManager tool uses the following syntax for batch loading multiple loader files. See Table 78 on page 519 for a description of the various commands and parameters.

```
ObjectManager <batch-mode> config|c <user> <password>
<batch-loader-dir> <batch-loader-list-file>
```

Sample Batch Loader List File

A batch loader list file is typically a text (.txt) file that contains a list of the XML loader files for batch processing by the ObjectManager tool.

A batch loader list file uses the following rules:

- Any line starting with a pound sign (#) is considered a comment
- Any line starting with greater than sign (>) is written to the screen for display
- All other lines are assumed to be the relative path to a loader file

The following sample batch loader list file was created in a text editor. It shows how to display an informational "loading" message (line starting with >) on the screen for files that are loading from different directories, and provides an example of how to list a loader file (example1-op-config.xml) from a top-level (c:\temp) directory and how to list multiple loader files (example2, example3, example4) from a subfolder (\loaders) located under the top-level directory.

```
# If the <batch-loader-dir> was given as c:\temp, the following lines
would
# write the "Loading..." message and then attempt to load the file
# c:\temp\example1-op-config.xml
>Loading example 1...
example1

# If the <batch-loader-dir> was given as c:\temp, the following lines
would
# write the "Loading..." message and then attempt to load the files:
# c:\temp\loaders\example2-op-config.xml
# c:\temp\loaders\example3-op-config.xml
# c:\temp\loaders\example4-op-config.xml
```

```
>Loading examples 2-4...
loaders\example2
loaders\example3
loaders\example4
```

Example

Let's say we save the above batch loader list file with the name 'load-reports.txt' in the c:\OpenPages default installation directory.

The instructions in the following example show how to run the sample 'load-reports.txt' batch loader list file to load or import data into IBM OpenPages . The top-level directory (c:\temp) is used for the <batch-loader-dir> parameter as it includes the loader files in the \loaders subfolder under it.

Procedure

1. Open a Command Prompt window.
2. Navigate to the bin installation directory, such as:
   ```
   cd C:\OpenPages\bin
   ```
3. Run the following batch command to load the 'load-reports.txt' batch loader list file:
   ```
   ObjectManager b c OpenPagesAdministrator OpenPagesAdministrator
    c:\temp load-reports.txt
   ```

Modifying the ObjectManager Properties File

The ObjectManager.properties file contains a number of settings that can control or limit the scope of exported (dumped) configuration and related data from the ObjectManager tool.

Depending on your export activity, you may be required to modify the value of some or all configuration or migration settings.

Note:

- Before you modify the ObjectManager.properties file, make a backup copy of the file.
- You can open and edit the ObjectManager.properties file in any text editor to modify values.

To determine which specific settings in the file may require modification, refer to the following topics in this chapter:

- "Exporting All Currency Exchange Rates" on page 524
- "Exporting Currency Field Definitions" on page 526
- "Exporting Computed Field Definitions" on page 527
- "Migrating Configuration Changes Using the ObjectManager Tool" on page 527

The ObjectManager.properties file is located in the <OP_Home>|bin directory of your IBM OpenPages installation.

Where: <OP_Home> represents the installation location of the IBM OpenPages GRC Platform application. By default, this is:	
Windows	C:\OpenPages
AIX	/opt/OpenPages

Managing Currency Exchange Rates

This section contains information on XML elements that you can use in ObjectManager loader files to update, export, and enable or disable currency exchange rates.

Note: To use these functions, the currency must have a standard 3-letter ISO code and exist in your system.

About Updating Currency Exchange Rates

There are several methods for updating currency exchange rates. You can:

- Upload a CSV file with currency exchange rates from:
  - The IBM OpenPages application user interface. "Uploading a CSV File - User Interface Procedure" on page 119
  - An ObjectManager loader file. "Importing Exchange Rates"
- Manually edit the rates in the IBM OpenPages application user interface. "Editing Exchange Rates for an Existing Currency Code - User Interface Procedure" on page 118
- Upload currency exchange rates in an ObjectManager loader file. "Importing Exchange Rates"

Importing Exchange Rates

You can use a data loader file to import exchange rates for existing currency codes by specifying the new rates in the file or by uploading a properly formatted CSV file with the new rates.

Note: For CSV file format information, see "Formatting a CSV File for Upload" on page 118.

Procedure

1. Create an XML data loader file (see "Creating a Data Loader File" on page 518).
2. To load exchange rate data:
   - If the exchange rate data is specified in a loader file - use the element tags in the following example and substitute the values of the attributes listed in the table:

Element	Attribute	Description
exchangeRate	isoCode	A 3-letter ISO currency code
	rate	The currency exchange rate

Example

The following example loads currency exchange rates for the Canadian dollar (CAD), Mexican peso (MXN), and Hong Kong (HKD) dollar.

```
<exchangeRates>
    <exchangeRate isoCode="CAD"
                  rate="0.8636"/>
    <exchangeRate isoCode="MXN"
                  rate="0.0951"/>
    <exchangeRate isoCode="HKD"
                  rate="0.1289"/>
</exchangeRates>
```

- If the exchange rate data is contained in a CSV file for upload - use the element tag in the following example to upload a .csv file and substitute the value of the attribute listed in the table:

Element	Attribute	Description
uploadFile	name	The file path and name of the CSV file

Example

```
<uploadFile name = "c:loaders\rate-update1.csv"
        dataType = "Exchange Rates" />
```

3. Use the ObjectManager `load` command to import the data. See the "Load Command Example" on page 520.

Exporting All Currency Exchange Rates

To export (dump) all the currency exchange rates from your system, you must modify some of the settings in the `ObjectManager.properties` file (for information about the file, see "Modifying the ObjectManager Properties File" on page 522).

Procedure

1. In the `ObjectManager.properties` file:
   a. Set the values of the following properties as shown:

```
configuration.manager.migrate.configuration.objects=false
configuration.manager.dump.currency.exchange.rates=true
```

   a. Set the dump options for all other objects to `false`.
2. Use the ObjectManager `dump` command to export the data. See the "Dump Command Example" on page 520.

Enabling and Disabling Currencies

You can enable one or more currency to make it available to the appropriate processes, or you can disable one or more currencies from the IBM OpenPages application. A disabled currency can be enabled at a later time.

Procedure

1. Create an XML data loader file (see "Creating a Data Loader File" on page 518).
2. To enable or disable one or more currencies, use the element tags in the following example and substitute the values of the attributes listed in the table:

Element	Attribute	Description
`currency`	isoCode	A 3-letter ISO currency code
	enabled	If you set the value to: • `true` - the currency is enabled • `false` - the currency is disabled

Example

The following example enables Euros and disables United Kingdom pounds.

```
<currencies>
   <currency isoCode="EUR"
             enabled="true"/>
   <currency isoCode="BBP"
             enabled="false"/>
</currencies>
```

3. Use the ObjectManager `load` command to import the data. See the "Load Command Example" on page 520.

Importing and Exporting Currency Field Definitions

This section describes how you can import or export field definitions for currency data types.

Importing Currency Field Definitions

Procedure

1. Create an XML data loader file (see "Creating a Data Loader File" on page 518).
2. To import currency field definitions, use the element tags in the following example and substitute the values of the attributes listed in the table:

Element	Attribute	Description
`bundleType`	`name`	The name of a field group
	`description`	A brief description of the field group
`propertyType`	`name`	The name of a currency field within the specified field group
	`description`	A brief description of the currency field
	`required`	If you set the value to: • `true` - the field is required • `false` - the field is not required
	`multiValued`	If you set the value to: • `true` - multiple values can be selected from the list • `false` - only one value can be selected from the list

Example

The following example loads the definition for the currency field 'testCurrency' that belongs to a group of the same name.

```
<bundleTypes>
    <bundleType name="testCurrency"
        description="Sarbanes-Oxley Self-Assessment system bundle"
               type="Content Type">
       <propertyType name="testCurrency"
               description="Annualized Value may be used to capture the account
balance from operational systems."
              dataType="Currency"
              minValue=""
              maxValue=""
          defaultValue=""
              required="false"
          currencyCode=""
           multiValued="false">
      </propertyType>
   </bundleType>
</bundleTypes>
```

3. Use the ObjectManager `load` command to import the data. See the "Load Command Example" on page 520.

Exporting Currency Field Definitions

To export (dump) currency field definitions from your system, you must modify some of the settings in the `ObjectManager.properties` file (for information about the file, see "Modifying the ObjectManager Properties File" on page 522).

Procedure

1. In the `ObjectManager.properties` file:
   a. Set the values of the following properties as shown:

   ```
   configuration.manager.migrate.configuration.objects=false
   configuration.manager.dump.bundle.types=true
   ```

   a. Set the dump options for all other objects to `false`.
2. Use the ObjectManager `dump` command to export the data. See the "Dump Command Example" on page 520.

Importing and Exporting Computed Field Definitions

This section describes how you can import or export computed field definitions.

Importing Computed Field Definitions

Note: For additional information on computed fields, see "Defining a Computed Field" on page 124.

Procedure

1. Create an XML data loader file (see "Creating a Data Loader File" on page 518).
2. To import computed field definitions, use the element tags in the following example and substitute the values of the attributes listed in the table:

Element	Attribute	Description
`computationHandler`	`name`	Do not change. A field definition attribute of the computed field.
	`value`	A value that corresponds to a particular field definition attribute.

Example

The following example loads the definition of a computed field.

```
<computationHandler name="CognosComputationHandler">
    <computationHandlerAttribute name="Equation"
                                 value="count(distinct
[DEFAULT].[SOXTEST].[TE_TEST_ID])"/>
    <computationHandlerAttribute name="Namespace"
                                 value="DEFAULT"/>
    <computationHandlerAttribute name="Object ID Column"
         value="Just some text"/>
           <computationHandlerAttribute name="Reporting Period ID
Column"
        value="Value for testing"/>
</computationHandler>
```

3. Use the ObjectManager `load` command to import the data. See the "Load Command Example" on page 520.

Exporting Computed Field Definitions

To export (dump) computed field definitions from your system, you must modify some of the settings in the `ObjectManager.properties` file (for information about the file, see "Modifying the ObjectManager Properties File" on page 522).

Procedure

1. In the `ObjectManager.properties` file:
   a. Set the values of the following properties as shown:

      ```
      configuration.manager.migrate.configuration.objects=false
      configuration.manager.dump.computed.field.definitions=true
      ```

   a. Set the dump options for all other objects to `false`.
2. Use the ObjectManager `dump` command to export the data. See the "Dump Command Example" on page 520.

Migrating Configuration Changes Using the ObjectManager Tool

You can use the ObjectManager tool to migrate configuration changes from one deployment environment to another.

About Multi-deployment Environments

If you have a multi-deployment environment where changes to the IBM OpenPages application are tested and validated prior to implementation, you can use ObjectManager, a command line interface (CLI) tool, to migrate configuration changes from one deployment environment to another.

Multi-deployment environments may vary from company to company. For example, a multi-deployment environment for "Company 1" may contain the following deployments:

- Development Deployment - configuration changes are made to the user interface and tested to validate that the changes are applied correctly. The IBM OpenPages repository used in this deployment may contain fewer objects (partial instance data) than the "Production" deployment.
- Test Deployment - configuration changes from the "Development" configuration are imported (to avoid error) and validated through the ObjectManager tool and tested. The IBM OpenPages repository used in this deployment generally mirrors the instance data in the "Production" deployment.
- Production Deployment - The tested configuration changes from the "Test" configuration are imported (to avoid error) and validated through the ObjectManager tool, and then made available to end users ("Live Production").

"Company 2" may, for example, combine "Development" and "Test" into a single "Test" deployment before migrating configuration changes to a "Production" environment.

About the Migration Process

Using the ObjectManager tool, you can migrate configuration changes from one deployment to another for the following objects:

- Field Groups
- Object Types
- Filters
- Field Dependencies

- Dependent Picklists
- Object Type Relationships
- Profiles
- Application Text
- Object Text
- Settings (excludes machine specific settings in the IBM OpenPages repository)

To limit the scope of the changes to the above listed configuration objects, you can edit settings in the ObjectManager.properties file. For details, see “Modifying ObjectManager Settings” on page 529.

Table 79 outlines the process you would follow if you were to migrate configuration changes, for example, from a "Test" deployment to a "Production" deployment environment.

Note: If you have a multi-deployment environment that also includes a "Development" system, you can use the tasks outlined in Table 79 to do an initial export of the configuration data from the "Development" system to the "Test" deployment system.

Table 79. Tasks for Migrating Configuration Changes

Task	Use this deployment...	To do this task...	Related Topic...
1	Test	Modify settings in the ObjectManager.properties file to limit the scope of the export data to only configuration objects.	See “Modifying ObjectManager Settings” on page 529 for step-by-step setup instructions before you export configuration data.
2	Test	Export the configuration changes into a file.	See “Exporting Configuration Changes” on page 531 for step-by-step instructions on how to export configuration metadata.
3	Production	Compare the configuration changes from the previous deployment (in Task 2) against this deployment.	See “Verifying Configuration Changes” on page 531 for step-by-step instructions on how to verify configuration changes.
4	Production	Import the configuration changes (from Task 3) into the current deployment.	See “Importing Configuration Changes” on page 533 for step-by-step instructions on how to update configuration changes.
5	Production	To verify that all the updates were applied, compare the configuration changes from the previous deployment (in Task 2) against the newly updated deployment.	See “Verifying Configuration Changes” on page 531 for step-by-step instructions on how to verify configuration changes.

Modifying ObjectManager Settings

Before you begin migrating configuration object changes from one deployment to another, you can use the ObjectManager tool to include only configuration objects in the migration process and exclude additional object data, such as Resource or Job Type data, from the migration metadata and changes.

Limiting the Export of Changes to Configuration Objects

By default, the ability to export metadata changes is set to include all objects. So that you can export changes made only to configuration objects, you must modify some of the settings in the `ObjectManager.properties` file.

To enable only the export of changes for configuration objects, follow these steps.

Procedure

1. In a text editor of your choice, open the ObjectManager.properties file (see "About the ObjectManager Command File" on page 519).
2. Navigate to the following setting in the file:

   ```
   configuration.manager.migrate.configuration.objects=false
   ```
3. Change the value of this setting from `false` (default) to `true` (export only configuration object changes) as follows:

   ```
   configuration.manager.migrate.configuration.objects=true
   ```
4. When finished, save your changes to the file.
5. If you want to modify IBM OpenPages repository settings that are excluded, by default, from the migration process, follow the instructions in "Modifying Excluded Settings From Export (Optional)."

Modifying Excluded Settings From Export (Optional)

If the value of some IBM OpenPages repository settings were changed to reflect a particular deployment environment, you can, if wanted, exclude these settings from migrating to the next deployment environment. For example, if the address of the Notification Mail Server differs from the "Development" machine to the "Test" machine, you can exclude this setting from the export of configuration metadata and changes.

You can optionally exclude settings from export by modifying the ObjectManager.properties file. A statement that excludes a setting from export has the following syntax:

```
configuration.manager.migrate.configuration.exclude.registry.entry.<n>=<setting>
```

Where:

`<n>` is a sequential number.

`<setting>` is the full path and name of the setting you want to exclude.

By default, the IBM OpenPages platform excludes the following configuration settings from the export process. These settings are listed by number in the order in which they appear in the ObjectManager.properties file along with their full path and name.

```
1=/OpenPages/Applications/Common/Email/Mail Server
2=/OpenPages/Platform/Application Server Guest Password
3=/OpenPages/Platform/Publishing/Mail/From Address
4=/OpenPages/Platform/Publishing/Mail/Host
5=/OpenPages/Platform/Publishing/Mail/Username
```

```
6=/OpenPages/Platform/Reporting Schema/Object URL Generator/Host
7=/OpenPages/Platform/Reporting Schema/Object URL Generator/Port
8=/OpenPages/Platform/Workflow/Email/Mail From
9=/OpenPages/Platform/Workflow/Email/Mail Server
```

You can, if wanted, add additional settings to the list for exclusion or remove an existing setting from the list to include it in the export.

Procedure

1. Open the ObjectManager.properties file (see "Modifying the ObjectManager Properties File" on page 522).
2. Locate the following setting in the file - you will use this setting as the basis for creating additional settings for exclusion:

   configuration.manager.migrate.configuration.exclude.registry.entry.1=/OpenPages/Applications/Common/Email/Mail Server
3. To exclude additional settings from export, copy the line of code in Step 2 and do the following:
   a. Paste the code at the end of the list (for example, after '9').
   b. Increment the number (for example, '10').
   c. Specify a full setting path and name.

      For example (do not wrap - use a single line):

      ```
      configuration.manager.migrate.configuration.exclude.registry.entry.10=/OpenPages/Platform/Reporting Schema/Object URL Generator/Populate Past Periods
      ```
4. To export a configuration setting that is on the excluded list, remove the line of code for that setting from the list.
5. When finished, save your changes to the properties file.
6. To apply the changes, stop and then restart the Oracle WebLogic service (OpenPagesAdminServer).

Disabling Triggers When Migrating Environments

When extracting and restoring environments using Object Manager, you may need to disable any triggers that are checking data validity.

This setting is normally applied automatically, but you can disable triggers if the need arises.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages** | **Applications** | **GRCM** folder hierarchy.
3. Click the **Disable Triggers** setting to open its detail page.
4. In the **Value** field, type `true`.
5. Click **Save**.

Results

All triggers in the system are disabled.

Migrating Configuration Changes

After you modify setting in the ObjectManager.properties file, you can begin the migration process. Migrating configuration changes from one environment to another involves exporting, verifying, and importing the changes.

Exporting Configuration Changes

Exported data represents a snapshot of the configuration objects in the IBM OpenPages repository for a particular deployment. When you export configuration changes, you specify a file path and prefix for the file name in the command line. When the data is exported, the ObjectManager tool automatically appends *-op-config.xml* to the file name prefix to complete the file name.

For example, if you were to specify the myconfig prefix in the command line for the file name, it would result in this file name: `myconfig-op-config.xml`.

Procedure

1. Verify that the IBM OpenPages application is running.
2. Open a command or shell window and change to the `<OP_Home>|bin` directory of your IBM OpenPages GRC Platform installation.
3. From the command or shell window, run the following ObjectManager command on a single line:

   Windows ObjectManager dump config < admin-user > < password > < config-folder-path > < prefix >

   AIX ObjectManager.sh dump config < admin-user > < password > < config-folder-path > < prefix >

   Where:

   < admin-user > is the user name of the Super Administrator account (for example, OpenPagesAdministrator).

   < password > is the password of the Super Administrator account.

   < config-folder-path > is the file path to the folder where the exported file will reside. If the folder does not already exist, the ObjectManager will create it.

   < prefix > is the prefix for the file name that will be used by the ObjectManager.

   Example (Windows) `ObjectManager dump config OpenPagesAdministrator OpenPagesAdministrator c:\temp myconfig`
4. To compare the exported configuration data against the configuration data in the IBM OpenPages repository of the next deployment environment, see "Verifying Configuration Changes."

Verifying Configuration Changes

After you export or import configuration changes, you can compare the exported data file from the previous deployment environment against the data in the IBM OpenPages repository of the current deployment environment.

When you run the verify command using the ObjectManager:

- The results are displayed on the screen during the verification process. If you want to review the results at a later time, you can re-direct the screen output to a file.
- An ObjectManager.log file containing exception errors is automatically created. This log file is located in the selected root installation folder. By default, this is the c:\OpenPages folder.

Procedure

1. Copy the exported configuration file from the previous deployment environment (for example, "Development") to a folder in the current deployment environment (for example, "Production").

2. From the <OP_Home>|bin directory of your IBM OpenPages GRC Platform installation, open a command or shell window.
3. From the command or shell window, run the following ObjectManager command on a single line (optionally re-direct the output to a file):

   Windows ObjectManager verify config < admin-user > < password > < config-export-folder-path > < prefix >

   AIX ObjectManager.sh verify config < admin-user > < password > < config-export-folder-path > < prefix >

   Where:

   < admin-user > is the user name of the Super Administrator account (for example, OpenPagesAdministrator).

   < password > is the password of the Super Administrator account.

   < config-export-folder-path > is the file path to the folder where the export file (from the previous deployment) resides.

   < prefix > is the prefix of the export file name.

   Example (Windows) The command in the following example compares configuration data in the export file 'myconfig-op-config.xml' located in the c:\temp folder to configuration data in the OPX Repository on the current deployment, and re-directs the display output (from a Windows server) to a text file called 'config_log.txt' also located in the c:\temp folder:

   ```
   ObjectManager verify config OpenPagesAdministrator
   OpenPagesAdministrator c:\temp myconfig >c:\temp\config_log.txt
   ```
4. Review the output for any validation and verification errors (see the sample output following these steps for more information).
5. To import the configuration changes and update the IBM OpenPages repository of the current deployment environment with these changes, see the topic "Importing Configuration Changes" on page 533.
6. To verify that the updated IBM OpenPages repository of the current deployment matches the configuration changes from the export file, repeat Steps 2-4.

Results

Generally, validation errors indicate a problem with the data itself and should be corrected before importing the configuration changes into the next deployment. The following sample validation error shows the "name" field in the export file as having an empty value.

```
VALIDATION ERROR (Line: 104481 Column: 57): Attribute 'name' is either
empty or not provided.
```

Generally, verification errors indicate differences in the content of the configuration data between the export file and the IBM OpenPages repository. The following sample verification error shows a discrepancy in the display label text for the Control Method object field between the export file of the previous deployment ("Control Method") and the IBM OpenPages repository of the current deployment ("Implementation Method").

```
VERIFICATION ERROR (Line: 104873 Column: 52): Attribute 'singularValue' for
element 'fieldString'(Control Method) did not verify. XML Value: <Control
Method> OPX Platform Value: <Implementation Method>.
```

When the processing is complete, a summary of the configuration objects that were processed displays.

Once the IBM OpenPages repository is updated with the configuration changes from the export file and the validation process is repeated, the data in the export file and IBM OpenPages repository should match and no errors should be displayed.

Importing Configuration Changes

After comparing and verifying the configuration metadata and changes, you can, if wanted, migrate the changes to the current deployment environment or system. When you import the configuration changes from the previous deployment, the configuration objects in the IBM OpenPages repository of the current deployment are upgraded with those changes.

Procedure

1. Verify that the IBM OpenPages application is running.
2. Open a command or shell window and change to the `<OP_Home>|bin` directory of your IBM OpenPages GRC Platform installation.
3. From the command or shell window, run the following ObjectManager command on a single line:

   Windows ObjectManager load config < admin-user > < password > < config-folder-path > < prefix >

   AIX ObjectManager.sh load config < admin-user > < password > < config-folder-path > < prefix >

   Where:

   < admin-user > is the user name of the Super Administrator account (for example, OpenPagesAdministrator).

   < password > is the password of the Super Administrator account.

   < config-folder-path > is the file path to the folder where the exported file will reside. If the folder does not already exist, the ObjectManager will create it.

   < prefix > is the prefix for the file name that will be used by the ObjectManager.

   Example (Windows) `ObjectManager load config OpenPagesAdministrator OpenPagesAdministrator c:\temp myconfig`
4. To see the configuration changes in the application, stop and then restart the IBM OpenPages application service (OpenPagesAdminServer).
5. To verify that the newly updated IBM OpenPages repository matches the configuration changes from the export file, see the topic "Verifying Configuration Changes" on page 531.
6. To export the configuration data to a file, see the topic "Exporting Configuration Changes" on page 531.

Chapter 20. Managing Workflows

Interstage Business Process Manager 10.1 (referred to as Interstage BPM in this guide) is a third-party application used to develop, manage, and remediate workflow processes within the IBM OpenPages GRC Platform application environment.

The Interstage BPM application is composed of the following components:

- **Interstage BPM Studio** — A Windows-based standalone tool used to design and integrate workflow processes for use within the IBM OpenPages GRC Platform application.
- **Interstage BPM Console** — A browser-based tool used to remediate running workflow process instances (jobs).
- **Interstage BPM Server** — The run-time environment workflow engine (referred to in this chapter as the IBM OpenPages GRC Platform workflow server).

This chapter describes various workflow-related administrative functions in IBM OpenPages , use of the Job Launch Manager to start batch jobs from the command line, job remediation using Interstage BPM Console, and workflow troubleshooting.

Note: For information on how to use Interstage BPM Studio to create process definitions and publish them for use in workflows in the IBM OpenPages application, see the *IBM OpenPages 6.1.0 Workflow Authors Guide.*

This chapter contains the following topics:

Starting Jobs from Objects

The IBM OpenPages application allows users with the correct privileges to:

- Start jobs that are associated with IBM OpenPages objects
- Monitor the progress of jobs

Starting a Job from an IBM OpenPages Object

To start a job from an object in the IBM OpenPages application, you must first associate the process definition with an IBM OpenPages object type in Interstage BPM Studio. If you have not created this association, you will not be able to select the job correctly in the IBM OpenPages application once it is published. For more information on this topic, see "Associating a Process Definition With an Object Type" in the IBM *OpenPages 6.1.0 Workflow Authors Guide*.

For a description of how to start a job from an object in OpenPages, see the *IBM OpenPages 6.1.0 Help*.

Monitoring Job Progress

You can keep track of the activity that has occurred for a job through the My Jobs list on your IBM OpenPages Home page, if My Jobs is configured for display on the Classic tab. Each job is shown with its name, description, the object it is attached to, and the currently active task. For instructions on how to configure the My Jobs list for display on the Home page, see "Configuring Predefined Lists" on page 188.

Alternatively, users with administrative privileges can view job status, progress, and many other job-related properties from the Jobs page. For a description of information on the Jobs page and how to access it, see "Managing Jobs."

Managing Jobs

The IBM OpenPages application allows administrative users with the correct permissions to view the status of all current and past jobs that have been run on the IBM OpenPages system.

Accessing the Jobs Page

To access the Jobs page, do the following.

Procedure

1. Log on to the IBM OpenPages application as a user with the **Collaboration** application permission. The user must also belong to the `WorkflowAdministrators` group to view jobs.
2. From the **Administration** menu, select **Jobs**.

About the Jobs Page

On the Jobs page, you can use various selection criteria in the Filters table to filter the list of displayed jobs. The jobs that fit the criteria display in the Jobs table.

Table 80 describes the columns in the Jobs table.

Table 80. Jobs Table Column Descriptions

Column	Description
Name	The name of the job.
Description	The description of the job.
Attachments	Links to the object type(s) associated with the job.
Current Task	The task that is currently active and assigned to a user.
Owner	The list of users that are defined as Job Owners for the current job.
Start Date	The date and time the job was started.

Table 80. Jobs Table Column Descriptions (continued)

Column	Description
Status	The status of the current job. Possible statuses are: • **Starting** — Job is being initialized during startup. This is a transient state. • **Running** — Job is active. • **Suspended** — Job is waiting for a child process to complete (for example, when a subprocess node starts a child job). • **Error** — Job is in an error state (exception was thrown). • **Terminated** — Job is terminated by the user. • **Completed** — Job has completed (has reached the Exit node).

Filtering Jobs

To filter the list of jobs displayed in the Jobs table, do the following.

Procedure

1. Access the Jobs page (see "Accessing the Jobs Page" on page 536).
2. To filter the list of jobs displayed in the Jobs table, do the following.
   a. In the Filters table, select any combination of the following criteria:

Table 81. Job Filters Table Criteria

Criteria Type	Behavior
Owner	Limits the displayed jobs to only those jobs that are owned by the selected user. **Note:** Filter is not currently supported for groups, only for users.
Start Date	Limits the displayed jobs to only those jobs that were started between the selected dates.
Status	Limits the displayed jobs to only those jobs that are currently in the selected state(s). Possible statuses are: • **Starting** — Job is being initialized during startup. This is a transient state. • **Running** — Job is active. • **Suspended** — Job is waiting for a child process to complete (for example, when a subprocess node starts a child job). • **Error** — Job is in an error state (exception was thrown). • **Terminated** — Job is terminated by the user. • **Completed** — Job has completed (has reached the Exit node). **Note:** **Ctrl**-click an entry in the status list to select more than one status.

   For example, you can choose to display only 'Terminated' jobs that belong to the owner 'GMartin.'
   b. When finished, click **Search** to update the Jobs table with the jobs that match the criteria.
   c. If the job list is large, click the icon at the bottom of the page to view the next group of jobs.
3. To view the detail page of a job, click the name of the job in the Jobs table.

Terminating Jobs

To terminate a running job, do the following.

Procedure

1. Access the Jobs page (see "Accessing the Jobs Page" on page 536).
2. If the job to be terminated is not listed, use the filter criteria to search for the job.
3. Once the job is displayed, click the name of the job in the list to open its detail page.
4. On the **Job Details** table of the selected job, click **Terminate**.
5. On the Terminate this Job page:
   a. Navigate to the **Add a Comment** table.
   b. In the **Comment** field, type a comment.
   c. When finished, click **Terminate**.

Managing Tasks

The IBM OpenPages application allows administrative users with the correct permissions to view the status of all current and previous tasks that have been run on the IBM OpenPages system.

Accessing the Tasks Page

Procedure

1. Log on to the IBM OpenPages application interface as a user with the **Collaboration** application permission.
2. From the **Administration** menu, select **Tasks**.

About the Tasks Page

On the Tasks page, you can use various selection criteria in the Filters table to filter the list of displayed tasks. The tasks that fit the criteria display in the Tasks table.

Table 82 describes the columns in the Tasks table.

Table 82. Tasks Table Column Descriptions

Column	Description
Status	The status of the current tasks. Possible statuses are: • **New** — Task assigned, not yet accepted. • **Accepted** — Task assigned, and accepted by assignee. • **Declined** — Task assigned, but declined by assignee. • **Waiting for SubJob** — Parent job of the task is waiting for child job to complete. • **Voted** — Vote has been submitted for task. Applies only to Voting tasks. • **Suspended** — Assigned task has been suspended due to an error state (typically in another branch of the job).
Name	The name of the task.
Description	The description of the task.

Table 82. Tasks Table Column Descriptions (continued)

Column	Description
Attachments	A comma-separated list of all the attachments currently attached to the task. The first entry in the list is always the name of the object type that the task's job is associated with.
Job Name	The name of the job to which the task belongs.
Assignee	The list of user names that the task is assigned to (or could potentially be assigned to). If the task has not been accepted yet, all potential assignees are shown.
Start Date	The date and time the job was started.

Filtering Tasks

To filter the list of tasks displayed in the Tasks table, do the following.

Procedure

1. Access the Tasks page (see "Accessing the Tasks Page" on page 538).
2. To filter the list of tasks displayed in the Tasks table, do the following.
   a. In the Filters table, select any combination of the following criteria:

Table 83. Task Filters Table Criteria

Criteria Type	Behavior
Assignees	Limits the displayed tasks to only tasks that are assigned to the selected user. **Note:** Filter is not currently supported for groups, only for users.
Start Date	Limits the displayed tasks to only tasks that were started between the selected dates. **Note:** When filtering on start date, reassigned tasks will display (or not) based on their original start date, not the reassigned start date. The task will still display a start date that reflects the date it was reassigned.
Status	Limits the displayed tasks to only the tasks that are currently in the selected state(s). Possible statuses are: • **New** — Task assigned, not yet accepted. • **Accepted** — Task assigned, and accepted by assignee. • **Declined** — Task assigned, but declined by assignee. • **Waiting for SubJob** — Parent job of the task is waiting for child job to complete. • **Voted** — Vote has been submitted for task. Applies only to Voting tasks. • **Suspended** — Assigned task has been suspended due to an error state (typically in another branch of the job). **Note:** **Ctrl**-click an entry in the status list to select more than one status.

   For example, you can choose to display only 'Accepted' tasks that belong to the user 'OCard.'
   b. When finished, click **Search** to update the list with the tasks that match the criteria.
   c. If the task listing is large, click the icon at the bottom of the page to view the next group of tasks.

3. To view the detail page of a task, click the name of a task in the Tasks table.

Reassigning a Task

Note: You cannot reassign a Voting task.

If you want to reassign an active task from the Tasks page, do the following.

Procedure

1. Access the Tasks page (see "Accessing the Tasks Page" on page 538).
2. If the task to be reassigned is not listed, use the filter criteria to search for the task.
3. Once the task is displayed:
   a. Select the check box next to the name of the task in the list.
   b. Click **Reassign** on the **Task Details** table.
4. On the **Reassign** table:
   a. Click the selector icon to choose a user or group to be the new assignee.
   b. In the **Comment** box, enter a comment.
   c. When finished, click **Reassign**.

Managing Job and Task Attachments

To manually add, associate, disassociate, or delete an attachment (such as a file or link) to a running job or task, do the following.

Procedure

1. Depending on your activity, do one of the following. To access the:
   - Jobs page (see "Accessing the Jobs Page" on page 536), or
   - Tasks page (see "Accessing the Tasks Page" on page 538).
2. If the job or task you want is not listed, use the filter criteria to search for the job or task.
3. Once the job or task is displayed, click the name of the job or task in the list to open its detail page.
4. On the detail page of the selected job or task, navigate to the **Attachments** table.
5. On the **Attachments** table, do one of the following:

If you want to...	Then, do this...
add a file	1. Click **Add File**. 2. On the Adding File page, select the file you want to upload and click **Create**.
add a link	1. Click **Add Link**. 2. On the Adding Link page, provide a name and URL, and click **Create**.

If you want to...	Then, do this...
associate a file or form	1. Click **Associate**. 2. On the Files and Forms page, select the box next to the file or form you want to associate. **Note:** You may need to expand a folder to access the file or form. 3. Click **Associate**.
disassociate a file or link	1. Click the box next to the file or link you want to disassociate. 2. Click **Disassociate**. 3. At the confirmation prompt, click **OK**.
delete	1. Click the box next to the file or link you want to delete. 2. Click **Delete**. 3. At the confirmation prompt, click **OK**. **Note:** If the file or link is already attached to at least one other job or task, an error message displays and you will be unable to delete the file or link.

Managing IBM OpenPages Workflow Groups

To create, edit, or delete projects or process definitions in Interstage BPM Studio, a user must have administrative privileges.

In addition, to perform object type associations and publish workflows to OpenPages from Interstage BPM Studio, the user must be a member of the `WorkflowAdministrators` group. Any user who needs to view all jobs in OpenPages must also be included in the `WorkflowAdministrators` group.

Note: A special-purpose group named `WorkflowHierarchicalJobOwners` is used by the workflow component of the IBM OpenPages application to support creation and use of hierarchical jobs in workflows. This group is intended for internal use only.

Important: Do not add users to the `WorkflowHierarchicalJobOwners` group, as this will cause the hierarchical jobs workflow function to fail.

Deploying a Business Calendar on the Workflow Server

If workflow authors will be using a custom business calendar when defining due dates or timers in a process definition, you must add the business calendar to a specific directory location on the IBM OpenPages workflow server.

Note: For more information on using business calendars, see the "Creating Your Own Business Calendars" section in the IBM *OpenPages 6.1.0 Workflow Authors Guide*.

To deploy a business calendar on the server, use the following steps.

Procedure

1. Locate the business calendar on the Windows system where Interstage BPM Studio is installed. The default path is `C:\IBPMStudio\InterstageBPM_studio\workspace\<application-project-name>\<business_calendar_name>.cal`.
2. Do the following on the workflow server (or on each workflow server instance, if this is a cluster):
   a. Log on to the IBM OpenPages workflow server as a user with administrative privileges.
   b. Copy the business calendar from the Windows system to the following directory location on the server:

      Windows

      `<drive>:<Workflow_Home>\server\instance\default\calendar`

      AIX

      `<Workflow_Home>/server/instance/default/calendar`
   c. Stop and then restart all services on the workflow server.

      Note: For information on how to stop and start services on workflow (Fujitsu Interstage BPM) servers, see "Starting and Stopping OpenPages Application Servers" on page 465.

Configuring Custom E-mail for Workflows

When a workflow is launched, standard (out-of-the-box) automated e-mails and task messages are created for the user. The mail server settings available in the IBM OpenPages application user interface are used to send remediation e-mails and standard task messages from a workflow to users or groups (see "Configuring a Mail Server for Workflow" on page 323). These default automated e-mails and messaging are generally sufficient for most workflow configurations.

If you want to configure custom e-mail from a specific mail server or disable the standard e-mail messages that are auto-generated from a task, you can use the procedures described in this section.

Note: You can only configure custom e-mail for workflows after the IBM OpenPages installation is completed.

Setting Up a Custom E-Mail Server

Use the Interstage BPM Configuration tool to designate a specific custom e-mail server for workflow-related e-mails and task messages.

Procedure

1. Start the Interstage BPM Configuration Tool in a web browser with the following URL:

   `http://<server_name>:<port>/fujitsu-ibpm-config-webapp/IBPMConfigServlet`

   where `<server_name>` is the host name of your IBM OpenPages application server and `<port>` is the port number of the managed server in your workflow server configuration. For Windows, the managed server port numbers for the workflow server typically start at 49951; for AIX, 9081.
2. Log on to the configuration tool as a user with administrative privileges.
3. Enter values in the following fields:

In this field...	Enter this value...
SMTPPassword	The password for your SMTP mail server (only required if your mail server requires password authentication).
SMTPServerHost	The fully qualified domain name of your SMTP mail server. For example, `myserver01.mydomain.com`.
SMTPServerPort	The port number of your SMTP mail server. For example, `25`.
SMTPUserName	The user login name for your SMTP mail server (only required if your mail server requires user authentication).
ServerEmailAddress	The "From" (sender) e-mail address for the custom e-mails. For example, `sysadmin@mycompany.com`.

4. To save the changes, click **Save and Reload properties**. The new mail server settings take effect immediately (no IBM OpenPages application server restart is required).
5. If you have more than one managed server in your workflow server configuration, repeat the previous steps for each managed server. Use the unique port number assigned to each managed server in the URL.

Disabling Standard Task E-mails

By default, sending auto-generated e-mail messages from a task is enabled. To disable all auto-generated e-mail messages from tasks, follow the steps below.

Procedure

1. Start the Interstage BPM Configuration Tool in a web browser with the following URL:

   `http://<server_name>:<port>/fujitsu-ibpm-config-webapp/IBPMConfigServlet`

   where `<server_name>` is the host name of your IBM OpenPages application server and `<port>` is the port number of the managed server in your workflow server configuration. For Windows, the managed server port numbers for the workflow server typically start at 49951; for AIX, 9081.
2. Log on to the configuration tool as a user with administrative privileges.
3. In the **EmailNotificationEnabled** field, change the value to **false**.
4. To save the changes, click **Save and Reload properties**. The new mail server settings take effect immediately (no IBM OpenPages application server restart is required).
5. If you have more than one managed server in your workflow server configuration, repeat the previous steps for each managed server. Use the unique port number assigned to each managed server in the URL.

Using the Job Launch Manager

IBM OpenPages includes a command line tool that allows workflow administrators to batch start jobs from existing process definitions based on a property value or other criteria. The Job Launch Manager must be run from a command line on the IBM OpenPages application server.

Only one set of jobs can be launched from a single execution of the Job Launch Manager; that is, all of the jobs created as a result of the execution of the tool will share the same process definition, same job name, same resource selection criteria, and so on. To specify multiple criteria or multiple process definitions, you must run the Job Launch Manager multiple times and use a different configuration file for each set of settings.

Users can specify options for the tool by providing a pointer to a predefined configuration file.

When you run the Job Launch Manager, you must specify a user name that has **Start Jobs** permission.

When the Job Launch Manager is started, it performs the following tasks:

Procedure

1. Reads in the command line arguments.
2. Validates that all necessary input has been provided at the command line.
3. Logs in with the specified user name and password.
4. Loads the specified configuration file.
5. Validates that all necessary input has been provided in the configuration file.
6. Retrieves the specified process definition.
7. Reads the object content type and object filter criteria (if any exist).
8. Validates that the process definition is associated with the specified content type.
9. Retrieves all objects that match the content type and filter criteria.
10. Validates that all job properties specified in the configuration file exist for the specified process definition. If any of the specified job properties do not exist for the process definition, they are ignored.

Results

For each resource that meets the specified criteria, the Job Launch Manager then:

- Creates a new job based on the resource and process definition properties.
- Sets the specified system and custom property values for the new job.
- Starts the new job.

About the Job Launch Manager Command File

The Job Launch Manager command file is named as follows:

Windows JobLaunchManager.cmd
AIX JobLaunchManager.sh

The file is located in the <OP_Home>|bin directory of your IBM OpenPages installation.

Where: <OP_Home> represents the installation location of the IBM OpenPages GRC Platform application. By default, this is:	
Windows	C:\OpenPages
AIX	/opt/OpenPages

The following section details the allowable parameters that can be used with the Job Launch Manager command line interface.

Job Launch Manager Syntax

Windows

```
JobLaunchManager.cmd -Username <name> -Password <password>
-ConfigurationFile <path-to-config-file> [-LogSession true|false]
[-Verbose true|false][-Host <hostname> [-Port <port>]]
```

AIX

```
./JobLaunchManager.sh -Username <name> -Password <password>
-ConfigurationFile <path-to-config-file> [-LogSession true|false]
[-Verbose true|false][-Host <hostname> [-Port <port>]]
```

Table 84 lists the parameters for the JobLaunchManager command.

Table 84. JobLaunchManager Parameters

Parameter	Description
Username	Required. The user account that is used to retrieve the resources and start the jobs.
Password	Required. The plaintext password for the `Username` parameter.
ConfigurationFile	Required. The full path to the configuration file that contains the settings required to filter the resources and start the jobs. The JobLaunchManager configuration file is explained in detail in "Configuring the Job Launch Manager" on page 546.

LogSession	A boolean parameter that controls whether the output of the command is written to a log file.
	
	By default, this parameter is set to `true` and the output is automatically written to the following log file:
	
	`<OP_Home>|aurora|logs|OpenPagesServer1`
	
	`-JobLaunchManager.log`
	
	Where: `<OP_Home>` represents the installation location of the IBM OpenPages application. By default, this is:
	
	Windows `C:\OpenPages`
	
	AIX `/opt/OpenPages`

Verbose	A boolean parameter that controls whether the output of the command is written to the command window. If this parameter is not specified, the output is written to the command window by default.
Host	The machine host name for the IBM OpenPages application server. If this parameter is not specified, the host name from the appropriate properties file in IBM OpenPages is used by default.
Port	The port number for the service instance port (Windows) or the bootstrap port for the OpenPages server instance (AIX). If this parameter is not specified, the port from the appropriate properties file in IBM OpenPages is used by default.

Configuring the Job Launch Manager

The Job Launch Manager requires a plain text configuration file that contains the properties required to batch start jobs. You can use any name for the configuration file, although a `.txt` file extension is recommended.

Each property is listed in a `property=value` syntax, as follows:

```
jobtype_name=ExcellentJob
job_name=A Really Clever Name
...
```

Table 85 lists the properties for the JobLaunchManager configuration file.

Table 85. Job Launch Manager Configuration File Properties

Property	Description
`jobtype_name`	The name of the process definition that is used to create jobs for the resources that fit the criteria.
`job_name`	The name that is assigned to all jobs created from this command. If this property is not specified, the process definition name is used as the job name.
`job_description`	The description that will be assigned to all jobs created from this command. If this property is not specified, the job description is empty.
`job_duedate`	The due date for the jobs, in the format `mm/dd/yyyy`. If this property is not specified, no due date is assigned to the job.
`job_owner`	The name of the user or group that is assigned as the job owner for all jobs started from this command. If this property is not specified, the process definition owner is assigned as the job owner.
`job_priority`	The priority level that is assigned to the jobs created from this command. Valid values are `High`, `Medium`, and `Low`. If this property is not specified or a value is invalid, all jobs are assigned `Medium` priority.
`job_doc_attachments`	A comma-separated list of the full repository paths for any documents that are assigned to all jobs created from this command. **Example**: `job_doc_attachments=/_op_sox/Project/Default/Issue/Sample Process issue.txt, ./_op_sox_documents/Files and Forms/Procedures/Budget/ReportNarrative.doc`

Table 85. Job Launch Manager Configuration File Properties (continued)

Property	Description

`job_property_name_<N>`
 	
`job_property_value_<N>`
	The `job_property_name_<N>` property is used with the `job_property_value_<N>` property to specify the name and value for an existing process definition custom property.
	
	You can specify multiple custom properties. `<N>` starts at 1 and is incremented by 1 for each successive name-value pair that you define.
	
	Example: If a process definition property named NumberOfDaysRemaining has a default value of 365 and another property named Destination has a value of Unknown, the Job Launch Manager can override these default settings by providing new custom values in the configuration file, as follows:
	`job_property_name_1=NumberOfDaysRemaining`
	`job_property_value_1=100`
	`job_property_name_2=Destination`
	`job_property_value_2=Earth`
	
	When the Job Launch Manager is started, the NumberOfDaysRemaining property value is changed from 365 to 100. Likewise, the Destination property value is changed from Unknown to Earth.
	Note: The name of the custom property must match the name of an existing process definition custom property exactly.

`parent_object_name`	The name of the parent object that is used as the scoping object for the job launch operation. Only resources under the parent object that match this property are considered as candidates for starting new jobs. If this property is not specified, all resources in the repository are considered as job start candidates.
`parent_object_content_type`	The content type of the scoping parent object. This property is required if `parent_object_name` is used.
`content_type`	The content type of the objects that are used to launch jobs. If this property is not specified, a single job instance is launched, and it will not be associated with an object type.

Table 85. Job Launch Manager Configuration File Properties (continued)

Property	Description

`object_property_name_<N>`
 	
`object_property_value_<N>`
 	
`object_operator_<N>`
	These three properties are used in combination to set up the filtering criteria for the resources that are used to start jobs.
	
	You can specify multiple filtering criteria. `<N>` starts at 1 and is incremented by 1 for each successive name-value-operator mapping that you define. The `logicalGrouping` property setting, described later in this table, determines whether any or all of these filtering criteria must be satisfied to start a job from a resource.
	
	The `object_property_name_<N>` value must be in the form `Field Group.Field Name`, such as `SOXControl.Control Owner`. **Note:** The fields **Name**, **Description**, **Creation Date**, and **full path** do not belong a field group as such and should be listed in the form `System.Name`.
	
	The `object_property_value_<N>` value must be a single value that exactly matches the desired value of the object field.
	
	The `object_operator_<N>` value must be one of the following: `=`, `<>`, `>=`, or `<=`.
	
	Example: If you want to launch jobs for all Control objects where the Control Method field has a value set to Manual, you would set the three properties as follows:
	`object_property_name_1=SOXControl.Control Method`
	`object_property_value_1=Manual`
	`object_operator_1==`
	
	If you wanted to restrict those to only the resources not owned by the user KArthur, you would specify:
	`object_property_name_2=SOXControl.Control Owner`
	`object_property_value_2=KArthur`
	`object_operator_2=<>`

`logicalGrouping`	This property evaluates whether any or all of the specified criteria (set with the `object_property_name`, `object_property_value`, and `object_operator` properties) must be fulfilled when starting a job.
	
	Valid values are `AND` and `OR`, as follows:
	`logicalGrouping=AND`
	
	or
	`logicalGrouping=OR`
	
	If the `logicalGrouping` property is set to `AND`, all object criteria must be valid before a job is started from a resource.
	
	If the `logicalGrouping` property is set to `OR`, any single criterion that evaluates to `true` starts a job for the current resource.

Table 85. Job Launch Manager Configuration File Properties (continued)

Property	Description
resource_hierarchy_depth	This property specifies the depth of the parent resource hierarchy from which child resources are selected. Valid values are 1 to 999999999. Use the maximum value (999999999) to retrieve all the possible levels. This property is used if values for parent_object_content_type and parent_object_name properties in the same file have been set. The resource_hierarchy_depth property value determines how many levels under the root object instance are included in the search to find all instances of the object type that is set as the value of content_type property. **Example**: parent_object_content_type = SOXBusEntity parent_object_name = Company ABC/Company ABC resource_hierarchy_depth = 1 content_type = SOXProcess When Job Launch Manager is executed with the above values, it searches for all instances of SOXProcess directly associated to the Business Entity "Company ABC". Job Launch Manager searches only one level down for direct children. **Example**: parent_object_content_type = SOXBusEntity parent_object_name = Company ABC/Company ABC resource_hierarchy_depth = 2 content_type = SOXProcess When Job Launch Manager is executed with the above values, it searches for all instances of SOXProcess that are children or grandchildren associated to the Business Entity "Company ABC".

Remediating Jobs

Occasionally, a job will enter an error state when it cannot perform a required action or when it encounters a situation that it cannot resolve. An example of this is attempting to modify a property on a locked object. The property cannot be modified, so the job enters an error state.

Resolving the situation that caused the error and reactivating the job is known as remediation. You use Interstage BPM Console to identify nodes in error and to reactivate those nodes once the problems are resolved.

This section describes the steps that you can take to remediate a job that is in an error state, and also how to modify the settings involved in the remediation process to fit your own situation.

Important: Structural edits to jobs using Interstage BPM Console are not supported. Interstage BPM Console should only be used to view details of a job and to reactivate it as part of job remediation process.

Overview of the Remediation Process

The remediation process typically follows this sequence of events and tasks:

Procedure

1. A task run in IBM OpenPages encounters a problem.
2. The job is put into an error state.
3. Remediation e-mails are sent to the following users:
   - **Job Initiator** — User who launched the job in an error state
   - **Job Owners** — User or group who owns the job in an error state
   - **Remediator** — User or group assigned to the Remediator role
   - **WorkflowAdministrators group** — User group with the ability to create and modify process definitions and jobs

   You can designate the recipients of these notifications as well as configure other remediation settings in IBM OpenPages .
4. The Remediator does the following:
   a. Clicks the web link in the e-mail to access Interstage BPM Console.
   b. Identifies the job in error in Interstage BPM Console and notes any problems shown for specific nodes.
   c. Logs on to the IBM OpenPages application and corrects the problems.
   d. Returns to Interstage BPM console to re-activate the node or nodes in error.

Results

Certain errors may require more or less effort to remediate, but the above process is typical of most remediations. Steps 3 and 4 are described in more detail in the remainder of this section.

Setting Up Remediation Notifications and Actions

This section describes settings that can be configured in IBM OpenPages to control the notifications and actions that occur when a remediation job is started. These settings, described in Table 86 on page 551 and Table 87 on page 552, are optional and you are not required to modify them before you can remediate jobs. All of the settings have default values.

Important: Before you can automatically initiate remediation e-mails, you must designate an e-mail server for the workflow jobs to use. For details on configuring an e-mail server and sender's e-mail address, see "Configuring a Mail Server for Workflow" on page 323. To customize these settings, see "Configuring Custom E-mail for Workflows" on page 542.

Modifying Job Remediation Settings

To modify job remediation settings, do the following.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | Platform | Workflow | Job Remediation** folder hierarchy.
3. Click the configuration setting you want to change to display its detail page. See Table 86 on page 551 for a list of available settings and default values.
4. In the Value box of the selected setting, type a value.
5. When finished, click **Save**.

Job Remediation Settings

The following settings are used to configure the job remediation actions:

Table 86. Job Remediation Settings

Setting	Description
Job Initiator Mail Subject	Contains the text used as the subject for the e-mail sent to the Job Initiator. Wildcards can be specified in this setting, as described in Table 87 on page 552. **Default**: The job, `{0}`, has encountered an error.
Job Initiator Mail Body	Contains the text used as the body for the e-mail sent to the Job Initiator. Use `\n` to indicate the start of a new line of text. Wildcards can be specified in this setting, as described in Table 87 on page 552. **Default**: Hello `{4}`.`\n\n`This mail was sent to notify you that the job, `{0}`, which you initiated has encountered the following error during its execution:`\n\n{5}\n\n`The specified workflow remediators and job owners have been notified of this issue. Please coordinate with them to remedy the issue and to reactivate the job.
Job Owner Mail Body	Contains the text used as the body for the e-mail sent to the Job Owner. Use `\n` to indicate the start of a new line of text. Wildcards can be specified in this setting, as described in Table 87 on page 552. **Default**: Hello `{4}`.`\n\n`This mail was sent to notify you that a job of which you are an owner has encountered an error. The job, `{0}`, has encountered the following error during its execution:`\n\n{5}\n\n`The specified workflow remediators have been notified of this issue. Please coordinate with them to remedy the issue and to reactivate the job.
Job Owner Mail Subject	Contains the text used as the subject for the e-mail sent to the Job Owner. Wildcards can be specified in this setting, as described in Table 87 on page 552. **Default**: The job, `{0}`, has encountered an error.
Kickoff Remediation Workflow	Can be `true` or `false`. Determines whether a remediation job is launched when a job enters an error state. **Default**: `false`.
Remediation Job Name	Determines the name of the remediation job. Wildcards can be specified in this setting, as described in Table 87 on page 552. **Default**: Remedy Job `{0}`.
Remediation Job Type	Determines the process definition name that will be launched when a job enters an error state. If for some reason you need to edit the remediation process definition, this is the process definition to modify. **Default**: JOB_REMEDIATION.
Remediator	The single user or group responsible for correcting jobs that are in an error state. **Default**: WorkflowAdministrators.

Table 86. Job Remediation Settings (continued)

Setting	Description
Remediator Mail Body	Contains the text used as the body for the e-mail sent to the Remediator. Use `\n` to indicate the start of a new line of text. Wildcards can be specified in this setting, as described in Table 87. **Default**: Hello {4}.\n\nThis mail was sent to notify you that the job, {0}, has encountered the following error during its execution:\n\n{5}\n\nPlease check the OpenPages and InterstageBPMCS log files in <OP_HOME>/aurora/logs and <WORKFLOW_HOME>/InterstageBPM/server/instance/default/logs directories for more information on the error that occurred. In order for the job to complete successfully, please work with the job owner(s), {1}, to remedy the error, and then reactivate the job at the point at which the error occurred.\n\nTo reactivate the job, please use the job administration console available in the InterstageBPM console. You may click on the following link to get to the job detail page:\n\n{7}\n\nFor more information on how to reactivate a job that is in error state, please consult the Workflow Remediation section in the OpenPages Users Guide.
Remediator Mail Subject	Contains the text used as the subject for the e-mail sent to the Remediator. Wildcards can be specified in this setting, as described in Table 87. **Default**: The job, {0}, has encountered an error.
Send Job Initiator Mail	Can be `true` or `false`. Determines whether the job initiator will receive an e-mail when a job enters an error state. **Default**: `true`.
Send Job Owner Mail	Can be `true` or `false`. Determines whether the job owner will receive an e-mail when a job enters an error state. **Default**: `true`.
Send Remediator Mail	Can be `true` or `false`. Determines whether the Remediator will receive an e-mail when a job enters an error state. **Default**: `true`.

The following wildcards can be inserted into the Subject, Body, and Remediation Job Name settings for job remediation in the form {N}, where N is a number from the table below:

Table 87. Supported Wildcards

This wildcard...	Resolves to...
{0}	Name of the job in an error state
{1}	List of the Job Owners for the error job
{2}	Name of the Job Initiator for the error job
{3}	ID of the error job.
{4}	User name of the e-mail recipient.
{5}	Exception message returned by the error job
{6}	Stack trace for the exception.
{7}	Constructed link to the detail page of the job in an error state.

Remediating the Job in Error

There are several tasks to remediate the job:

Procedure

1. Access the job in error in Interstage BPM Console.
2. Identify the problems that are causing the error and resolve them in the IBM OpenPages application.
3. Reactivate the node or nodes in error so that the job can continue.

Access the Job in Error in Interstage BPM Console

In order to remediate the job, you must display the job's detail page on the IBM OpenPages application server. From here you can access Interstage BPM Console and begin correcting the error. The Remediator e-mail contains a link to the job's detail page.

Note: Interstage BPM Console, which launches within the Internet Explorer 8.0 web browser, does not support Adobe® Flash® technology in the 64-bit version of the browser. Flash is required in order to render a graphical view of the job in error. Ensure that you are using the 32-bit version of Internet Explorer 8.0 before accessing Interstage BPM Console for job remediation.

To access the job in an error state in Interstage BPM Console, do the following.

Procedure

1. Open the e-mail containing the remediation notification.
2. Click the link in the body of the e-mail to the job's detail page.
3. Log on to the IBM OpenPages application server as a user with administrative permissions.
4. On the job's detail page is a field named **Remediation Link** with a web link. Click the link to launch Interstage BPM Console.

   Interstage BPM Console's Main window displays (no logon is required). The Process Instance Viewer pane in the Main window presents a graphical view of the job in error.

Results

You can also find jobs in error in the IBM OpenPages application by clicking **Jobs** in the Administration menu, selecting **Error** from the Status list, and clicking **Search**. A list of all jobs in error displays and you can click the job name to display its detail page.

Identify and Resolve the Error

In the Process Instance Viewer pane in Interstage BPM Console, any node(s) in an error state are colored red. You can position the cursor over a red node to display a text box describing the cause of the error. Generally, the most useful information about the error can be found in the last sentence of the text box, such as `The argument must be a String type`.

Once you have viewed the nodes in error and noted the error descriptions, you must log on to IBM OpenPages to resolve the issue. Depending on the cause of the error, there may be multiple ways to fix the problem.

This guide cannot predict all of the possible scenarios that might cause an error state, but two of the most common causes are:

- **Attempting to Modify a Locked Object** — If a task or other node is attempting to modify the field properties on an object, and that object is locked or checked out by another user, the modification will fail and an error state will occur. To fix the problem, remove the lock from the object or check in the resource.
- **Assigning a Task to a Non-Existent User** — In some cases, the job may attempt to assign a task to a user or group that no longer exists. This puts the job in an error state until the task is assigned to a valid user. To fix the problem, either create the missing user or group, or change the task's assignee to a valid user or group.

Reactivate the Nodes in Error

Once you have corrected the problem, you must remove the error state from the job. To do this, you must reactivate the node or nodes that caused the error.

To reactivate the node or nodes in error, do the following.

Procedure

1. In the Process Instance Viewer pane, for each node in error (colored red) that you want to activate, right click the node and click **Activate**.

   Note: If the job associated with the node is locked, you will only be able to activate the node if you unlock the job. To unlock the job, click the **Unlock** button in the Process Instance Viewer pane. A confirmation message displays indicating that the job is now unlocked, and the list of jobs displays in the top half of the pane.
2. When you are done, click the **Refresh BPMN** button to update the status of the nodes in the graphical display. Any nodes that you re-activate are now colored green. The job is activated and the tasks will be assigned to the designated user.

Alternate Methods for Accessing Jobs in Error in Interstage BPM Console

This section describes two other methods for accessing Interstage BPM Console.

From a Web Link

As an alternative to accessing Interstage BPM Console through a link on a Remediator e-mail or a job's detail page, you can access Interstage BPM Console through the following URL:

`http://<server_name>:<port>/openpages/ibpm.console.do`

where `<server_name>` is the host name of your IBM OpenPages application server and `<port>` is the port number of the managed server in your IBM OpenPages application server configuration. For Windows, the managed server port numbers for the application server typically start at 7009; for AIX, 10108.

This displays the IBM OpenPages logon page. After you log on to IBM OpenPages , you will be automatically redirected to the Interstage BPM Console main window (no logon is required).

From the IBM OpenPages Application

You can also access Interstage BPM Console from the IBM OpenPages application.

Note: You must have **Start Jobs** or **View All Jobs** permission to use this access method.

Procedure

1. Log on to the IBM OpenPages application.
2. From the **My OpenPages** menu, select **IBPM Console**.

Results

This displays the Interstage BPM Console main window in a separate browser window (no logon is required).

Troubleshooting Workflows

This section provides a quick reference to setting up job remediation e-mail, the location of Interstage BPM Studio error logs and IBM OpenPages workflow server runtime logs, and a flow chart of the workflow troubleshooting process.

Setting Up Job Remediation E-mails

The following is a quick overview of the process for setting up job remediation e-mails. For more detail on setting up job remediation e-mail, see "Setting Up Remediation Notifications and Actions" on page 550.

Procedure

1. Open an Internet Explorer browser window.
2. Go to the IBM OpenPages URL.
3. Log on as a user with administrator privileges.
4. From the menu bar, select **Administration** and click **Settings**.
5. Expand the **OpenPages** | **Platform** | **Workflow** folder hierarchy, and do the following:
   a. Expand the **Email** folder and make sure that the values in the **Mail From** and **Mail Server** settings are properly configured for your environment.
   b. Expand the **Job Remediation** folder and enable or disable the types of job remediation e-mails to receive with the settings:
      - Send Job Initiator Mail
      - Send Job Owner Mail
      - Send Remediator Mail

      Note: If the **Send Remediator Mail** setting is enabled (set to **true**), then define the group or user that will receive and act upon the job remediation e-mails in the **Remediator** setting.

About Interstage BPM Studio Error Logs

Interstage BPM Studio includes several error log files that may be useful in troubleshooting workflow-related problems. Table 88 on page 556 provides a brief description and the default location of the error log files.

Table 88. Interstage BPM Studio Error Logs

Log File Name	Description	Default Path
`studio.log`	Error messages from the core Interstage BPM Studio application only. Does not include errors from OpenPages-specific functions integrated into Interstage BPM Studio.	`C:\OpenPages\IBPMStudio\InterstageBPM_studio\logs`
`.log`	Eclipse-related error messages from the core Interstage BPM Studio application only. Does not include errors from OpenPages-specific functions integrated into Interstage BPM Studio. **Note:** If the Windows Folder View option **Hide extensions for known file types** is enabled, this log file does not display any file name when viewed in Windows Explorer. It is recommended that you disable or clear this option in order to see the `.log` file name.	`c:\OpenPages\IBPMStudio\InterstageBPM_studio\workspace\.metadata`
`op_ibpm_studio.log`	Error messages from OpenPages-specific functions integrated into Interstage BPM Studio.	`c:\OpenPages\IBPMStudio\InterstageBPM_studio\logs`

About IBM OpenPages Workflow Runtime Error Logs

IBM OpenPages workflow server and application servers include a number of workflow-related runtime error log files that may be useful in troubleshooting workflow problems. See below for a brief description and the default location of the error log files.

The following parameters are used throughout:

- `<server-name>` — Machine name of the IBM OpenPages workflow server (for example, opworkflow_svr).
- `<server#>` — Number of the managed server instance on the IBM OpenPages workflow server (for example, InterstageBPMCS**1**.log, refers to the error log for managed workflow server instance **1**).

Windows only operating environment

Log File Name

`<server-name>-InterstageBPMCS<server#>.log`

Description

Runtime errors and exceptions logged by the IBM OpenPages workflow server application

Path

`<drive>:<Workflow_Home>\server\instance\default\logs`

Log File Name

<server-name>-InterstageBPMCS<server#>.log

Description

Log entries written by the underlying Oracle WebLogic application server about the status of various J2EE resources being used

Path

<drive>:<Workflow_Home>\IBPMDomain\servers\<server-name>-serverName\logs

AIX only operating environment

Log File Name

<server-name>-IBPMNode<server#>Server.log

Description

Runtime errors and exceptions logged by the IBM OpenPages workflow server application

Path

<Workflow_Home>/server/instance/default/logs

Log File Name

SystemOut.log

Description

Log entries written by the underlying IBM WebSphere application server about the status of various J2EE resources being used.

Path

<Workflow_Home>/profiles/<server-name>-IBPMNode<server#>/logs/<server-name>-IBPMNode<server#>Server/

Log File Name

SystemErr.log

Description

Log entries written by the underlying IBM WebSphere application server

Path

<Workflow_Home>/profiles/<server-name>-IBPMNode<server#>/logs/<server-name>-IBPMNode<server#>Server/

Windows and AIX operating environments

Log File Name

<server-name>-InterstageBPMCS<server#>-startup.log

Description

Log entries written during initialization of IBM OpenPages metadata caches on IBM OpenPages workflow server.

Path

- **Windows**

  `<drive>:<OpenPages_Home>\aurora\logs`

- **AIX**

  `<OpenPages_Home>/aurora/logs`

Log File Name

`<server-name>-InterstageBPMCS<server#>-aurora.log`

Description

Log entries written by IBM OpenPages integration code that runs on IBM OpenPages workflow server.

Path

- **Windows**

  `<drive>:<OpenPages_Home>\aurora\logs`

- **AIX**

  `<OpenPages_Home>/aurora/logs`

Workflow Troubleshooting Process

The workflow troubleshooting process flow chart in Figure 15 on page 559 outlines a basic decision tree for troubleshooting workflow issues. It makes the following assumptions:

- Job remediation e-mail is enabled and properly configured on the system
- Workflow administrators have a basic understanding of job remediation

The flow chart is laid out for a single application server. If the workflow environment has more than one application server, the administrator should collect the logs and files from each individual application server.

In instances where the IBM representative may be involved in troubleshooting a workflow issue, the Support Engineer may ask for the standard set of log files. For a listing of the various log files provided by IBM OpenPages , see "Using Log Files" on page 453.

Note: The workflow runtime error logs mentioned in the flow chart refer to the logs listed in "About IBM OpenPages Workflow Runtime Error Logs" on page 556.

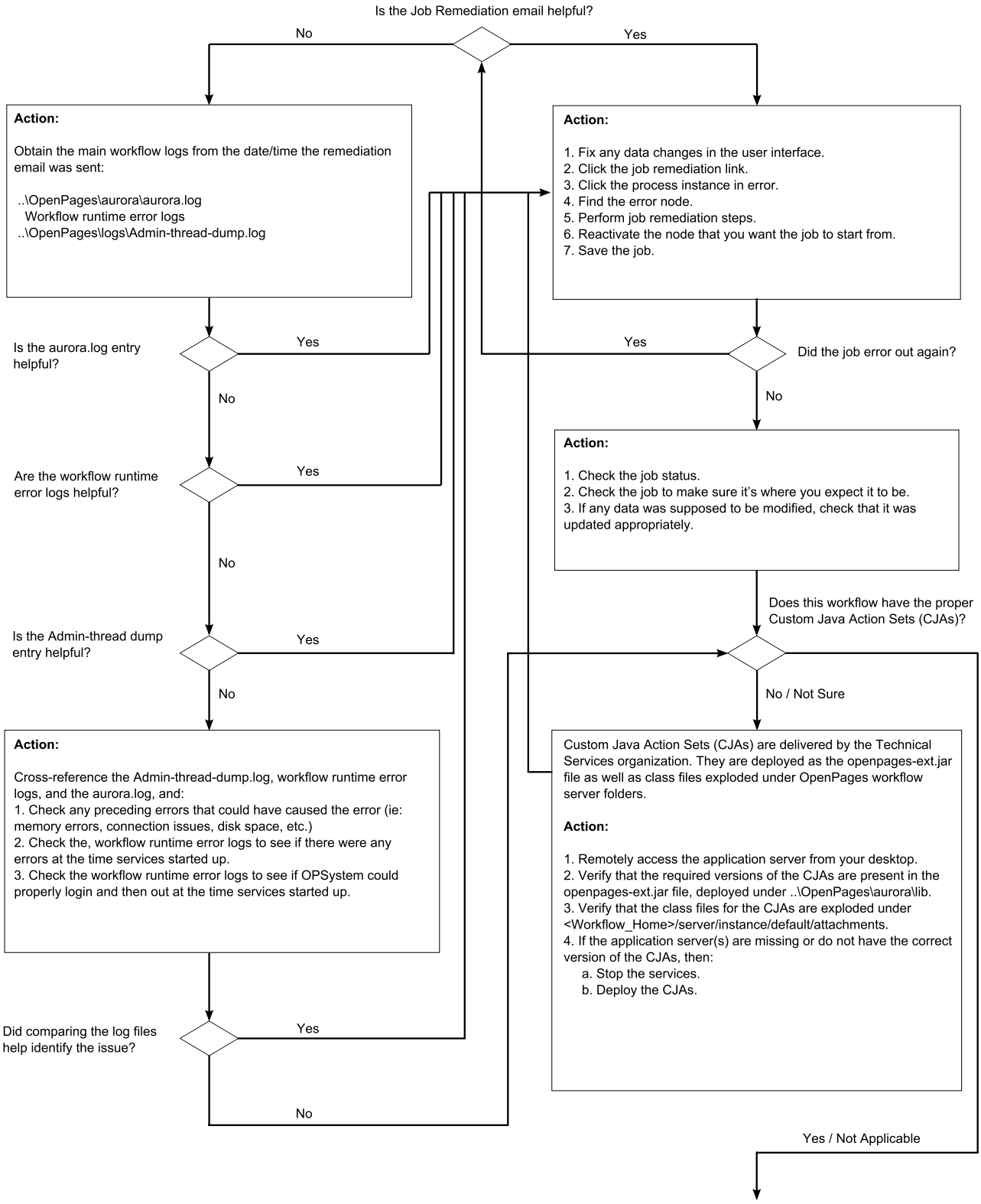
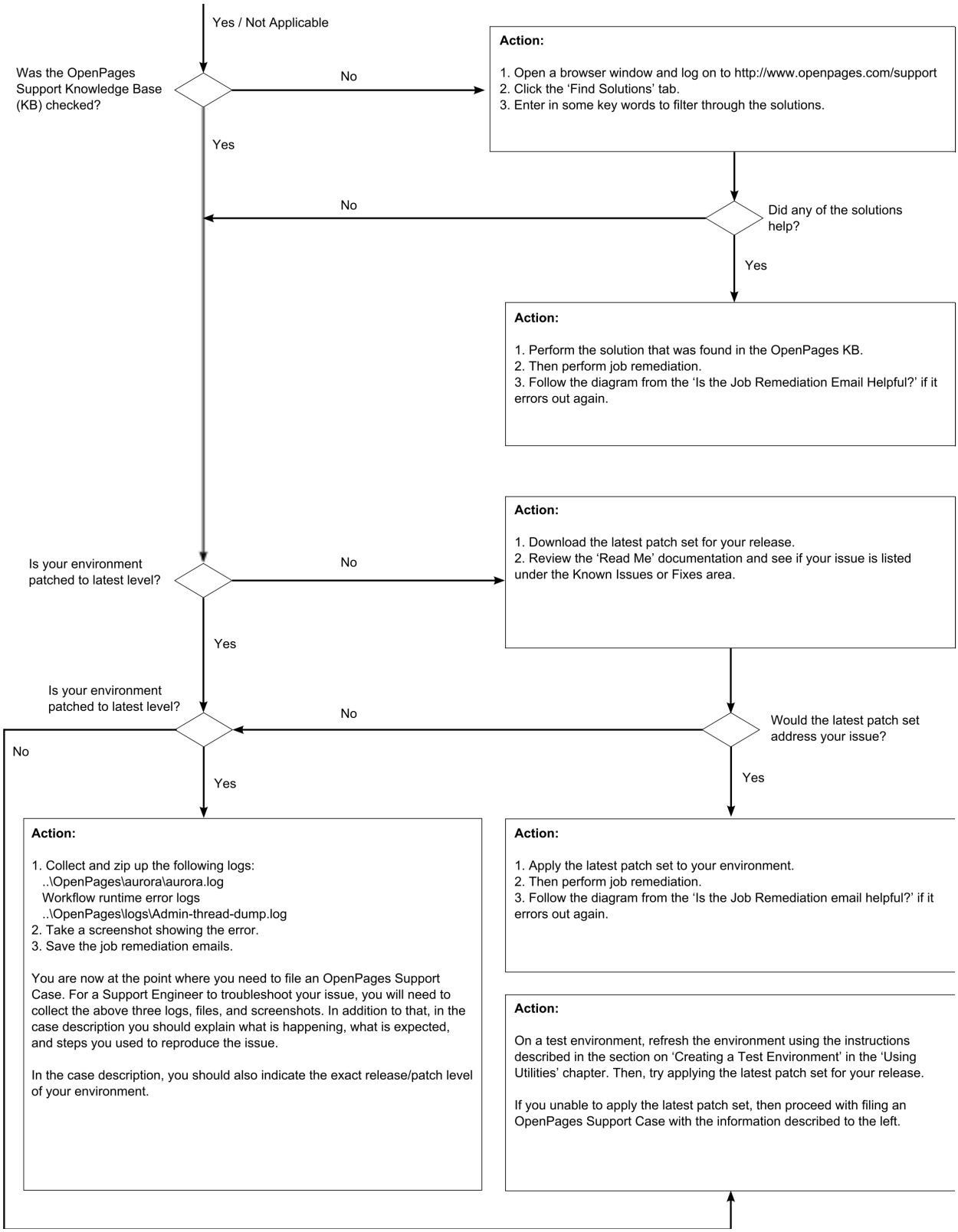


Figure 15. Workflow Troubleshooting Flow Chart

Workflow Troubleshooting Flow Chart (Continued)


Yes / Not Applicable
Was the OpenPages Support Knowledge Base (KB) checked?
No
Action:
1. Open a browser window and log on to http://www.openpages.com/support
2. Click the 'Find Solutions' tab.
3. Enter in some key words to filter through the solutions.
Yes
No
Did any of the solutions help?
Yes
Action:
1. Perform the solution that was found in the OpenPages KB.
2. Then perform job remediation.
3. Follow the diagram from the 'Is the Job Remediation Email Helpful?' if it errors out again.
Is your environment patched to latest level?
No
Action:
1. Download the latest patch set for your release.
2. Review the 'Read Me' documentation and see if your issue is listed under the Known Issues or Fixes area.
Yes
Is your environment patched to latest level?
No
Would the latest patch set address your issue?
No
Yes
Yes
Action:
1. Collect and zip up the following logs:
..\OpenPages\aurora\aurora.log
Workflow runtime error logs
..\OpenPages\logs\Admin-thread-dump.log
2. Take a screenshot showing the error.
3. Save the job remediation emails.
You are now at the point where you need to file an OpenPages Support Case. For a Support Engineer to troubleshoot your issue, you will need to collect the above three logs, files, and screenshots. In addition to that, in the case description you should explain what is happening, what is expected, and steps you used to reproduce the issue.
In the case description, you should also indicate the exact release/patch level of your environment.
Action:
1. Apply the latest patch set to your environment.
2. Then perform job remediation.
3. Follow the diagram from the 'Is the Job Remediation email helpful?' if it errors out again.
Action:
On a test environment, refresh the environment using the instructions described in the section on 'Creating a Test Environment' in the 'Using Utilities' chapter. Then, try applying the latest patch set for your release.
If you unable to apply the latest patch set, then proceed with filing an OpenPages Support Case with the information described to the left.

Chapter 21. Using FastMap

FastMap is an IBM OpenPages productivity tool that works with the IBM OpenPages export feature, and automates the importing and batch processing of object data into the IBM OpenPages application.

The FastMap tool uses a data load template (a Microsoft Excel workbook in .xls format) to capture data for import. When you import data into IBM OpenPages , FastMap validates the data and then, if no errors are found, populates the repository with the new or updated records.

Sample Scenario

You have 150 Process and 175 Risk objects (records) that require either creation or updating. Rather than manually creating or updating individual Process and Risk objects through the IBM OpenPages application interface, you use a FastMap data load template to capture the data for batch processing.

Once the data is captured, you log on to the IBM OpenPages application and import the template (.xls format) through FastMap for validation. During the validation phase, you receive a few validation errors. You fix the errors in the template and resubmit it. This time, no validation errors are reported and the data is automatically processed. Once processing is complete, the objects become available for reports and updating by users.

This chapter contains the following topics:

FastMap Overview

Figure 16 on page 562 provides an overview of the various tasks that are involved with using FastMap to import data into the IBM OpenPages application. The FastMap tool uses a JSP report format to:

- Import and validate data (FastMap Import)
- Display the status of the imported job, a background batch process (FastMap Import Status)

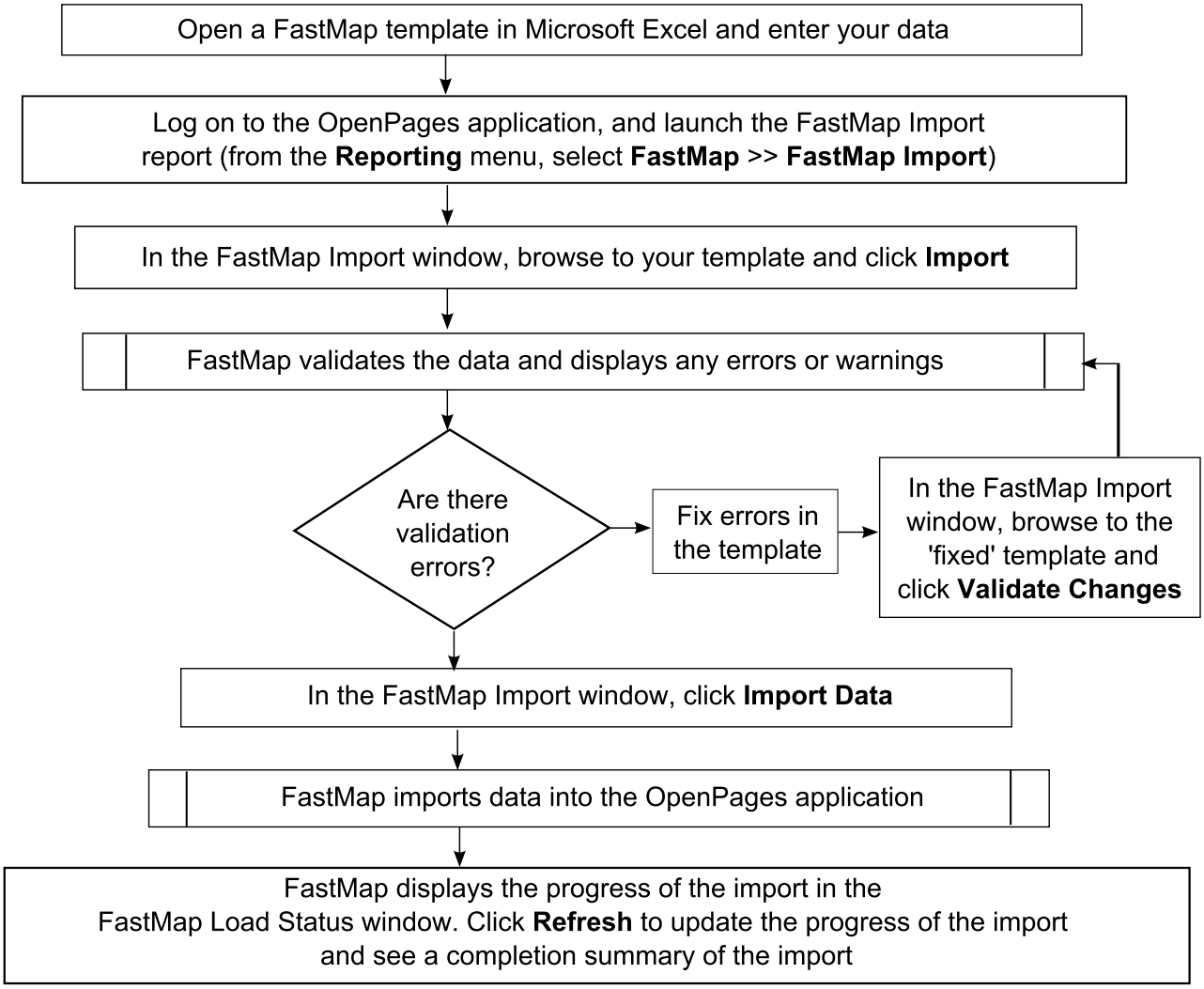


Figure 16. FastMap Task Flow

About FastMap Templates

A FastMap template is a Microsoft Excel workbook with one or more data load worksheets that you create.

A *workbook* for FastMap import has the following characteristics:

- Contains one or more data load worksheets (must be in XLS format). .
- Has only one data load worksheet per object type.
- By default, is in the user's locale.
- Optionally includes a 'Definition' worksheet in a workbook to configure FastMap import and/or export behavior.

A *data load worksheet* within a workbook has the following characteristics:

- Is specific to an object type.
- Has a variety of columns where you specify parent and folder paths and change data for listed objects.
- Each column must have a heading name.

- Optionally includes one or more special column headings.
- Must contain localized column names and data.

Example

Let's say you want only users who are assigned the "Upload Data" profile to import changed or new data for the following five object types: "Business Entities", "Processes", "Risks", "Controls", and "External Losses". You could either create a workbook with multiple worksheets - one for each object type for a total of five data load worksheets, or multiple workbooks - one for each object type.

Note:

- You cannot import attachments or signatures with FastMap.
- FastMap supports only the XLS format in Microsoft Office 2010.
- Only versions of IBM OpenPages 5.5.2 or greater are supported.
- User access is based on the Role Template assigned to a user or group. For details about Role Templates, see "Using Role Templates" on page 43.

About the Data Validation Process

When a FastMap template is imported into the IBM OpenPages application, FastMap checks the user profile, and the setup and format of the worksheets.

By default, FastMap uses the profile of the logged-on user to determine which object types and fields are valid. For example, if an object type or certain object fields are included in a data load template but are excluded in a user's profile, then that object type or those object fields will be excluded from the data imported by FastMap.

In general, FastMap uses the same validation rules that apply to data that is manually entered into the application. For example, validation errors would occur if the profile of the logged-on user includes required fields that are missing from the worksheet, or the maximum number of characters allowed for a field is exceeded, and so forth.

For more details about validation, see "Resolving Validation Errors" on page 565.

About Localization

By default, FastMap uses the locale of the logged-on user to validate data in templates.

As a result, all data in FastMap templates, such as column headings, text, enumerated drop-down or multivalued selection field values, should be localized in the locale of the end user. For example, an end user with the Italian locale (`it_IT`) setting should only import FastMap templates with localized Italian values.

If wanted, you can override the locale of the end user by explicitly specifying a locale in the Definition worksheet of a template. For example, if you specify the `locale` parameter as `en_US` and localize the template in English, the Italian user could upload the template for validation in English, not Italian. For more information, see "Using the Definition Worksheet" on page 581.

When you export object type data from the IBM OpenPages application, the locale is automatically set on the Definition worksheet.

Validation messages that are displayed by FastMap during processing can be localized through application strings.

Using FastMap to Import Data

Accessing FastMap to Import Data and View Status

You can access FastMap in multiple ways from the **Reporting** menu on the IBM OpenPages application user interface to import data or check the status of your data imports.

Note: Access to FastMap depends on your permissions.

Procedure

1. Log on to the IBM OpenPages application.
2. Do one of the following to access FastMap:
   - Select **Reporting** on the menu bar and choose **FastMap** and one of the following reports listed in Table 89.

Table 89. FastMap Reports

Select this report...	To do this...
FastMap Import	Import data from a workbook template
My FastMap Import Status	View the status of all your data imports

   - Select **Reporting** on the menu bar and choose **All Reports** from the list.
3. Navigate to the **FastMap** folder and, if necessary, expand the folder.
4. Click the report you want (see Table 89).

   A separate browser window opens with the selected report.

Importing a FastMap Data Load Template

Note: You can only view FastMap import jobs that you submit.

Procedure

1. Select the **FastMap Import** report to open it (for details, see "Accessing FastMap to Import Data and View Status").
2. In the file selection box, type the name of the data import file, or click **Browse** to navigate to the file.
3. When finished, click **Import**.
4. If validation errors are detected, fix the errors in the workbook template.

   For more information, see "Resolving Validation Errors" on page 565.
5. Resubmit the modified file for validation against the application:
   a. In the **Import changes and revalidate** box, browse to or type the name of the modified file.
   b. Click **Validate Changes**.
6. If validation errors are still detected, repeat Steps 4 and 5 until all the errors are resolved and no validation errors are displayed.
7. When finished and no errors are detected, click **Import Data**.

8. When the **FastMap Import Status** report window is displayed, use the **Refresh** button to view the current status of the import (see "Understanding Import Status Messages" on page 572 for more details).

Resolving Validation Errors

Before FastMap can import data into the IBM OpenPages application, all validation errors that are displayed in the FastMap Import window must be resolved. You resolve these errors by opening the FastMap template in Microsoft Excel and modifying the data.

When finished, you must resubmit the updated template to FastMap for another validation check. If errors are still found, you must repeat the resolution process until all validation errors are resolved. Once all validation errors are resolved, FastMap is ready to import the data into the IBM OpenPages application.

Understanding Validation Errors

Validation errors and warnings are displayed as they occur in the FastMap Import window.

If the FastMap validation process completes with:

- No validation errors - a status message is displayed indicating the number of objects to be imported.
- Warnings - you can load your data or correct the warnings and revalidate.
- Errors - a "Validation Failed" status is displayed along with information about the error.

Table 90 lists some of the most common messages that may be displayed in a FastMap Import window.

Table 90. FastMap Import Validation Error Information

This column...	Displays this...	Possible values...
Type	The category of the message.	• Error • Warning
Description	The type of error, and the name of the missing or invalid object field or invalid value.	See Table 91 on page 566.
Sheet	The name of the object type worksheet.	For example, 'Processes' or 'Risks'.
Row	The row within the Excel worksheet containing the error.	The index number corresponding to a row, for example, '2'.
Column Index	The column index within the Excel worksheet containing the error.	The index letter corresponding to a column, for example, 'N'.
Column Header	The name of the column within the Excel worksheet containing the error.	The localized label of a field name, for example, 'Domain'.

Examples

If the following validation message was displayed in the table on the FastMap Import window:

```
Error Required property is missing value.(Domain) Processes 2 N Domain
```

You would open the data load template, and enter the missing value (such as 'Financial Management') in row 2 under the `Domain` column (N) on the 'Processes' worksheet.

Troubleshooting the Conflict with Recent Updates Warning Message

If you are unable to import changes and the following warning message is displayed:

"Record conflicts with more recent updates and will be ignored."

you need to check the timestamp value for the `exportDate` parameter on the Definition worksheet in the template. The warning message is displayed whenever you try to import a template and the data for an object has been updated since the specified export timestamp.

Important:

Only if you are certain that the changes you want to import are current for all objects in the workbook, you can remove the export timestamp from the template as follows.

Procedure

1. Open the FastMap template in Excel.
   a. If necessary, unhide the Definition worksheet (see "Unhiding a Definition Worksheet" on page 581).
   b. Remove the `exportDate` parameter.
   c. Save the change.
2. Resubmit the template for import.

Troubleshooting FastMap Validation Messages

Table 91 contains a list of FastMap validation messages, a brief description of the cause of the message, and what a user can do to resolve the issue. The messages are listed in alphabetical order and are grouped by type.

Table 91. FastMap Validation Messages

Message	Type	Cause	Resolution
Currency field is missing currency code.	Error	A local amount is entered but the `Local Code` field is blank.	Make sure a value is set for `Local Code` in currency fields.
Currency field is missing local amount.	Error	A local code is entered but the `Local Amount` field is blank.	Make sure a value is set for `Local Amount` in currency fields.
Exchange rate for base currency can only be set to 1.	Error	The `Local Code` and `Base Code` fields are set to the same value but the `Exchange Rate` field is set to a value other than 1.	If the `Local Code` and `Base Code` values are the same, set the `Exchange Rate` field to a value of 1.
Import of Signature Objects not supported.	Error	Signature objects are not supported for import.	Remove Signature objects from the worksheet.

Table 91. FastMap Validation Messages (continued)

Message	Type	Cause	Resolution
Invalid boolean format. Value must be either true or false.	Error	An invalid Boolean value is specified.	Ensure the Boolean value is set to either `true` or `false`.
Invalid currency code.	Error	An invalid value was entered for a currency code.	Ensure the 3-letter ISO currency code is spelled correctly and is valid.
Invalid date format.	Error	The cell contents for a Date field are not recognized.	Format the cell in Excel as `Date` to resolve the issue. If you leave the format as either `General` or `Text`, the text in the cell must match the `inputDateFormat` parameter. You can set this on the Definition worksheet to values such as `dd/mm/yy`.
Invalid decimal format.	Error	A non-numeric value was entered for a decimal field.	Make sure that decimal fields have a numeric value.
Invalid decimal range.	Error	The numeric value entered is outside the minimum or maximum range defined for that field.	Make sure the specified value is within the numeric range defined for that field.
Invalid Exchange Rate.	Error	Exchange rate is 0 or negative.	Make sure the exchange rate value is greater than 0 (zero).
Invalid group.	Error	An invalid value was entered for a Group field.	Ensure the name of the group is spelled correctly and is valid.
Invalid Integer format	Error	A non-numeric value was entered for a numeric value.	Make sure the field has a numeric value.
Invalid Integer range.	Error	The numeric value entered is outside the minimum or maximum range defined for that field.	Make sure the specified value is within the numeric range defined for that field.
Invalid Object Profile. Unable to properly validate spreadsheet.	Error	A value for the profile is specified that is not recognized.	Ensure the name of the profile is spelled correctly and is valid.
Invalid parent resource provided.	Error	The value of the `parentResource` parameter is invalid.	Make sure the full path of the specified parent object is correct.

Table 91. FastMap Validation Messages (continued)

Message	Type	Cause	Resolution
Invalid Property Type.	Error	The column header is not recognized as a property by FastMap. Possible causes: • The field is misspelled in the column heading on the worksheet • The field is missing from the Detail View of the profile being used to import data.	Ensure the column header is spelled correctly. If so, make sure the property is present in your profile's Detail View. **Note:** If you do not want the column to be processed, you can list it under the `ignoreColumns` parameter on the Definition worksheet.
Invalid URL.	Error	An invalid URL was entered for a URL field.	Ensure the URL is correct and fully qualified.
Invalid user.	Error	An invalid value was entered for a User field.	Ensure the name of the user is spelled correctly and is valid.
Invalid user/group.	Error	An invalid value was entered for a User/Group selector.	Ensure the name of the user or group is spelled correctly and is valid.
Locale is invalid.	Error	The locale value specified is not recognized.	Ensure the value of the locale is spelled correctly and is valid.
Missing currency code column.	Error	The local code column is missing and a local amount is specified.	Make sure the local Currency code column is present in your worksheet and has a value for this record.
Missing local amount column.	Error	The local amount column is missing and a local code is specified.	Make sure the local Amount column is present in your worksheet and has a value for this record.
Multiple resources found with the same key value.	Error	When using Key fields, a key is specified that is not unique and FastMap cannot determine which resource to update.	Make sure the value specified for each Key is unique.
Name cannot be blank.	Error	An object type that is not configured for autonaming has an empty `Name` field or the `Name` column is missing from the worksheet. **Note:** This error will not occur if autonaming is enabled for an object type.	Make sure the `Name` column is present in your worksheet and has a value in it for this record.

Table 91. FastMap Validation Messages (continued)

Message	Type	Cause	Resolution
Name contains illegal characters.	Error	Name contains backslashes or forward slashes.	Remove any backward slash (\) or forward slash (/) marks from the name of the object.
Name exceeds maximum characters (in bytes).	Error	Name is longer than 252 characters or bytes for multicode locales.	Make sure the name of the object is shorter than 252 characters or bytes.
Object cannot be associated to a parent of this type.	Error	A parent-child relationship does not exist between the object types being associated.	Either enable an association between the object types you want to associate or modify the worksheet to reflect object types that have a child-parent association already configured.
Parent not specified.	Error	A parent is not specified for a new object and the `allowOrphans` setting is not set to 'true'. Objects being updated do not need to have a parent specified.	Ensure that all three parent fields are present and populated correctly.
Parent Resource content type not recognized. Check that it is viewable in your profile.	Error	The object type of the resource specified by the `parentResource` parameter is not recognized.	Ensure the object type value is spelled correctly. If so, make sure the object type is present in your profile's Detail View.
Parent Resource not found.	Error	A parent is specified in your spreadsheet, but FastMap cannot find it in the IBM OpenPages repository.	Make sure that the `Parent Path` is pointing to the proper folder location and that the `Parent Objects` value is the proper name of the object.
Property value exceeds maximum characters.	Error	A text field contains more characters than is allowed in the IBM OpenPages application.	Modify the text field so it does not exceed the character or byte limit.
Required property is missing value.	Error	A required field for the object type is missing a value. Possible causes: • The column is present on the worksheet and the cell is missing a value • The column for the required field is missing.	Make sure that you have a value set for all properties required on the object.

Table 91. FastMap Validation Messages (continued)

Message	Type	Cause	Resolution
System error.	Error	Any unexpected error occurred. Similar to a 'Requested operation could not be completed' system error message.	Contact your IBM representative.
Text field formatted as number in spreadsheet.	Error	A text property value is formatted as a number or a date in the spreadsheet. A `Text` field in IBM OpenPages is formatted in the worksheet cell as `Number` or `Date`. The field cannot be read in by IBM OpenPages in this state and maintain all of the Excel formatting.	Change the format of the cells in Excel to `Text`.
The file exceeds the maximum number of rows allowed for import.	Error	The total number of rows in the workbook is greater than the value set in the `Maximum Workbook Rows` setting (see "Limiting the Number of Rows for Import" on page 591).	Modify the worksheet so it does not exceed the row limit or change the value of the setting.
The value entered is not a valid selection for this field.	Error	The value for a single select drop-down field is not a valid value. The value must be in the proper locale of the user for it to be recognized.	Ensure the value is typed correctly and is in the correct locale.
The value(s) entered are not valid selections for this field.	Error	The value for a for multi-select drop-down field is not a valid value. The value must be in the proper locale of the user for it to be recognized.	Ensure the value is typed correctly and is in the correct locale.
Full import will result in objects being deleted.	Warning	When setting `fullImport` to 'true,' FastMap identifies objects to be deleted.	Informational message, no action required.

Table 91. FastMap Validation Messages (continued)

Message	Type	Cause	Resolution
Invalid Content Type	Warning	The worksheet name is not recognized by FastMap as a valid object type in the system. Possible causes: • The object type is misspelled on the worksheet tab. • The object type is missing from the Detail View of the profile being used to import data. Although FastMap will import the workbook, the invalid worksheet will be ignored.	Make sure that the object type is spelled correctly on the tab of the worksheet. FastMap treats each worksheet in the workbook as a content type sheet. **Note:** If you do not want the worksheet to be processed, you can list it under the `ignoreSheets` parameter on the Definition worksheet.
Property is read only.	Warning	A value was entered for a field that is read-only in the Detail View of the profile used for import. Although FastMap will import data, the read-only field will be ignored.	Remove the columns from your worksheet. You can also specify the `ignoreReadOnlyWarnings` parameter so that these messages do not occur. However, these fields will not be updated when importing.
Record conflicts with more recent updates and will be ignored.	Warning	A record's last modified date is more recent than the value from the `exportDate` parameter.	See "Troubleshooting the Conflict with Recent Updates Warning Message" on page 566 for details.

Viewing Import Status

After all validation errors are resolved, FastMap displays a status message indicating the number of objects to be imported. Once you initiate the import process, the FastMap Import Status report window opens and displays a variety of messages, and a status summary as whether or not the import was successful.

Using the FastMap Import Status Report Window

The **FastMap Import Status** report window does not automatically update the progress of the import and requires a manual refresh.

Important:

Regularly check the status of your FastMap jobs to know if an import has successfully completed. Templates that have large amounts of data for import have

long running processes. If services, for example, are restarted while FastMap import processes are still running, FastMap jobs will be terminated and the import will not be successful.

Procedure

1. If the **FastMap Import Status** report window is not already opened, open the window (see "Accessing FastMap to Import Data and View Status" on page 564).
2. To view the current status of an import, click the **Refresh** button on the report.
3. To close the report window, click the **X** in the top-right corner of the report.

Results

To understand the various status messages that may be displayed, see "Understanding Import Status Messages."

Understanding Import Status Messages

The FastMap Import Status report window displays a progress meter showing the percentage completed, and the information listed in Table 92.

Table 92. FastMap Import Status Information

This column...	Displays this...	Possible values...
Id	A job identifier.	A generated numeric value, for example: 547.
Name	The name of the import job.	FastMap Import
Status	A progress summary of the import.	• Running • Completed Successfully • Completed With Errors • Terminated (System)
Percent Complete	A progress meter showing the percentage completed	A numeric value, for example: 20%
Create Date	The date and time the import job was created.	A timestamp, for example: Sep 24, 2009 4:23:38 PM EDT

Table 92. FastMap Import Status Information (continued)

This column...	Displays this...	Possible values...
Message	The task detail of the import. Processing task messages contain such information as: • The start and end of the task • The type of task • The number and type of objects being processed • The number of objects created, modified, and unchanged	• Initialized • Preparing to create/update <number> resources • Objects being uploaded: <number> • Processing <number> <object-name> • Finished processing <number> <object-name> • Processed <number> rows • Upload Complete • Objects Created: <number> • Objects Updated: <number> • Objects with no changes: <number> • Terminated by system at startup • ERROR Sheet (object-name) <additional-detail>
Status	The status of each processing task that is displayed.	• Started • Running • Completed Successfully • Completed With Errors • Terminated (System)
Date	The start date and time of each processing task.	A timestamp, for example: Sep 24, 2009 4:23:42 PM EDT

For information about using the FastMap Import Status report window, see "Viewing Import Status" on page 571.

Creating FastMap Import Templates

The quickest way to create a FastMap data load template is to export data from a Filtered List View page for an object type into a Microsoft Excel workbook. You can use that workbook to modify the data, and then use FastMap to import the modified data into the IBM OpenPages application.

About the Data Exported to a Workbook

When you export object data from a Filtered List View page, the resulting Microsoft Excel workbook has the following characteristics:

- All object fields that are displayed on an object's Detail View page for a given user profile are exported to a corresponding worksheet in the workbook.
- Each object field is represented by a column on the worksheet.
- The plural label of the exported object type is displayed on the worksheet tab in the workbook.

  Note: For compatibility with Microsoft Excel, FastMap removes the following special characters from a plural label on the worksheet tab:

/ \ ? * : [ ]

Example

If the localized plural label of Risk object types is `/Risks10*`, the tab on the exported worksheet would be `Risks10`.

- In the default (out-of-the-box) IBM OpenPages export template the special '`Delete`' column and the three '`Parent`' columns are hidden on the object type worksheet.

  See Table 93 for details.

- The Definition worksheet is included in the workbook and populated, by default, with the `profileName`, `locale`, `exportDate`, and `ignoreReadOnlyWarnings` parameters.

  See Table 97 on page 581 for details.

An Overview of the FastMap Import Process

The following steps provide an overview of the process for creating and using a FastMap template to import data.

Procedure

1. Create a Microsoft Excel workbook by either exporting data from a Filtered List View page or creating a template manually.

   To export data from a Filtered List View:

   a. Select the object type you want.
   b. If wanted, use a filter to narrow the search results for export.
   c. Once the desired results are displayed, click the **Export** button (to export in `.xls` format). The fields that are exported correspond to the fields that are on an object's Detail View page.
2. Add or modify the object data on the worksheet as needed. Unhide columns if necessary.
3. Optionally, add or modify parameters on the Definition worksheet as needed.
4. When finished, save the file.
5. Import the workbook using the FastMap tool (see "Accessing FastMap to Import Data and View Status" on page 564).

Working With Data Load Worksheets

A data load worksheet for an object type contains columns that identify the path and fields of objects (resources) of the same type for which you want to import change data into the IBM OpenPages application.

Defining Paths for Objects

Figure 20 on page 580 lists the various worksheet columns that you use to define the path of an object.

- The path columns in Figure 20 on page 580 must precede any object field columns that are listed in a worksheet.
- If you have set the `parentResource` parameter on the Definition worksheet, the columns in Figure 20 on page 580 are optional.

Table 93. Columns That Define the Path of an Object

This column...	Contains...
Folder Path	The path of an object.

Table 93. Columns That Define the Path of an Object (continued)

This column...	Contains...
Parent Path	The path of an object's parent folder.
Parent Object Types	The type of parent object to which the child object will be associated.
Parent Objects	The name of the parent object.

For a sample worksheet showing these columns, see "Sample Worksheets" on page 578.

Using Special Column Headings

You can optionally add special column headings to a FastMap data load worksheet to:

- Delete objects from the IBM OpenPages repository (see "Deleting Objects")
- Disassociate objects (see "Disassociating Objects" on page 576)

Note:

- Adding a special column heading to a worksheet is optional.
- The special column headings and values must be localized.
- The values associated with special column headings are not case sensitive.
- Special column headings can be placed anywhere in a worksheet. As a best practice, we recommend placing these columns at the beginning of a worksheet.

Deleting Objects

To delete objects from the IBM OpenPages application, add a `Delete` column to the data load worksheet. By default, the `Delete` column is present on the worksheet when data is exported from the IBM OpenPages application. To see how the `Delete` column is used in an example, see Figure 18 on page 579.

Table 94. Delete Column Values

If the value is set to...	Then...
`Y`	Only objects that are specified for deletion (that is, have a 'Y' in their row under the `Delete` column) will be deleted from the IBM OpenPages repository. Any child objects associated with the specified object will remain in the repository.
`N` or "blank" (no value specified)	The object will not be deleted. This value is set by default.

Table 94 shows the values for the 'Delete' column.

Renaming Objects

To rename objects within the IBM OpenPages application, add a `New Name` column to the data load worksheet.

For each object you want to rename, specify the new name for the object in the corresponding row under the `New Name` column.

Note:

- Names that are entered into the `New Name` column will override names of objects that have auto-naming enabled for new objects and/or editing of an auto-generated name disabled.
- The rename function is not supported for self-contained objects or objects in a security context.

Disassociating Objects

To disassociate objects within the IBM OpenPages application, add a `Remove Association` column to the data load worksheet. See Figure 18 on page 579 for an example.

Table 95. Remove Association Column Values

If the value is set to...	Then...
`Y`	Child objects with a 'Y' in their row under the `Remove Association` column will be disassociated from the specified parent object. A parent object is defined by placing information in the corresponding row of the child object for the following columns: • `Parent Path` • `Parent Object Types` • `Parent Objects`
`N` or "blank" (no value specified)	The object will not be disassociated. This value is set by default.

Table 95 shows the values for the Remove Association column.

Defining Property Fields for Objects

The number and type of object field columns in a template for an object type are optional and depend on the type of data you want to import.

Here are some general rules for defining object fields:

- Each object field that you want to update for a selected object type requires a separate column on the worksheet.
- You must use localized column names and values.
- All object field columns follow the path definition columns as described in Table 93 on page 574.

For more information about working with object fields, see "Guidelines for Entering Object Data into Templates."

Guidelines for Entering Object Data into Templates

The following are some general rules you should follow when entering object data into a FastMap data load template.

Associating Child Objects

To associate child object to parent objects, use the following columns:

- `Parent Object Types` - This localized column identifies the type of parent to which you are associating the record. For example, Business Entity or Risk.

- `Parent Objects` - This localized column identifies the name of the parent object to which you are associating the record.

Auto-naming

If auto-naming is enabled for an object, the `Name` column can be excluded or left blank.

Currency Fields

For each currency field that you include in your template, you must use a special column syntax that defines the local currency code, the amount, and exchange rate of that currency data.

Where:

<*field name*> in Table 96 represents the name of a currency field for a specified object.

Table 96. Column Syntax for Currency Fields

Use this column syntax...	To define...
`<field name>.Amount`	The amount based on the local currency code.
`<field name>.Currency`	The local currency code of the data being entered.
`<field name>.Exchange Rate`	The exchange rate to apply when calculating the value in the System Base Currency. **Note:** • This field is optional. • If an exchange rate is not specified in the template, it will use the default exchange rate set in the application. • When entering data where the Local Currency Code is the same as the System Base Currency Code, this column should not be populated.

Note: If the following currency-related fields are included on a worksheet, these fields will be ignored during import:

`Base Amount` (this value is set globally)

`Base Code` (this is a derived value)

Enumerated Multivalued Selection Fields

When entering data for enumerated drop-down or multivalued selection fields, only localized values are valid. Each selection value should be entered on a separate line within the same worksheet cell.

Note: To enter data for multiple values in the same worksheet cell, press the **Alt** + **Enter** keys simultaneously on your keyboard (after you type the value) to enter a Microsoft Excel line break.

Example

Let's say you have a multivalued enumerated field called "Domain" with the following selection values: Compliance, Operational, Technology, Financial

Management, Internal Audit. Figure 17 shows how data containing multiple values for the "Domain" field might look in the worksheet.

Figure 17. Sample Multivalued Selection Column with Values

About Adding Custom Columns and Worksheets

If wanted, you can add user-defined columns to a worksheet or user-defined worksheets to FastMap templates.

Each custom column that you add to a worksheet must have a heading name, and each custom worksheet that you add to a workbook must have a worksheet name.

So that FastMap does not try to validate any user-defined columns or worksheets, you must add the following parameters to the Definition worksheet:

- `ignoreColumns` - use for any user-defined columns and specify each heading name. For example, "column1;column2".
- `ignoreSheets` - use for any user-defined columns and specify the worksheet names. For example, "sheet1;sheet2".

See “About the Definition Worksheet” on page 581 for a sample Definition worksheet, and Table 99 on page 584 for additional parameters.

Sample Worksheets

Sample Object Worksheet for Updating and Creating Objects

The sample Processes worksheet in Figure 18 on page 579 and Risks worksheet in Figure 19 on page 579 contain a combination of existing objects for update and the creation of new objects.

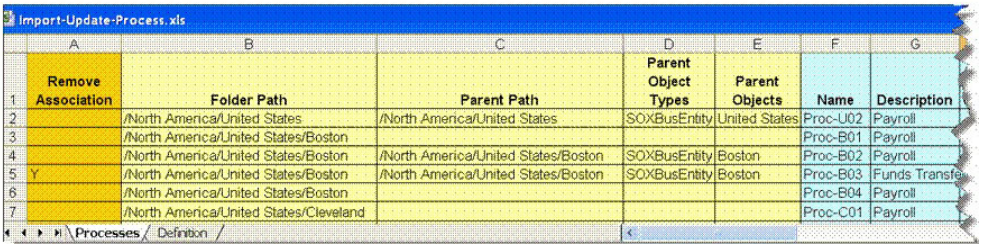
Sample Processes Worksheet:

The sample Processes worksheet in Figure 18 on page 579 shows the following:

- **Column A** (orange) - Remove Association column. **Row 5** contains an existing Process object (`Proc-B03`) that will be disassociated from the `Boston` entity.
- Columns B through E (yellow) define the path of the object.

- **Rows 3, 5, 6, and 7** contain existing Process objects that require updating. With the exception of Row 5 (an existing object that will be disassociated), Columns C, D, and E can remain blank for existing objects.
- Rows 2 and 4 contain information for the creation of new Process objects. Path and parent object information is provided in Columns C, D, and E for each new object to be created.

• **Columns F through Z** (blue) represent object-specific fields.



Import-Update-Process.xls

	A	B	C	D	E	F	G
1	Remove Association	Folder Path	Parent Path	Parent Object Types	Parent Objects	Name	Description
2		/North America/United States	/North America/United States	SOXBusEntity	United States	Proc-U02	Payroll
3		/North America/United States/Boston				Proc-B01	Payroll
4		/North America/United States/Boston	/North America/United States/Boston	SOXBusEntity	Boston	Proc-B02	Payroll
5	Y	/North America/United States/Boston	/North America/United States/Boston	SOXBusEntity	Boston	Proc-B03	Funds Transfe
6		/North America/United States/Boston				Proc-B04	Payroll
7		/North America/United States/Cleveland				Proc-C01	Payroll

Processes / Definition

Figure 18. Sample Processes Worksheet

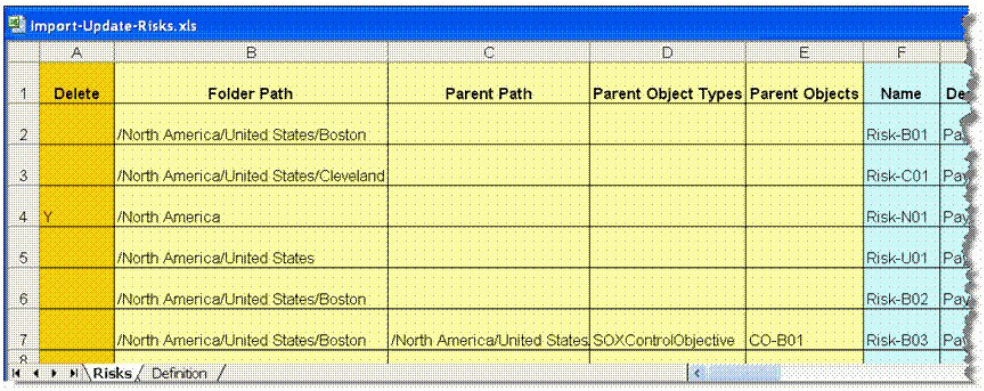
Sample Risks Worksheet:

The sample Risks worksheet in Figure 19 shows the following:

• **Column A** (orange) - Delete column. **Row 4** contains an existing Risk object (`Risk-N01`) under the `North America` entity. The `Y` in this column will result in `Risk-N01` being deleted from the repository.

• Columns B through E (yellow) define the path of the object. Notice the following:
  - **Rows 2 - 6** contain existing Risk objects that require updating (notice that Columns C, D and E can remain blank for existing objects).
  - Row 7 contains information for the creation of a new Risk object (notice that path and parent object information is provided in Columns C, D and E).

• **Columns F through Z** (blue) represent object-specific fields.



Import-Update-Risks.xls

	A	B	C	D	E	F
1	Delete	Folder Path	Parent Path	Parent Object Types	Parent Objects	Name
2		/North America/United States/Boston				Risk-B01
3		/North America/United States/Cleveland				Risk-C01
4	Y	/North America				Risk-N01
5		/North America/United States				Risk-U01
6		/North America/United States/Boston				Risk-B02
7		/North America/United States/Boston	/North America/United States	SOXControlObjective	CO-B01	Risk-B03

Risks / Definition

Figure 19. Sample Risks Worksheet

Sample Self-Contained Object Type Worksheet

If you are adding new self-contained objects, such as Processes in a Process-based security model, these objects must reside under their own folder. This folder must match the object's name.

Important: You must specify the container folder for a self-contained object.

Table 93 on page 574 shows how to specify folder and parent paths for Process objects in a Process-based security model. In this example, the Process folder is named 'PR-200' and is appended after the Business Entity 'Boston' folder.

Notice that the `Folder Path` column contains the name of the Process folder, 'PR-200'.

	A	B	C	D	E	F	G	
1	Delete	Folder Path	Parent Path	Parent Object Types	Parent Objects	Name	Description	Crea
2		/North America/United States/Boston/PR-200	/North America/United States/Boston	SOXBusEntity	Boston	PR-200	Payroll	
3								

Figure 20. Sample Worksheet for Process Objects (Process Security Model)

Figure 21 shows how to specify folder and parent paths for child Risk objects in a Process-based security model. Similarly, in this example, the Process folder is named 'PR-200'

Notice that both the `Folder Path` and `Parent Path` columns contain the name of the Process folder, 'PR-200'.

	A	B	C	D	E	F	
1	Delete	Folder Path	Parent Path	Parent Object Types	Parent Objects	Name	D
2		/North America/United States/Boston/PR-200	/North America/United States/Boston/PR-200	SOXProcess	PR-200	Risk-200	Pay

Figure 21. Sample Worksheet for Risk Objects (Process Security Model)

Sample Business Entity Worksheet for Creating a New Business Entity Structure

The sample business structure in Figure 22 shows three levels of business entities.

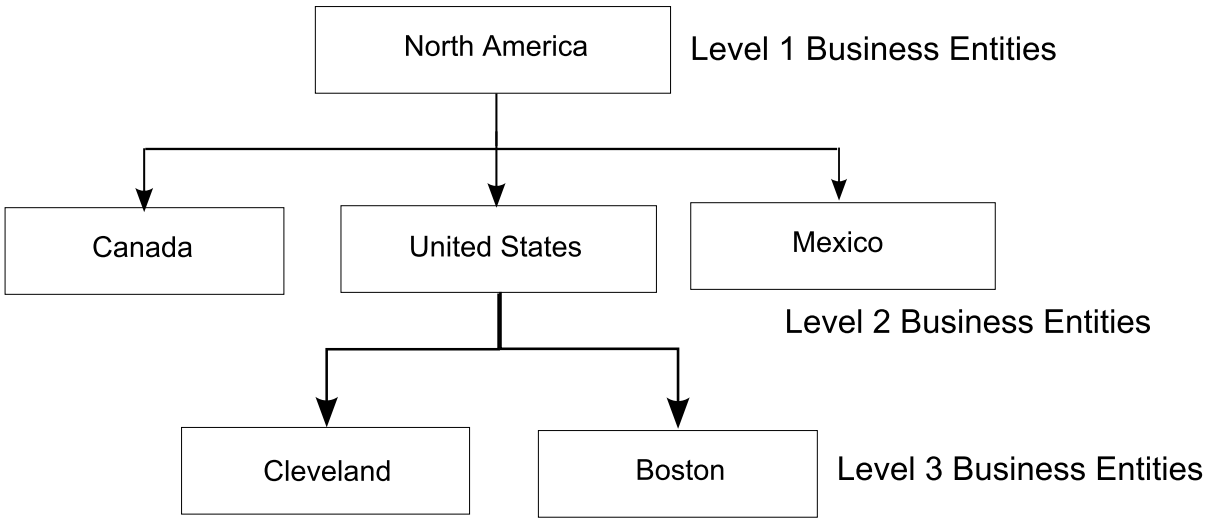
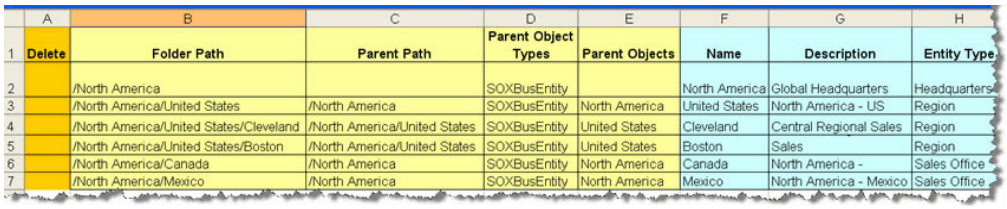


Figure 22. Sample Business Entity Structure

To create new Business Entity objects that map to the structure in Figure 22, you would create a Business Entities object worksheet in Microsoft Excel similar to the one shown in Figure 23 on page 581.

The sample Business Entities worksheet in Figure 23 creates new entities and shows the following:

- **Column A** (orange) - this is an optional field - use to delete existing objects. Since all the objects in this worksheet are new, none are marked for deletion (by default, the value is 'N' for no - do not delete).
- **Columns B through E** (yellow) define the path of the new object. Notice that Row 2 contains the top-level Business Entity (North America), so the `Parent Path` and `Parent Objects` columns are blank.
- **Columns F through Z** (blue) represent object-specific fields.



	A	B	C	D	E	F	G	H
1	Delete	Folder Path	Parent Path	Parent Object Types	Parent Objects	Name	Description	Entity Type
2		/North America		SOXBusEntity		North America	Global Headquarters	Headquarters
3		/North America/United States	/North America	SOXBusEntity	North America	United States	North America - US	Region
4		/North America/United States/Cleveland	/North America/United States	SOXBusEntity	United States	Cleveland	Central Regional Sales	Region
5		/North America/United States/Boston	/North America/United States	SOXBusEntity	United States	Boston	Sales	Region
6		/North America/Canada	/North America	SOXBusEntity	North America	Canada	North America -	Sales Office
7		/North America/Mexico	/North America	SOXBusEntity	North America	Mexico	North America - Mexico	Sales Office

Figure 23. Sample Business Entity Worksheet

Using the Definition Worksheet

Optionally, you can include a Definition worksheet in a workbook to configure FastMap behavior. Parameters that are listed in a Definition worksheet will override settings from other sources, such as JSP report parameters.

About the Definition Worksheet

When you export data from IBM OpenPages , by default (out-of-the-box), the Definition worksheet:

- Is not hidden from users in the workbook
- Does not have column headings.
- Has the following parameter values set by default:

Table 97. FastMap Definition Worksheet Default Parameters

Parameter	Value
ignoreReadOnlyWarnings	TRUE
locale	en_US
profileName	Default
exportDate	The date and time the data was exported. Example: 24-Jul-2009 10:12:52 AM

Note: For a description of these default parameters and a list of additional parameters that you can configure, see Table 99 on page 584.

Unhiding a Definition Worksheet

If you do not see the Definition worksheet in a FastMap template workbook, and you want to change or add parameters to it, then you must unhide the worksheet.

By default (out-of-the-box), the Definition worksheet is not hidden.

Procedure

1. In Microsoft Excel, select the workbook with the hidden Definition worksheet.
2. From the toolbar select **Format** | **Sheet** | **Unhide**.
3. In the **Unhide** box, select **Definition** and click **OK**.
4. Modify or add parameters as required. See Table 99 on page 584 for details.
5. When finished, save the file.

Configuring FastMap

This section contains settings and parameters you can use to configure FastMap behavior.

About FastMap Parameters

You can use FastMap parameters to customize how data is imported (uploaded) to and exported from the IBM OpenPages application.

To set FastMap parameters, you can do the following:

- List parameter names on the Definition worksheet of a FastMap template
- Pass parameters during an import through the FastMap JSP report page template

About Export Templates

An export template is used to format object data that is exported from a Filtered List View page into Excel. By configuring parameters on the Definition worksheet of an export template, you can control the behavior of the export or its subsequent import.

Unless another template is specified, the IBM OpenPages application uses `DefaultTemplate.xls` as the default export template.

Modifying Parameters in the Default Export Template

By default, the Definition worksheet in the `DefaultTemplate.xls` file has only the `ignoreReadOnlyWarnings` parameter set to `TRUE`.

To add or modify parameters in this file, use the following instructions.

Procedure

1. Open a browser window and log on to the IBM OpenPages server administrator interface (typically `/opx`) as a user with administrative privileges.
2. Click the **Browse files** link under the **Files** heading in the left navigation Action menu.
3. Navigate through the folder structure to the `DefaultTemplate.xls` as follows:

   `Templates >> FastMap >> FLV`
4. Modify the `DefaultTemplate.xls` as wanted. Available parameters are listed in Table 99 on page 584.

Specifying an Export Template

The IBM OpenPages application supports multiple export templates.

You can specify export templates based on one or more of the following criteria:

- ContentType
- Locale

- Profile

Rules for Specifying Criteria:

Use the following rules when specifying criteria for an export template:

1. Criteria is specified in the name of the export template.
2. Each criterion is separated in the template name by a hyphen.
3. The criterion must be specified in order: `ContentType-Locale-Profile`

The syntax for the export template name is:

```
<ContentType>-<Locale>-<Profile>.xls
```

Where:

`<ContentType>` is the system name of an object type (such as, SOXRisk), not the localized name. To specify all object types, use `DefaultTemplate` for the `<ContentType>`.

`<Locale>` is the language and locale code (for example, en_US). To specify all locales, use `All` for the `<Locale>`.

`<Profile>` is the name of a profile in the IBM OpenPages application.

Examples

For purposes of illustration, the examples listed in Table 98 for specifying criteria in export templates use the Risk object type (`SOXRisk`) in the U.S. English locale (`en_US`) for users assigned the 'FCM Module' profile.

Table 98. Example Syntax for Specifying Criteria

If you want to specify...	Example syntax...
a specific object type for a specific locale and profile	`SOXRisk-en_US-FCM Module.xls`
all object types (use 'DefaultTemplate') for a specific locale and profile	`DefaultTemplate-en_US-FCM Module.xls`
all locales (use 'All') for a specific object type and profile	`SOXRisk-All-FCM Module.xls`
all locales and all profiles for a specific object type	`SOXRisk.xls`
all profiles for a specific object type and locale	`SOXRisk-en_US.xls`
a specific profile for all object types and locales	`DefaultTemplate-All-FCM Module.xls`

Note: Subsets must honor ordering. For example, the following template names would be invalid:

`FCM Module.xls` - this is an invalid template name as the profile name must be the third criterion in the list (not the first).

en_US-FCM Module.xls - this is an invalid template name as the locale must be the second (not the first) and profile name must be the third (not the second) criterion in the list.

About Template Selection: The system selects templates based on the following precedence: ContentType -> Profile -> Locale

Examples

SOXRisk.xls will be selected before DefaultTemplate-en_US-FCM Module.xls.

SOXRisk-All-FCM Module.xls will be selected before SOXRisk.xls

Note: If no match is found, the DefaultTemplate.xls export template is used.

FastMap Parameters for Importing and/or Exporting Data

Table 99 lists the various FastMap parameters that you can use on a Definition worksheet to configure FastMap behavior.

Table 99. FastMap Definition Worksheet Import-only Parameters

Parameter Name	Default Value	Description
Import-only Parameters		
allowOrphans	FALSE	Determines if objects will be created when no parent object is specified. If the value is set to: • TRUE - creates an object if no parent is specified • FALSE - create an object only if a parent is specified
disableConflictDetection	FALSE	Determines if objects have been modified in the system since you last exported data into the worksheet. When a worksheet is exported from IBM OpenPages , it is marked with the time of the export. When data is imported back into the system, any objects that have been updated after this time will result in a validation message alerting the user and will not be updated. If the value is set to: • TRUE - no validation errors will be displayed and the worksheet values will override any recent changes in the system. • FALSE - a validation error will be displayed and the object will not be updated.

Table 99. FastMap Definition Worksheet Import-only Parameters (continued)

Parameter Name	Default Value	Description
`fullLoad`	FALSE	Used when the data in your worksheet is a complete representation of what should be in the IBM OpenPages repository. If used in conjunction with the `parentResource` parameter, only objects under that resource will be affected. Object types that are not being uploaded will not be deleted in the system. If the value is set to: • `TRUE` - any objects that are not in the set being uploaded will be deleted. • `FALSE` - any objects that are not in the set being uploaded will be retained.
`ignoreColumns`	null	Use if you want to include an additional column on a worksheet for information, and you want that column to be ignored by FastMap during validation. For example, "column1;column2"
`ignoreEmptyFields`	TRUE	Determines whether or not empty fields are blanked out during updates. If the value is set to: • `TRUE` - empty fields are ignored and not modified during an update. • `FALSE` - empty fields will be blanked out during an update.
`ignoreHiddenEnumWarnings`	TRUE	Determines if warning messages are displayed when values are submitted for hidden enumerated strings on a field in the IBM OpenPages application. If the value is set to: • `TRUE` - no warning is displayed for hidden enumerated string values, whether changed or not. • `FALSE` - a warning is displayed for hidden enumerated string values, whether changed or not. Hidden enumerated string values that have been changed on objects will be updated during the import process regardless of the value of this setting.

Table 99. FastMap Definition Worksheet Import-only Parameters (continued)

Parameter Name	Default Value	Description
ignoreReadOnlyWarnings	FALSE	If data is being uploaded into fields that are defined as read-only, IBM OpenPages will display a warning message indicating that these values will be ignored. Use this setting to hide or display warning messages for read-only fields. Regardless of the whether or not warning messages are displayed, the data will not be uploaded. If the value is set to: • TRUE - warning messages are hidden. **Note:** This value is set to TRUE in the default template when you export data from IBM OpenPages . • FALSE - warning messages are displayed.
ignoreSheets	null	Use if you want to include an additional worksheet for information, and you want that worksheet to be ignored by FastMap during validation. For example, "sheet1;sheet2".
parentResource	null	When set to the full path of an object, this parameter is used for all parent associations. All other parent information in the worksheet will be ignored.
shouldDefaultNotRequiredFields	TRUE	Determines whether or not default values will be used for all non-required fields that are missing values in a worksheet. If the value is set to: • TRUE - default values will be used for non-required fields that are missing values in a worksheet. • FALSE - no default values will be used for non-required fields that are missing values in a worksheet.
shouldDefaultRequiredFields	TRUE	Determines whether or not default values will be used for all required fields that are missing values in a worksheet. If the value is set to: • TRUE - default values will be used for required fields that are missing values in the worksheet. • FALSE - required fields that are missing values in the worksheet will display validation errors.

Table 99. FastMap Definition Worksheet Import-only Parameters (continued)

Parameter Name	Default Value	Description
shouldValidateRequiredFields	TRUE	Determines whether or not required fields are validated during import. If the value is set to: • TRUE - required fields will be validated. • FALSE - required fields will not be validated. This could result in errors during object creation if disabled.
suppressWarnings	FALSE	Determines whether or not warning conditions will be displayed. If the value is set to: • TRUE - warning conditions will not be displayed. • FALSE - warning conditions will be displayed.
useFirstInstance	TRUE	Determines whether or not to use and validate only the first instance of an object when multiple instances of the same object are in a worksheet. If the value is set to: • TRUE - only the first instance of the object will be used to update the object. • FALSE - only the last occurrence of the object will be used to update the object.

Table 100. FastMap Definition Worksheet Import and Export Parameters

Parameter Name	Default Value	Description
Import and Export Parameters		
exportDate	null	When exporting data from IBM OpenPages , this parameter is set, by default, to the current date and time. During the import validation process, each object is checked against the export timestamp. If changes to an object are more recent than the date and time of the export timestamp, a conflict exception warning message will be displayed during validation. The message alerts the user that they may be overwriting more recent changes made to an object. To disable this behavior you can set the disableConflictDetection parameter to TRUE.
headerRow	1	The row in the worksheet that stores the column headers.

Table 100. FastMap Definition Worksheet Import and Export Parameters (continued)

Parameter Name	Default Value	Description
`locale`	null	If a `locale` value is: • Not specified - the locale of the user will be used during validation. • Specified - the locale value that is set (such as, en_US, ja_JP, de_DE) will override the user's locale during validation.
`multiSelectDelim`	`\r\n`	Delimiter for multi-select enumeration lists. The default for Microsoft Excel is carriage return line feed that can be entered in Excel by using the **Alt+Enter** key sequence.
`profileName`	null	The name of the profile to validate against. If null, the profile of the currently logged-on user is used.
`useSystemNames`	FALSE	By setting this parameter to TRUE FastMap will use the system names of the fields, not the localized labels, for column headers. System names are in the format [FIELD GROUP].[FIELD NAME]. For example, `OPSSEnt.Domain`. When exporting, the labels will also be included on another row as a convenience.

Table 101. FastMap Definition Worksheet Export-only Parameters

Parameter Name	Default Value	Description
Export-only Parameters		
`exportComputedFields`	TRUE	Determines if computed fields will be evaluated and their values exported with other fields. If the value is set to: • `TRUE` - computed fields will be evaluated and their values exported with other fields. • `FALSE` - computed fields will be ignored during export.
`exportBaseAmount`	TRUE	When exporting currency field data from IBM OpenPages , this parameter determines whether or not to include a column for the Base Amount. If the value is set to: • `TRUE` - the Base Amount field is included. • `FALSE` - the Base Amount field is excluded.

Table 101. FastMap Definition Worksheet Export-only Parameters (continued)

Parameter Name	Default Value	Description
exportBaseCode	TRUE	When exporting currency field data from IBM OpenPages , this parameter determines whether or not to include a column for the Base Code. If the value is set to: • TRUE - the Base Code field is included. • FALSE - the Base Code field is excluded.
exportExchangeRate	TRUE	When exporting currency field data from IBM OpenPages , this parameter determines whether or not to include a column for the Exchange Rate. If the value is set to: • TRUE - the Exchange Rate field is included. • FALSE - the Exchange Rate field is excluded.
includeHTMLTags	FALSE	Determines if HTML tags are exported for Rich Text Field formatted data. Rich Text Field data that is exported without HTML tags can be more easily read in the spreadsheet. However, if this field is updated and then imported into FastMap, the field will be imported as plain text as it has lost its formatting. If the value is set to: • TRUE - HTML tags are exported with the data. • FALSE - HTML tags are not exported with the data.

Configuring a Lookup Key for FastMap

Within the IBM OpenPages application, the Name field for objects is a required field and must be unique. If you are importing data from an external system and want to use another field (other than the Name field) to identify objects, you can use the settings described in Table 102 on page 590 to configure a lookup key for FastMap and set the scope of the lookup. This is particularly useful when you want to update data for existing records from an external system and synchronize it with records in IBM OpenPages .

Note: You can only use object fields with the data type of Simple String, Integer, or Enumerated String as lookup keys.

Example

You want to import risk data from an external system into the IBM OpenPages repository. Data from the external system has a unique 'ID' field that you want to keep and use as a lookup key within IBM OpenPages .

You would create a custom field group and field definition within IBM OpenPages for the Risk object type (SOXRisk) for the 'ID' field in the external system, for example, `ExternalSys_A.Risk_ID`.

You would then use the custom field group and field definition, `ExternalSys_A.Risk_ID`, to configure the `Key` setting for FastMap. Once this setting is configured, you would add a column to your FastMap template for the `Risk_ID` field and populate it with values from the external system's 'ID' field. When you import data from the external system, FastMap would then match records based on this field.

If wanted, you could also scope the update of Risk data under a specific parent object. By setting the `Scoped` value to `true`, FastMap would only try to update objects under the parent that is specified in the worksheet.

Procedure

1. For each object type for which you want a lookup key, configure a field group and field definition (see Chapter 7, "Configuring Fields and Field Groups," on page 103).
2. Configure the key fields settings for FastMap as follows:
   a. Access the Settings page (see "Accessing the Settings Page" on page 268).
   b. Expand the **OpenPages | Applications | GRCM | FastMap | Key Fields** folder hierarchy.
   c. Navigate to the object type folder that you want and then expand the folder to see its settings.
   d. For each object type for which you want to define a lookup key, modify the following settings as needed:

Table 102. Lookup Key Settings

Setting Name	Description

Key	Used by FastMap to lookup objects when the name is not provided in a worksheet. Generally used in scenarios when objects are auto-named.
	
	The format is
	`field_group.field_name`
	
	Where:
	
	`field_group` is the name of the field group.
	
	`field_name` is the name of the object field.
	
	Example
	`ExternalSys_A.R_ID`
	
	If you have multiple fields, use a comma to delimit the fields. For example:
	`field_group.field_name,field_group.field_name`

Scoped	Used by FastMap to determine whether to lookup the value in the **Key** setting only under the parent objects or across all objects. If the value is set to: • **true** - the lookup is scoped only under parent objects. This is the default. • **false** - the lookup is not scoped and is across all objects.

e. Click a setting to open its detail page.
f. In the **Value** field, type a value.
g. When finished, click **Save**.

   The effect of the change is immediate.

3. In the FastMap template:
   a. For each field name that matches a `<field name>` value in the Key setting (from Step 2d), add a corresponding column to the template.
   b. Populate each corresponding column with values from your external system.
   c. When finished, import the template into FastMap.

Optimizing FastMap Performance

You can modify export and import settings to optimize FastMap performance.

Modifying Export Settings

Data is typically exported from a Filtered List View page for an object type, modified, and then imported back into FastMap. To optimize and control the export of data from a Filtered List View page, you can configure the following settings:

- **Maximum Export Size** - for details, see "Setting the Number of Objects for Export to Excel" on page 308.
- Concurrent Exports - for details, see "Setting the Number of Concurrent Export Requests" on page 308.

Modifying Import Settings

You can use the following settings to optimize FastMap import processing.

Limiting the Number of Rows for Import:

You can use the **Maximum Workbook Rows** setting to limit the number of rows that can be imported from a FastMap template.

By default, the value is set to 20000 rows (recommended maximum).

Note: Setting the number of rows for import above the recommended maximum of 20000 rows may result in slower performance and longer processing time. However, if you choose to set this value higher, then the processing timeout value in the **Transaction timeout** setting should also be increased (see "Setting a Transaction Timeout" on page 592 for details).

If the number of rows being imported exceeds the set value, then a validation error will be displayed stating that the workbook exceeds the allowable size.

Example

Let's say the 'Maximum Workbook Rows' setting has a value of 2500.

A user wants to import data into IBM OpenPages for Risk and Control objects. The workbook for the FastMap template contains:

- a worksheet for Risk objects with 1,000 rows of data
- a worksheet for Control objects with 2,000 rows of data
- a Definition worksheet with 5 rows of data

The total number of rows with data in the workbook is 3,005. Since the workbook exceeds the allowable size, a validation error will be displayed to the user.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages** | **Applications** | **GRCM** | **FastMap** folder hierarchy.
3. Click the **Maximum Workbook Rows** setting to open its detail page.
4. In the **Value** field, type a number greater than zero (for example, `2500`).
5. Click **Save**.

Setting a Transaction Timeout:

If you set the value in the **Maximum Workbook Rows** setting above the recommended maximum of 20000 rows, you can use the **Transaction timeout** setting to increase the maximum time a process can run before it times out and stops.

By default, the value is set to 7200 seconds (2 hours).

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages** | **Applications** | **GRCM** | **FastMap** folder hierarchy.
3. Click the **Transaction timeout** setting to open its detail page.
4. In the **Value** field, type a number greater than 7200 (the value represents seconds).
5. Click **Save**.

Adding a Processing Delay:

To reduce the processing impact of FastMap data imports on a system, you can use the **Process Delay** setting to set a delay in milliseconds between each record. If a value is set, the time to process the imported data will be extended.

By default, the value is set to 0 (zero).

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages** | **Applications** | **GRCM** | **FastMap** folder hierarchy.
3. Click the **Process Delay** setting to open its detail page.
4. In the **Value** field, type a number greater than zero.
5. Click **Save**.

Configuring Security and Cleanup for FastMap Import Templates

Securing FastMap Import Templates Stored on the Server

You can use the **Encrypt FastMap Files** setting to configure security on FastMap import templates that are stored on the server.

By default, the value is set to `true`, which encrypts FastMap import templates stored on the server.

Note: Before you change the value of the **Encrypt FastMap Files** setting, run the My FastMap Import Status report to verify that no FastMap import templates are pending processing (for details see "Accessing FastMap to Import Data and View Status" on page 564). If you change the value of this setting while FastMap processes are pending, the import will fail even if it the templates have passed data validation.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages** | **Applications** | **GRCM** | **FastMap** folder hierarchy.
3. Click the **Encrypt FastMap Files** setting to open its detail page.
4. In the **Value** field, type one of the following values.

   If the value is set to:

   - **true** - FastMap import templates are encrypted when stored on the server. This is the default.
   - **false** - FastMap import templates are not encrypted when stored on the server.
5. Click **Save**.

Cleaning Up FastMap Import Templates Stored on the Server

You can use the **Delete After Days** setting to configure the maximum number of days that a FastMap import template can remain on the server before it is automatically deleted.

FastMap import templates that will automatically be deleted from the server include templates that have:

- Finished processing - either successfully or with errors/warnings
- Exceed the maximum number of days specified in the **Delete After Days** setting. By default, this value is set to delete FastMap import templates after 1 day.

  Note: A FastMap import template that is older than the default value of 1 day will be automatically deleted regardless of whether or not the template has completed processing. We recommend a higher value for this setting if you upload large amounts of data using FastMap import templates.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages** | **Applications** | **GRCM** | **FastMap** folder hierarchy.
3. Click the **Delete After Days** setting to open its detail page.
4. In the **Value** field, type a number greater than zero. By default, this value is set to 1.
5. Click **Save**.

AFCON-generated FastMap Template Best Practices

If you use an IBM OpenPages Professional Services AFCON-generated FastMap template (in `.xls` format) to import data into the FastMap tool, you must add a Definition worksheet to the template for compatibility.

The Definition sheet should contain the following parameters and values:

- `firstDataRow` = [The first row from where the data starts]. This value is typically set to 11 for AFCON-generated templates.
- `useSystemNames = TRUE`
- `profileName` = [The name of the profile you are importing into]
- `inputDateFormat` = [Your date format]

If the IBM OpenPages Professional Services AFCON-generated FastMap template is using synonyms that are inconsistent with the object strings in the application, you must include the 'Synonyms' worksheet from `locale_support.xls` in your template. The worksheet must be labeled 'Synonyms', and you can specify the locale column to use by setting the `synonymsLocale` parameter on the Definition worksheet (see "Using the Definition Worksheet" on page 581).

A missing Definition worksheet in an IBM OpenPages Professional Services AFCON-generated FastMap template will result in validation errors, such as:

- Invalid Property Type errors for every property. For example,
  `Invalid Property Type. (RiskAssessment.Name)`
- Errors if autonaming is not enabled for an object type. For example,
  `Name cannot be blank`
- Errors about the parent object if autonaming is enabled for an object type. For example,
  `Parent not specified. (EL_11419)`

Appendix A. The Notification Manager

Overview of the Notification Manager

The Notification Manager is a JSP-based report and notification add-on utility for the IBM OpenPages GRC Platform (supports versions 3.0.1 and later) that automatically creates action items and notification e-mails when specified criteria are met.

With the Notification Manager, administrators can define a set of object properties and values that trigger the creation of an action item and send a notification e-mail to a user. The user responsible for the item will receive the e-mail and see the action item on their Home page, alerting the user to their necessary tasks.

For example, a notification event can be set to run nightly that will send a notification e-mail to all users who have Tests that do not have completed Test Results associated with them.

Why would I use Notifications?

Notifications allow you to alert people that important dates are approaching, and remind them that they still have outstanding tasks to perform before the date arrives. Since notification can be tied to the value of an object property, you can target the reminder to only those people who meet the criteria for the notification.

For example, you can set up a notification to remind all Control owners who have controls that have a value of "Undetermined" for the Control Evaluation field, and set the notification to start 20 days after the beginning of the quarter.

About Using the Notification Manager

Exploring the Notification Reports

When the Notification Manager is installed, a new folder on the IBM OpenPages server (typically `/opx`) is created under the `Publishing/Reporting/SOX` directory named "Notifications". This folder contains the reports and report templates required to set up a notification event. The contents of the folder are:

- **Test Notifications Page** (report) - This is a prepared report that will send e-mail to all Test Performers that have Tests that have not been performed and are due within the next 15 days.
- **Undetermined Controls Page** (report) - This is a prepared report that notifies users who have Controls assigned to them that are marked as "Undetermined".
- **Test Notification Template** - This report template is used when creating your own reports to notify Test Performers and Reviewers about incomplete Test Results.
- **General IBM OpenPages FCM Notifications Template** - This template is used to create your own notification reports using your own custom trigger conditions. Detailed information about creating your own notification reports can be found in “Using the General Notifications Template” on page 597 of this guide.

This guide will explain how to set up and run notification reports based on the included Test Notification Template and the General IBM OpenPages Notifications Template.

Requirements for Setting Up a Notification

In order to set up a notification event, you must have the following:

- A user account with the **Publishing** application permission set (see "Configuring Application Permissions" on page 18)
- Administrator access to the IBM OpenPages server machine (for scheduling reports to run automatically)
- Your notification mail server configured (see "Notification Manager Mail Server Settings" on page 325)

Tasks for Setting Up a Notification

The following tasks outline the process required for setting up and executing a notification:

- "Task 1: Prepare Your Data"
- "Task 2: Create the Notification" on page 597
- "Task 3: Trigger the Notification" on page 607

Once the steps for each task are completed, you will have a notification that can be run manually or scheduled to be run automatically, depending on your choices.

Results of Running a Notification Report

When a notification report is run, the following events occur (based on the setting you chose during the notification creation process):

- When the report is run, a milestone is generated with a name based on the report and the "Milestone Suffix" parameter.
- For each object that generates a notification, an action item is created under the report milestone. This action item is assigned to the Executive or Primary Owner of the object.
- A notification e-mail is generated for the Executive or Primary Owners detailing the objects that require attention.

Setting Up a Notification

Task 1: Prepare Your Data

Overview

The first step in setting up a notification is to make sure that your objects have the necessary information that will be required by the notification report. If the objects are not up-to-date, the report will not find the data it needs and will either return a sub-set of the entire results, or fail to run at all.

For example, when running the **Undetermined Controls** report, the report checks the Control Evaluation field for a value of "Undetermined". If your controls do not begin with a status of "Undetermined", the report will not be able to differentiate between legacy settings, and controls that have not been evaluated yet.

Using the Test Notification Template

If you plan to use notifications based on the Test Notification Template, or the provided Test Notifications report, you will need to make sure that your Tests have the following properties populated correctly:

- Test Reviewer (the person responsible for verifying that the tests are completed)
- Test Performer (the person responsible for executing the tests)
- Frequency (whether the test is performed Annually, Quarterly, or Monthly)
- Relative Due Date (when the test should be completed, measured in days after the beginning of the Frequency period)

Note: If you are viewing existing Tests that were created before version 3.0.1, the new properties will not be visible on the detail page of the Test. To display the new properties on an existing Test, click the **Edit** button. The new properties will be included on the Edit page. When you **Save** your changes, the new properties and values will now be displayed on the detail page. You will need to enter values for each pre-existing Test in order to use the Notification Manager.

Using the General Notifications Template

If you are creating notifications based on property values, make sure that the properties you are checking have valid values.

If you are creating custom properties and plan to run notifications based on those properties, make sure that you update all of the necessary objects with the new custom object field(s).

Note: The **General IBM OpenPages FCM Notifications Template** cannot compare date fields using the greater than/less than/equal/not equal operators.

Task 2: Create the Notification

Overview

The IBM OpenPages platform comes with the following templates for creating notification reports: **Test Notifications** and **General IBM OpenPages FCM Notifications**.

Reports created with the **Test Notification** template are targeted at Tests and are used to notify Test Performers and Reviewers that incomplete Tests exist. It also contains special logic to deal with setting relative due dates and gathering information from both Tests and Test Results.

The **General IBM OpenPages FCM Notifications** template allows users to set up to three properties and property values to evaluate. You can only evaluate properties for a single object type.

The following sections explain the various settings available to each type of notification report.

Creating a Notification

The steps in the following procedure apply to creating either a **Test Notification** or **General IBM OpenPages FCM Notifications** report.

Procedure

1. Log on to the IBM OpenPages server (typically /opx) as a user with **Publishing** privileges set.

2. Click the **Browse Channels** link under the **Publishing** heading on the Action menu to display the Channels page.
3. In the list on the **Channels** tab, click the **Reporting** link.
4. On the **Publishing** tab, navigate to the `SOX/Notifications` folder.
5. Click the **Add Page** button at the top of the folder list. The **Add a Page** screen is displayed.
6. Do the following:
   a. Enter a name and description for the notification report.
   b. Choose one of the following page templates:
      - **Test Notification** - use to create a notification based on test completion.
      - **General IBM OpenPages FCM Notifications** - use to create notifications of required work via e-mail and action items.
   c. Click **Next** to continue.
   d. Enter the information for your notification type.

      For detailed information about the various template fields, refer to the following tables:
      - For **Test Notification**, see "Understanding the Test Notification Fields"
      - For **General IBM OpenPages FCM Notifications**, see "Understanding the General IBM OpenPages FCM Notifications Fields" on page 602
   e. When finished, click **Apply** to save your changes.
7. When finished, click **Finish** to save the new report.

Understanding the Test Notification Fields

The following table contains an explanation of the various fields available to notification reports based on the **Test Notification** template.

Table 103. Test Notification Template Fields

Parameter	Description
Milestone Suffix	String appended to the milestone created as a result of running the report. When the report is run, a milestone is created to hold the action items that will be created as a result of the notification process. By default, the milestone is named for the content type that the report targets (in this case - Tests). The milestone suffix is added to the end of the milestone name to create a unique name for holding the results of the notification report. The name is appended with a dash, so a Milestone Suffix of "Weekly Reminder" will result in a milestone named "Tests - Weekly Reminder".
Sender Name	This is the name that will appear as the sender of the notification e-mail.
Sender Address	The e-mail address that appears as the sender e-mail address on the notification e-mail.
Subject	The subject of the notification e-mail. **Note:** This parameter can also contain a key defined under Application Text in the Configuration section of the Action menu in the IBM OpenPages application. This is required if you wish the notification e-mails to be sent in each recipient's selected locale.

Table 103. Test Notification Template Fields (continued)

Parameter	Description
Select a Test Frequency	Selecting a Test Frequency limits the notification report to only send out notifications for incomplete Tests that match the chosen frequency. Possible values are: Annually, Half-Yearly, Quarterly, Monthly, Weekly, Daily.
Notify Test Reviewer ___ days before due date	The number of days before the test due date that the notification e-mail will be sent to the user listed as the Test Reviewer. The Due Date for a Test is set in the Relative Due Date field on the Test object. The Relative Due Date is the number of days after the beginning of the test period (which is set in the 'Select a Test Frequency' field). For example, a Relative Due Date of 60 and a Frequency of Quarterly means that the Test must be completed 60 days after the beginning of the most recent quarter. If you set this field (Notify Test Reviewer...) to 14, then 14 days before the Relative Due Date the notification will alert the Test Reviewer. **Note:** The IBM OpenPages application considers financial quarters to begin on January 1st, April 1st, July 1st, and October 1st. If your financial quarter begins on a different date, you may want to adjust the Relative Due Date.
Notify Test Performer ___ days before due date	The number of days before the test due date that the notification e-mail will be sent to the user listed as the Test Performer. The Due Date for a Test is set in the Relative Due Date field on the Test object. The Relative Due Date is the number of days after the beginning of the test period (as set in Frequency - Annually, Half-Yearly, Quarterly, Monthly, Weekly, Daily). For example, a Relative Due Date of 60 and a Frequency of Quarterly means that the Test must be completed 60 days after the beginning of the most recent quarter. If you set this field (Notify Test Performer...) to 21, then 21 days before the Relative Due Date the notification will alert the Test Performer. **Note:** The IBM OpenPages application considers financial quarters to begin on January 1st, April 1st, July 1st, and October 1st. If your financial quarter begins on a different date, you may want to adjust the Relative Due Date to take this into account.

Table 103. Test Notification Template Fields (continued)

Parameter	Description
Also examine past ___ days when evaluating completeness	The number of previous days to check when looking for incomplete Tests. By default, the notification report only checks for the exact value of the "Notify Test Reviewer/Performer X days before due date" fields, so if the report is not run for a few days, some incomplete Tests with due dates that do not exactly match the values may not create notifications. This setting provides some overlap in case the report is not run every day. If an Action Item already exists for the Test, a new one will not be created.
Send repeat notifications	If this field is set to true, an e-mail will be sent to the Test Reviewer/Performer every time the notification report is run and the Test continues to be incomplete. If set to "false", the Performer/Reviewer will receive a single e-mail the first time the incomplete Test is included in the report results.
General Message	This text will appear as the introductory text in the body of the e-mail for both Test Performers and Test Reviewers. **Note:** This parameter can also contain a key defined under Application Text in the Configuration section of the Action menu in the IBM OpenPages application. This is required if you wish the notification e-mails to be sent in each recipient's selected locale.
Send mail to Test Reviewers	If set to "true", an e-mail message will be generated that contains the incomplete tests belonging to the Test Reviewer.
Message to Test Reviewers	This text will appear underneath the General Message on e-mails to Test Reviewers. **Note:** • The message text has a 200 character limit. • If you are entering a plain-text message, any escaped characters (such as new lines, etc.) must be preceded with two backslashes instead of one (e.g. \\n). If you are using HTML for your e-mail message, this is not necessary. • This parameter can also contain a key defined under Application Text in the Configuration section of the Action menu in the IBM OpenPages application. This is required if you wish the notification e-mails to be sent in each recipient's selected locale.
Send mail to Test Performers	If set to "true", an e-mail message will be generated that contains the incomplete tests belonging to the Test Performer.

Table 103. Test Notification Template Fields (continued)

Parameter	Description
Message to Test Performers	This text will appear underneath the General Message on e-mails to Test Performers. **Note:** • The message text has a 200 character limit. • If you are entering a plain-text message, any escaped characters (such as new lines, etc.) must be preceded with two backslashes instead of one (e.g. `\\n`). If you are using HTML for your e-mail message, this is not necessary. • This parameter can also contain a key defined under Application Text in the Configuration section of the Action menu in the IBM OpenPages application. This is required if you wish the notification e-mails to be sent in each recipient's selected locale.
Group notifications by	This setting is used to group the tests that meet the criteria for notification within the notification e-mail.
Test Reviewer property	Defines the property that contains the Test Reviewer user. Must be a property of the Test object that takes a group or user name as a value. Should only be modified if you are using a custom property.
Test Performer property	Defines the property that contains the Test Performer user. Must be a property of the Test object that takes a group or user name as a value. *Should only be modified if you are using a custom property.*
Test Due Date property	Defines the property that contains the Test Due Date. *Should only be modified if you are using a custom property.*
Test Frequency property	Defines the property that contains the Test frequency. *Should only be modified if you are using a custom property.*
Test Result Date Performed property	Defines the property that contains the date the Test Results were performed. *Should only be modified if you are using a custom property.*
Mail Server	The name of your mail server and domain. For example, `mail.mycompany.com`. If the value in the Mail Server field: • Is blank (no mail server name) - the value configured in the `\OpenPages\Applications\Common\Email\Mail Server` setting is used. This is the default. • Contains the name of a mail server - this value overrides the value configured in the `\OpenPages\Applications\Common\Email\Mail Server` setting. For more information about the `\OpenPages\Applications\Common\Email\Mail Server` setting, see "Setting the Address of the Mail Server" on page 325.

Table 103. Test Notification Template Fields (continued)

Parameter	Description
SOX Server	The full URL of the IBM OpenPages server machine. This address is used to create the links contained in the notification e-mail, and should NOT be set to *localhost*. If omitted, the server URL will be determined automatically.
Report Title	The text displayed as the title of the notification report.
Scope	The scope parameter is used to limit the range of the notification report. If you do not want to limit the scope of the notification report, leave it set to /_op_sox/Project/Default. If you wish to change the scope, click the **Browse** button and select the folder hierarchy you want to include in the notification report. Only the objects under that folder will be evaluated when the report is run.
Library Filter	When you are running a notification report, you do not usually want to include the Master Library in the report results, since they are not considered "active". If the path contains the value of the Library Filter parameter, it will not be included in the report results.
Project	Internal parameter. *Do not modify.*
Reporting Period	Internal parameter. *Do not modify.*

Understanding the General IBM OpenPages FCM Notifications Fields

The following table contains an explanation of the various fields available to reports based on the **General IBM OpenPages FCM Notifications** Template.

Table 104. General IBM OpenPages FCM Notifications Template Fields

Parameter	Description
Milestone Suffix	String appended to the milestone created as a result of running the report. When the report is run, a milestone is created to hold the action items that will be created as a result of the notification process. By default, the milestone is named for the content type that the report targets. The milestone suffix is added to the end of the milestone name to create a unique name for holding the results of the notification report. The name is appended with a dash, so a Milestone Suffix of "Weekly Reminder" might result in a milestone named "Process - Weekly Reminder".
Sender Name	This is the name that will appear as the sender of the notification e-mail.
Sender E-mail	The e-mail address that appears as the sender e-mail address on the notification e-mail.

Table 104. General IBM OpenPages FCM Notifications Template Fields (continued)

Parameter	Description
E-mail Subject	The subject of the notification e-mail. **Note:** This parameter can also contain a key defined under Application Text in the Configuration section of the Action menu in the IBM OpenPages application. This is required if you wish the notification e-mails to be sent in each recipient's selected locale.
General Message	This text will appear as the introductory text in the body of the e-mail for both Executive Owners and Primary Owners. **Note:** • The message text has a 200 character limit. • If you are entering a plain-text message, any escaped characters (such as new lines, etc.) must be preceded with two backslashes instead of one (e.g. \\n). If you are using HTML for your e-mail message, this is not necessary. • This parameter can also contain a key defined under Application Text in the Configuration section of the Action menu in the IBM OpenPages application. This is required if you wish the notification e-mails to be sent in each recipient's selected locale.
Send mail to Executive Owners	If set to `true`, an e-mail message will be generated and sent to the Executive Owner of the object that generated the notification. If no Executive Owner is set on the object, the Notification Manager will look up the hierarchy until a valid Executive Owner is found. If no Executive Owner is found, no notification will be generated.
Message to Executive Owners	This text will appear underneath the General Message on e-mails to Executive Owners. **Note:** • The message text has a 200 character limit. • If you are entering a plain-text message, any escaped characters (such as new lines, etc.) must be preceded with two backslashes instead of one (for example, \\n). If you are using HTML for your e-mail message, this is not necessary. • This parameter can also contain a key defined under Application Text in the Configuration section of the Action menu in the IBM OpenPages application. This is required if you wish the notification e-mails to be sent in each recipient's selected locale.
Send mail to Primary Owners	If set to `true`, an e-mail message will be generated and sent to the Primary Owner of the object that generated the notification. If no Primary Owner is set on the object, the Notification Manager will look up the hierarchy until a valid Primary Owner is found. If no Primary Owner is found, no notification will be generated.

Table 104. General IBM OpenPages FCM Notifications Template Fields (continued)

Parameter	Description
Message to Primary Owners	This text will appear underneath the General Message on e-mails to Primary Owners. **Note:** • The message text has a 200 character limit. • If you are entering a plain-text message, any escaped characters (such as new lines, etc.) must be preceded with two backslashes instead of one (e.g. `\\n`). If you are using HTML for your e-mail message, this is not necessary. • This parameter can also contain a key defined under Application Text in the Configuration section of the Action menu in the IBM OpenPages application. This is required if you wish the notification e-mails to be sent in each recipient's selected locale.
Send repeat notifications	If this field is set to `true`, an e-mail will be sent to the Executive and/or Primary owners every time the report is run and the object continues to meet the notification criteria. If set to `false`, the Executive and/or Primary owners will receive a single e-mail the first time the object is included in the report results. **Note:** If "Create Action Items" is set to `false`, then notification e-mails will be sent each time the report is run, regardless of the value of "Send repeat notifications".
Content type to send notifications for	Determines which objects will be evaluated when the report is run. Notification reports can only be run against a single object type. If you want to run the same report against multiple object types, you will have to create multiple reports, or provide different parameter values in the command line.

Table 104. General IBM OpenPages FCM Notifications Template Fields (continued)

Parameter	Description
Filter Property *n* Filter Evaluation *n* Filter Value *n* Where: *n* is a number	The report template contains three sets of Property/Value evaluations that can be performed when determining which objects will generate a notification. **Where:** • Filter Property *n* - Contains the property to be considered when evaluating whether a notification should be generated. • Filter Evaluation *n* - The evaluation method to be used when comparing the object property value with the Filter Value. **Note:** The possible operators are =,<> (not equals), <, >, <=, and >=. Only the "=" operator can be used with strings. All other operators only work with integers. • Filter Value *n* - Contains the value of the property to be considered when generating notifications. Example If the three parameters have the following values: Filter Property 1: `OPSS-Control.Operating Effectiveness` Filter Evaluation 1: = Filter Value 1: `Not Determined` then a notification would be generated if any Control had a value of 'Not Determined' selected for the 'Operating Effectiveness' object field.
Create notification if	Determines whether all property/value evaluations need to be `true` in order to create a notification, or if only one of them needs to be `true`.
Group Notifications by	This setting is used to group the objects that meet the criteria for notification within the notification e-mail.
Create Action Items	Determines whether an action item will be created for each notification e-mail sent to an Executive or Primary Owner. If an Action Item has already been created for the object, no new action item will be generated **Note:** If this option is set to `false`, then notifications will always be sent when the notification report is run, regardless of the "Send repeat notifications" setting.
Action Item Description	An optional description for the created Action Items.
Action Item should be completed in	If set, the Action Item's Due Date will be set to the number of days after the creation of the action item. For example, a value of 14 would give the created Action Item a due date two weeks after the creation of the Action Item.

Table 104. General IBM OpenPages FCM Notifications Template Fields (continued)

Parameter	Description
Mail Server	The name of your mail server and domain. For example, `mail.mycompany.com`. If the value in the Mail Server field: • Is blank (no mail server name) - the value configured in the `\OpenPages\Applications\Common\Email\Mail Server` setting is used. • Contains the name of a mail server - this value overrides the value configured in the `\OpenPages\Applications\Common\Email\Mail Server` setting. For more information about the `\OpenPages\Applications\Common\Email\Mail Server` setting, see "Setting the Address of the Mail Server" on page 325.
SOX Server	The full URL of the IBM OpenPages server machine. This address is used to create the links contained in the notification e-mail, and should NOT be set to *localhost*. If omitted, the server URL will be determined automatically.
Report Title	The text displayed as the title of the notification report.
Executive Owner Property	The property containing the Executive Owner value. Should not be changed unless you are using a custom Owner field. Valid values can be obtained by looking at the profile for the object selected in "Group Notifications by" above. In the Object Fields table on that page, concatenate the value under "Field Group" with the value under "Name". For example, "SOXBusEntity.Executive Owner" or "System Fields.Last Modified By". You should only use properties that can take a user name or group as a value.
Primary Owner Property	The property containing the Primary Owner value. Should not be changed unless you are using a custom Owner field. Valid values can be obtained by looking at the profile for the object selected in "Group Notifications by" above. In the Object Fields table on that page, concatenate the value under "Field Group" with the value under "Name". For example, "SOXBusEntity.Executive Owner" or "System Fields.Last Modified By". You should only use properties that can take a user name or group as a value.
Library Filter	When you are running a notification report, you do not usually want to include the Master Library in the report results, since they are not considered "active". If the path contains the value of the Library Filter parameter, it will not be included in the report results.
Scope	The scope parameter is used to limit the range of the notification report. If you do not want to limit the scope of the notification report, leave it set to /_op_sox/Project/Default. If you wish to change the scope, click the **Browse** button and select the folder hierarchy you want to include in the notification report. Only the objects under that folder will be evaluated when the report is run.

Table 104. General IBM OpenPages FCM Notifications Template Fields (continued)

Parameter	Description
Project	Internal parameter. *Do not modify.*
Reporting Period	Internal parameter. *Do not modify.*

Task 3: Trigger the Notification

You can run notification reports from the Reporting interface like any other report, or you can use the provided command line interface to run the notification reports from outside the IBM OpenPages GRC Platform environment.

You need to provide access (minimum Read, Write access) to **Milestone** and **Task** folders for all the users who need to run notification reports successfully. Notification reports in the **Reporting** menu require access to the **Milestone** folder, which is the container for Project Milestone objects (SOXMilestone), and access to the **Task** folder, which is the container for Project Action Item objects (ProjectActionItem). By default, both SOXMilestone and ProjectActionItem are custom ACL Object Types (based on the **OpenPages | Common | Custom ACL Object Types** setting). For instructions on setting up access for these objects, see "Creating an Access Control List" on page 50.

Using the Application User Interface

Running a notification report from the IBM OpenPages application user interface works the same as running any other report through the user interface.

Note: You cannot use the "Preview" functionality in the IBM OpenPages user interface with Notification reports.

Procedure

1. Log on to the IBM OpenPages application and click the **Reporting** menu on the menu bar.
2. Click the **Notifications** submenu to display the notification reports.
3. Choose the notification report you want to run and click the name of the report.

   The results of the report are displayed in a new browser window.

Using the Command Line Interface

You can manually run the NotificationManager from a command or shell window, or you can use standard operating system scheduler functions to automatically run the NotificationManager command file at a specified time. For example, in Windows, you could use the built-in Windows scheduler, in AIX, you could set up a cron job.

You can run a single report, an entire folder of reports, and run a single report against multiple datasets by providing parameters to the report directly through the command line.

The NotificationManager command file is named as follows:

Windows
`NotificationManager.cmd`

AIX `NotificationManager.sh`

The file is located in the <OP_Home>|bin directory of your IBM OpenPages installation.

Where: <OP_Home> represents the installation location of the IBM OpenPages GRC Platform application. By default, this is:	
Windows	C:\OpenPages
AIX	/opt/OpenPages

The following section details the allowable parameters that can be used with the NotificationManager command line interface.

Syntax:

```
NotificationManager -Username <user_name> -Password <password>
-NotificationProgram <full_path_to_notification_report>|-ProgramFolder
<path_to_folder-containing-notification-reports> [-SaveOutput <true|false>]
[-LogSession <true|false>]
[-<parameter_name> <parameter_value>] [-ParameterFile <full_path_to_file>]
```

Parameters:

All parameters are in the syntax -parameter "value or string". If the value of any parameter contains spaces, that value must be contained within quotation marks.

Table 105. Notification Manager Parameters

Parameter	Description
-Username	The name of a valid IBM OpenPages user with permission to run the notification reports.
-Password	The password for the user name set in -Username.
-NotificationProgram	(Required unless -ProgramFolder is specified) The full path to the notification report the command will run, starting with the Reporting channel. Should not begin with a leading slash. **Example** -NotificationProgram "Reporting\SOX\Notifications\ Test Notifications Report"
-ProgramFolder	(Required unless -NotificationProgram is specified) Specifies a folder containing notification reports. All reports in that folder will be executed when the command is run. **Example** -ProgramFolder "Reporting\SOX\Notifications"
-SaveOutput	(Optional) Can be **true** or **false**. If set to true, the output of the report will be saved to an output file in the output_files directory under the |bin|NotificationManager directory. If the parameter is not present, no output file will be created. The file name is the name of the notification report (or folder) with an "html" extension. If an output file with that name already exists, a timestamp extension will be added to the end of the existing file's name and the older file will be moved to the output_files|archive folder. **Example** Undetermined Controls.html.200406060103

Table 105. Notification Manager Parameters (continued)

Parameter	Description
-LogSession	(Optional) Can be set to **true**. If set, the activities of the NotificationManager will be written to a log file. The log file will be located in the `logs` directory under the `|aurora|bin|NotificationManager` directory. The name of the log file is `NotificationManager.log`. The file has a maximum size of 1 MB, and will be rotated into the `|logs|archives` directory when the limit is exceeded.
`-<parameter_name> <parameter_value>` **Where:** `<parameter_name>` *is the name of a specific parameter* `<parameter_value>` *is the value of that parameter*	(Optional) If you want to pass a value for a specific notification report parameter, you can include the parameter and value directly in the command line. The parameter name must match the report parameter name exactly. The parameter names can be viewed by logging on to the IBM OpenPages server interface (typically opx) and navigating to the channel folder containing the report page. The parameter names are shown in the detail page for the report, which can be viewed by clicking on the name of the report in the channel folder view. **Examples** • `-mailServer mail.openpages.com` • `-generalMessage "Please do not ignore this e-mail."`
-ParameterFile	Specifies a text file containing a list of parameter value pairs (equivalent to entering individual `-parameter "value or string"` entries into the command line directly). Each parameter value pair should be on a single line. Value is the full path to the file, including the file name. **Example** - for Windows: `-ParameterFile "c:\OpenPages\bin\NotificationManager \notification_parameters.txt"`

Appendix B. Installing and Configuring HTTP Compression

This appendix applies to Microsoft Windows IIS 7 only and is a one-time setup for HTTP compression on the CommandCenter server.

This appendix contains the following topics:

- "Installing HTTP Compression"
- "Configuring HTTP Compression"

Installing HTTP Compression

HTTP compression is usually available on the default installation of IIS 7. However, only static compression is installed by default.

To verify and/or install static or dynamic compression, use the following steps.

Procedure

1. On the CommandCenter server:
   a. Click the Windows **Start** menu and point to **Administrative Tools**.
   b. Select **Server Manager**.
2. In the Server Manager hierarchy pane:
   a. Expand Roles.
   b. Click Web Server (IIS).
3. In the Web Server (IIS) pane, verify if compression is installed:
   a. Scroll to the Role Services section.
   b. Under Performance, verify whether Static Content Compression and/or Dynamic Content Compression are installed.
   c. If these are installed, skip the remaining steps in this procedure and go to "Configuring HTTP Compression." Otherwise, proceed to the next step.
4. To add static or dynamic content compression, click the **Add Role Services** link.
5. On the Select Role Services page of the Add Role Services Wizard:
   a. To install:
      - Dynamic compression, select **Dynamic Content Compression**.
      - Static compression, select **Static Content Compression**.
   b. Click **Next** to continue.
6. On the Confirm Installation Selections page, click **Install**.
7. On the Results page, click **Close**.

Configuring HTTP Compression

To configure HTTP compression for Windows IIS 7, use the following steps.

Procedure

1. On the CommandCenter server, click the Windows **Start** menu and select **Control Panel**.
2. Open Administrative Tools as follows:

a. Do one of the following:

For Windows Server...	Do this...
2008	Click **System and Maintenance**.
2008 R2	Click **System and Security**.

b. Click the **Administrative Tools** link.

3. In the Administrative Tools window, double-click **Internet Information Services (IIS) Manager**.
4. In the Connections pane, select the server name.
5. In Features View, under 'IIS', double-click **Compression**.
6. In the Compression pane:
   a. Select 'Enable static content compression' to configure IIS to compress static content.
   b. Under Static Compression, select 'Only compress files larger than (in bytes)' and enter 150 in the box.
   c. Select 'Per application pool disk space limit (in MB)' and enter 1000.
   d. In the Actions pane, click **Apply**.
7. In the Connections pane:
   a. Expand Sites > Default Web Site.
   b. Select the name of the Cognos folder (for example, c8).
8. In Features View, under 'IIS':
   a. Double-click **Compression**.
   b. Select both 'Enable dynamic content compression' and 'Enable static content compression'.
   c. In the Actions pane, click **Apply**.
9. Add the mime types of the files to be compressed as follows:
   a. Open Windows Explorer and navigate to <System Drive>:/Windows/System32/inetsrv/config/.
   b. Create a backup of the applicationHost.config file:
      1) Copy and paste the applicationHost.config file into the same or different folder.
      2) Rename the copied file to applicationHost.config.bak.
   c. In a text editor (such as Notepad), open the applicationHost.config file and find the httpCompression tag.
   d. Use the sample code that follows to verify the static and dynamic mime types, and add any missing mime types to the file (such as xml, xml-dtd, vnd.ms-excel, and octet-stream).

```
<httpCompression directory="%SystemDrive%\inetpub\temp\IIS
 Temporary Compressed Files" maxDiskSpaceUsage="1000"
 minFileSizeForComp="0">
            <scheme name="gzip" dll="%Windir%\system32\inetsrv\gzip.dll" />
            <staticTypes>
                <add mimeType="text/*" enabled="true" />
                <add mimeType="message/*" enabled="true" />
                <add mimeType="application/x-javascript" enabled="true" />
                <add mimeType="application/atom+xml" enabled="true" />
                <add mimeType="application/xaml+xml" enabled="true" />
                <add mimeType="application/xml" enabled="true" />
                <add mimeType="application/xml-dtd" enabled="true" />
                <add mimeType="*/*" enabled="false" />
            </staticTypes>
```

```
        <dynamicTypes>
            <add mimeType="text/*" enabled="true" />
            <add mimeType="message/*" enabled="true" />
            <add mimeType="application/x-javascript" enabled="true" />
            <add mimeType="application/vnd.ms-excel" enabled="true" />
            <add mimeType="application/octet-stream" enabled="true" />
            <add mimeType="*/*" enabled="false" />
        </dynamicTypes>
    </httpCompression>
```

e. When finished, save the changes to the file.

10. Return to the IIS Manager, and then stop and restart the IIS service.

Appendix C. Legacy Reporting Framework Generation Settings

Note: Information in this appendix applies only to systems that have been upgraded from versions of OpenPages 5.x or earlier and are using the Legacy Reporting Framework.

About Namespaces in the Legacy Reporting Framework

If the Legacy Framework is enabled, a relational data model is generated under the `OPENPAGES_DEFAULT` legacy namespace. The folder path to the `OPENPAGES_DEFAULT` legacy namespace is:

`OpenPages|Platform|Reporting|Framework|Generation|Namespaces`

Each non-default legacy framework namespace contains the following required entries:

Procedure

1. **Folders** - this folder contains a **Reporting Periods** subfolder with entries for **Items** and **Name**. These entries are used by the framework generator and should not be changed.
2. **BY_RELATIONSHIPS** - this entry is only used for non-default namespaces. If no 'BY' relationships are required, you can leave this entry blank.
3. **Is Default** - in the supplied (out-of-the-box) framework model, the value of the `DEFAULT` namespace is set to `true` and should not be changed. All other IBM OpenPages supplied namespaces are defined as non-default namespaces. All new namespaces that are added should also be defined as non-default (value is set to false) namespaces.
4. **Is Enabled** - in the supplied (out-of-the-box) framework model, this setting determines whether or not the namespace is generated in the reporting framework. By default, this value is set to true.
5. **ObjectModel 1** - if your object model (schema) ***includes*** **Control Objectives**, the framework generator uses the value pairs in this entry to define the parent-child relationships in the generated framework model that includes Control Objectives in the object hierarchy. This entry requires values and must include all recursive object relationships.
6. **ObjectModel 2 -** if your object model (schema) ***excludes*** **Control Objectives**, the framework generator uses the value pairs in this entry to define the parent-child relationships in the generated framework model that does not include Control Objectives in the object hierarchy. This entry requires values and must include all recursive object relationships.

Results

The CommandCenter framework generator uses the definition of a namespace (from **ObjectModel 1** and **ObjectModel 2**) to create corresponding namespaces in the framework model. The table below lists the relationship between objects when a namespace is generated.

Table 106. Namespaces and Object Relationships

If a relationship defined in a namespace does this...	and the namespace is a...	Then the framework generator...
matches a relationship that is defined in the object model	default namespace	automatically creates a direct relationship between these objects
	non-default namespace	
excludes a relationship that is defined in the object model	default namespace	automatically creates an associative 'BY' relationship between these objects
	non-default namespace	creates an associative 'BY' relationship between these objects only if the BY_RELATIONSHIPS entry contains value pairs. If the BY_RELATIONSHIPS entry is blank, then no 'BY' relationships are created.

Defining a New Non-Default Namespace in the Legacy Reporting Framework

When you create a new non-default namespace, you initially create a container (folder) that must be populated with the required namespace entries. You can use the copy operation to copy these entries from an existing non-default namespace into the new namespace.

About Legacy Reporting Framework Custom Namespace Names

The following list contains best practices to keep in mind when naming legacy reporting framework namespaces:

- Use all capital letters in the namespace name.
- Use an underscore - no spaces - in the name.
- Do not use `OPENPAGES_` as a prefix for the new namespace as this is reserved for the supplied (out-of-the-box) namespace names.

Do not use `_DEFAULT` as a suffix for the new namespace as this is reserved for the supplied (out-of-the-box) IBM OpenPages default namespace name.

Adding a New Non-Default Namespace to the Legacy Reporting Framework

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Set the value in the **Show Hidden Settings** setting to `true` (for details, see "Showing Hidden Settings" on page 273).
3. Expand the **OpenPages** | **Platform** | **Reporting** | **Framework** | **Generation** | **Namespaces** folder hierarchy.
4. Select the box next to the **Namespaces** folder, and then click the **Add Folder** button.
5. In the **Add Folder** box, type a name for the new namespace. For example, MYCOMPANY_NAMESPACE.

The newly created non-default namespace is represented by a folder icon under the **Namespaces** folder.

6. Copy the required entries into the new non-default namespace folder as follows:

   Important: Use entries from any non-default namespace for the copy operation; do not select any entries from the DEFAULT namespace.

   a. Select a **Folders** entry from any non-default namespace.
   b. Click the **Copy To** button.
   c. In the copy window, select the name of the new namespace folder (for example, MYCOMPANY_NAMESPACE).
   d. Click **OK**.
   e. Repeat Steps a - d for each of the following entries: **BY_RELATIONSHIPS**, **Is Default**, **ObjectModel 1**, and **ObjectModel 2**.

7. Verify the value of the **Is Default** entry is false. If the value is set to true, then change the value.
8. Modify the values of the **ObjectModel 1** and **ObjectModel 2** entries to reflect any new parent-child object relationships you may have defined for your reports.

   Note: You must include all recursive objects (business entities, sub-processes, sub-accounts, and sub-mandates) in both **ObjectModel 1** and **ObjectModel 2** entries.

   The syntax for adding parent-child object relationships is:

   <parent object>|<child object>,<parent object>|<child object>

   Example

   The following example shows the values you would use to add recursive objects to the **ObjectModel 1** and **ObjectModel 2** entries:

   SOXBusEntity|SOXBusEntity,SOXSubprocess|SOXSubprocess,SOXSubaccount|SOXSubaccount,Submandate|Submandate

9. Define any 'BY' relationship values in the **BY_RELATIONSHIPS** entry.

   The syntax for adding 'BY' object relationships is:

   <parent object>|<child object>,<parent object>|<child object>

   Example

   The following example shows the values you could use if you wanted parent-child 'BY' relationship between Application and Control objects, Personnel and Control objects, and Infrastructure and Control objects:

   Application|SOXControl,Personnel|SOXControl,Infrastructure|SOXControl

   When the framework model is generated, the framework generator will create 'BY' relationship query subjects from the values in this entry.

10. Reset the value in the **Show Hidden Settings** setting to false.
11. When you are finished, regenerate the framework model. For details, see "Updating the Reporting Framework" on page 64.

    Once the framework generation has completed, the new namespace will be available in CommandCenter to report authors.

Editing an Existing Legacy Reporting Framework Namespace

You can modify the values contained in an existing namespace so that namespace satisfies your reporting requirements.

Important: We do not recommend changing the relationships of any IBM OpenPages supplied (out-of-the-box) namespaces.

Procedure

1. Access the Settings page (see "Accessing the Settings Page" on page 268).
2. Expand the **OpenPages | Platform | Reporting | Framework | Generation | Namespaces** folder hierarchy.
3. Expand the namespaces folder you want to modify.
4. Change the following entries as required: **BY_RELATIONSHIPS**, **ObjectModel 1**, and **ObjectModel 2**.
5. When you are finished, regenerate the framework model. For details, see "Updating the Reporting Framework" on page 64.

Results

Once the framework generation has completed, the modified namespace will be available in CommandCenter to report authors.

Appendix D. Non-Role Based Access Control

For backward compatibility with IBM OpenPages Governance Platform 5.1x (and earlier), this appendix is provided for your reference.

About Non-Role Based Access Controls

Important: For flexible role-based security administration, OpenPages highly recommends that you migrate your access control data to the role-based security model (for details, see "About Role-based Security Models" on page 33). For assistance with upgrading your system, contact your IBM representative.

Using non-role based security, administrators can grant or deny read, write, delete, and associate permissions to groups or specific users based on folders. These permissions are set using an Access Control List, or ACL. An ACL is the list of groups and users who have permissions for the specified folder. You can explicitly set permissions on folders or inherit permissions from a parent folder.

This section provides an overview of the procedures involved in setting up security for non-role based access control, which can be set to control the ability to read, write, delete, and associate the objects in a folder. Each of these settings can be set individually, allowing fine-level control over user and group access to the contents of a folder. Any folders that contain IBM OpenPages Governance Platform 5.1x (and earlier) objects (business entities, accounts, risks, etc.) can be administered through ACLs.

Note: Non-role based security access control can only be set at the folder level. Individual objects within a folder cannot have ACLs - they automatically assume the ACL of the folder. If you have permissions for one item in a folder, you have the same permissions for the other objects in that folder.

Using ACLs with Top-Level Folders

When setting up your business entity and other object hierarchy, certain folders are already created for you by the IBM OpenPages installation. These folders are created with pre-set ACLs, and should not be modified.

Make sure you do not modify the ACLs for the following folders:

```
Default
   BusinessEntity
   ICDocumentation
   Issue
   IssueActionItems
   Plan
Files and Forms
```

The Object Folder Structure

When the object hierarchy is viewed from the application interface, the folder structure is listed in alphabetical order, unlike the overview screens, which display relationships.

Business entities are contained in their own folder, while all of the other object types have their own folder underneath the Documentation folder.

Note: ACLs should never be added to folders that were automatically created during installation (e.g., ICDocumentation, BusinessEntity, etc.). Always create ACLs using the IBM OpenPages administrative user interface.

When you add a new business entity called Enterprise, a folder with the name of the business entity is created underneath the *BusinessEntity* folder.

When you add a sub-entity named "Region" to the "Enterprise" entity, a corresponding folder is created.

When you add other objects to a business entity hierarchy, the folder structure of the business entities it belongs to is automatically created under the object type folder. All objects of that type created for that business entity are placed in the same folder.

Important: When you are setting ACLs, it is important to remember to set ACLs for the business entity folders under the *ICDocumentation* folder structure, as well as the *Business Entity* folder structure. If you do not, when you try to access the objects you will not be able to browse to the objects. You should never set ACLs on the container folders (e.g., *ICDocumentation, BusinessEntity*).

Accessing the Access Control Page

Only an IBM OpenPages Super Administrator can access the **Custom Security** menu item.

Procedure

1. Log on to the IBM OpenPages application as a Super Administrator user with the **Access Control Lists** application permission set.
2. From the menu bar, select **Administration** and click **Custom Security**.

Using Inheritance with Access Control Lists

By default, in a non-role based access control environment, the object folder hierarchy inherits security ACLs from the folders above them. If a folder does not have an ACL set for a particular group, the application looks back up the folder tree until it finds an ACL for that group and uses it for the current folder. By default, all users can edit any object in the entire project.

This setup is extremely useful for smaller projects, where there is a single (or very few) teams all working on the same business entity structure. In the odd case where you have specific users who are denied viewing or editing permissions, you can easily deny them access to a particular folder structure by setting an explicit ACL for the group or user that denies them access.

However, this paradigm rapidly becomes unwieldy for large numbers of groups or business entities. If you only want a group to see one particular region or site out of 50, it is much simpler to grant access to the single site than to deny access to the other 49.

Breaking Inheritance

Using the IBM OpenPages application user interface, you can break the inheritance property on any folder. When you break inheritance, access is limited to ONLY the groups and users who have an ACL for that business entity. All other groups and users (besides the creator of the object) are automatically set to Denied/Denied/Denied/Denied.

For large teams and projects who wish to restrict which areas of the project can be seen or modified, breaking the inheritance "chain" is very helpful, since it automatically denies all groups and users access to the particular business entity structure. Only the groups and users specifically included in an ACL have access to the business entity children.

Instead of denying a group access to 49 sites, as in the example above, now you only have to grant access to the desired site, and the other 49 are denied by default.

Note: Breaking inheritance is not without its drawbacks. Because all groups (except OpenPagesAdministrators and OPAdministrators) are denied access to the business entity, groups that do not have an ACL entry cannot see the business entity or any object underneath the business entity. This is true even if an ACL entry for a specific group is added to a sub-entity. Because the group (or user) is denied Read access at the parent business entity, they cannot browse the tree to view the sub-entity where they have access. The following sections will explain how to circumvent this restriction using nested groups.

To break the inheritance on a folder:

Important: Once you break the inheritance on a folder, the new permissions (or lack thereof) go into effect immediately. Only members of the OpenPagesAdministrators and OPAdminstrators groups will be able to access the object, unless a specific ACL for a user or group is created.

Procedure

1. Access the Access Control page (see “Accessing the Access Control Page” on page 620).
2. Navigate to the business entity folder where you want to break inheritance (under the *Default* directory).
3. When you have found the desired folder, click the name of the folder to display the detail page.
4. Click **Add** and choose the desired group or user from the list.
5. Choose the desired permissions for the group or user by highlighting the appropriate entries and click the **OK** button to add the new ACL to the folder.
6. Now that a valid ACL exists for the folder, click the **Disable Inheritance** button under the Folder heading. The value of the "Inherit ACL" field is changed to "false" and the **Disable Inheritance** button changes to **Enable Inheritance**.
7. Click **Access Controls** in the breadcrumb trail to return to the Access Controls folder list.

Results

Remember, no one except the groups (and sub-groups of those groups) listed in the Access Controls table will be able to see the folder or its contents.

Note:

- The OpenPagesAdministrators group and the creator of a folder or object is exempt from ACL restrictions. The creator always has Delete access to files and folders he or she has created, while the OpenPagesAdministrators group has total access to all files and folders.
- If you have broken inheritance for a folder, there will be entries for the OpenPagesAdministrators and OPAdministrators groups. These ACLs cannot be edited or deleted.

Creating a New ACL on a Folder

You must have the **Access Control Lists** application permission to view or edit ACL settings.

Procedure

1. Access the Access Control page (see "Accessing the Access Control Page" on page 620).
2. Navigate to the folder in which you want to create a new ACL. Click the folder name to display the detail page of the folder.
3. Click **Add** to add a new access control to the list.
4. In the Create an Access Control Setting page, choose the desired group or user from the drop-down list.
5. Select the desired permissions by highlighting the appropriate choices and clicking **OK** when finished. The dialog closes, and the new ACL appears in the list area of the folder detail page.

   Read permission is required for Write and Associate access, and Write access is required in order for Delete access to be granted. You can select any combination of permissions, but when you save the ACL, it will be modified to be a valid combination of permissions.

   For example, if you set Read/Write/Delete/Associate to Denied/Granted/Granted/Granted, when you click **OK**, the displayed permissions will be Granted/Granted/Granted/Granted. Because users must have Read permissions in order to have Delete permissions, the Read permission is changed to "Granted".

   In order to set Read to Denied, Write, Delete, and Associate must also be set to Denied.
6. Once you have finished setting the permissions, click the **Access Control** link in the Action menu to return to the Access Control list.

Editing an Existing ACL

You can edit an existing ACL.

Procedure

1. Access the Access Control page (see "Accessing the Access Control Page" on page 620).
2. Click the folder name to display the detail page with the list of existing ACLs.
3. Click the check box next to the existing ACL you wish to modify and click the **Edit** button to display the Edit an Access Control Setting page.
4. Select the desired permissions by highlighting the appropriate choices and clicking **Save** when finished. The dialog closes, and the updated ACL appears in the list area of the Access Control page.

Read permission is required for Write and Associate access, and Write access is required in order for Delete access to be granted. You can select any combination of permissions, but when you save the ACL, it will be modified to be a valid combination of permissions.

For example, if you set Read/Write/Delete/Associate to Denied/Granted/Granted/Granted, when you click **Ok**, the displayed permissions will be Granted/Granted/Granted/Granted. Because users must have Read permissions in order to have Delete permissions, the Read permission is changed to "Granted".

In order to set Read to Denied, Write, Delete, and Associate must also be set to Denied.

For example, if you set a folder ACL for a group to Granted for Read, and leave Write and Delete blank, they will be shown in the UI as Granted/Inherited/Inherited. However, if you set the permissions to Granted for Delete, and left Read and Write blank, the ACL is displayed as Granted/Granted/Granted, since Delete requires Read and Write permissions.

Deleting an Existing ACL

You can delete an existing ACL.

Procedure

1. Access the Access Control page (see "Accessing the Access Control Page" on page 620).
2. Navigate the folder tree to display the folder containing the ACL you want to delete.
3. Click the folder name to display the detail page with the list of existing ACLs.
4. Click the check box next to the existing ACL you wish to remove and click the **Delete** button to remove the ACL.

Using Groups to Establish User Roles

User groups fulfill three functions - to segregate users into meaningful subsets, to define ACLs to limit both the range of actions that can be performed on a folder's contents, and to limit the scope of a user's activity to a specific folder or set of folders. In this section, we will examine how groups can be used to separate a set of users into different roles within an organization.

The "Core" IBM OpenPages Governance Platform 5.1x (and earlier) Groups

The IBM OpenPages Governance Platform 5.1x (and earlier) application has two predefined user groups already created as part of the initial installation. These groups are:

- **OpenPagesApplicationUsers** - This group is a container for all users who are part of the IBM OpenPages Governance Platform 5.1x (and earlier) application. Every IBM OpenPages Governance Platform 5.1x (and earlier) user will be a part of this group through inheritance. The OpenPagesApplicationUsers group has a single sub-group - OpenPagesAdministrators.

  Note: The OpenPagesApplicationUsers group should never be used to set ACLs on any folder. The group exists for administrative purposes only.
- **OpenPagesAdministrators** - In order to have administrative-level permissions, users must be part of this group. Administrators can customize reports, create

users and groups through the IBM OpenPages Governance Platform 5.1x (and earlier) user interface, and assign and modify ACLs. They also have access to all folders and objects in the IBM OpenPages Governance Platform 5.1x (and earlier) hierarchy, regardless of ACLs.

Example: Using Groups to Establish User Roles

Widgets, Inc. has decided that they will divide their IBM OpenPages Governance Platform 5.1x (and earlier) users into four main teams, each responsible for a different area of their financial controls documentation project. These four teams are:

- **The Executive Team**. These are people who do not document or modify individual objects. As a team, they are only interested in viewing the entire financial controls documentation process as a whole, and quantifying the results. CFOs and high-level corporate users fall into this category. They need read access to almost all folders in order to run reports on the documentation project as a whole.
- **The System Team**. This group is responsible for setting up and maintaining the entire hierarchy of IBM OpenPages Governance Platform 5.1x (and earlier) objects. They are also the only ones allowed to modify anything above the control level. In most companies, the IT department or a sub-set of the central accounting team is responsible for these activities.
- **The Regional Teams**. These groups are responsible for developing, maintaining, and overseeing the objects for all of the sites within their regions.
- **The Site Teams**. These groups are responsible for documenting the controls for their sites, as well as uploading test results and control documents.

The Executive and System teams are both based in the Corporate Center, while the Regional Teams and Site Teams are located in their respective regional and site headquarters.

Although you can have user groups that correspond to the entire team, they are not necessary when setting ACLs. However, so-called "team" groups can be helpful for organizational purposes as well as assigning tasks or other uses. The important groups within each team will divide the teams according to the level of interaction (Reading, Writing, Deleting, Associating) they will be allowed, as well as the scope of the folders they can act on. These groups will be explained in the following sections.

Using Groups to Limit User Activities

Groups are used in folder ACLs to limit what each group of users can do to the objects located in the folder. In general, you will want a group of users who are limited to just viewing the objects, a group who can both view and edit the objects, and another group who can view, edit, associate and delete the objects.

In the following sections, we will divide each team into subgroups with different access permissions.

The Executive Team

The Executive team is interested mainly in the overall status of the financial controls documentation project, and gathers most of their information by running reports on the various objects and drilling down into the objects via the report links. As such, they only need read access to objects, but their scope needs to be extremely wide.

Some possible sub-groups of the Enterprise team are:

- FinancialOfficers
- ExternalAuditors
- InternalAuditors

In the case of the Executive Team, the sub-groups are merely organizational in nature. However, by making them sub-groups of the Executive Team group, you gain the flexibility of categorizing the Executive users by roles without adding complexity to your ACL definitions.

All of the sub-groups require the same access to the object hierarchy - they only need Read access in order to run reports and view individual objects from those reports. As an organizational grouping, the ExecutiveTeam group will not appear in any ACLs directly - rather, it will be added as a member of many other groups with read-only access.

Once you have created your Executive Team sub-groups, add the appropriate users to each sub-group. Users should NOT be added directly to the ExecutiveTeam group - add them to a sub-group instead.

The Regional Teams

Each Regional team (one for each region) is responsible for reviewing and maintaining the objects that are specific to the sites in their region. In function, they are quite similar to the System team, but their influence is limited to all of the sites in their region.

The various sub-groups for the Regional teams are actually two levels - first you need an "umbrella" RegionalTeams group. Under that group, you need to create sub-groups for each region.

For example:

- **Region01Reviewers** - responsible for reviewing and reporting on all of the sites in Region 01. They require Read access to everything in Region 01.
- **Region01Writers** - responsible for making any necessary changes to the objects in any of the sites in Region 01. They require Read, Write, and Associate access to everything in Region 01.
- **Region01Directors** - responsible for deleting obsolete objects or defunct sites in Region 01. They require Read, Write, Associate, and Delete access to everything in Region 01.

You would create a set of groups for each region in your company (Region02Reviewers, Region02Writers, etc.). Once you have completed creating a set of groups for each region and added all of the users from the Regional Teams who belong directly to each group, it is time to create the groups for each Site.

The Site Teams

Below the Regional level, each Site has its own team of Reviewers, Writers, and Directors. For each site in each region, you would create a set of sub-groups as follows:

- **R01Site01Reviewers** - responsible for reviewing and reporting on Site 01 in Region 01. They require Read access to everything in Site 01.

- **R01Site01Writers** - responsible for making any necessary changes to the objects in Site 01 in Region 01. They require Read, Write, and Associate access to everything in Site 01.
- **R01Site01Directors** - responsible for deleting obsolete objects or defunct sites in Site 01 in Region 01. They require Read, Write, Associate, and Delete access to everything in Site 01.

Just like at the Regional level, you would create a set of sub-groups for each site in each Region. Although by this time we are probably creating a lot of groups, each group will only have to be declared in an ACL once at the site level.

As you create the Site groups, you can add the users who belong directly to each group. Adding groups to other groups will be handled in the next section.

Using Nested Groups to Limit User Scope

By now, you have created dozens of groups and you haven't actually created any ACLs! Not to worry - this is where all of those groups come in handy. In this section, we will nest our groups inside one another, add ACLs to our regions and sites, and break the inheritance of our business entities to restrict the scope of our users and groups. Let's take the last one first.

Task 1: Breaking Folder Inheritance

The first step in limiting user access to regions and sites is to break the inheritance of all of our business entity folders - all regions and all sites. Breaking the inheritance sets all of the groups and users without an ACL (except those with the Access Control Lists application permission) on the business entity folder to Denied/Denied/Denied/Denied. They can't view, edit, or delete the folder, create or remove associations, or view any business entity folder underneath it, even if they have an ACL set on a lower-level folder.

The Read permission is the most important, for Read allows you to see folders underneath the business entity and navigate down to them. However, with so many Regions and Sites to set up, we don't want to have to keep Denying access to all sorts of groups.

Procedure

1. Access the Access Control page (see "Accessing the Access Control Page" on page 620).
2. Navigate to the business entity folder where you wish to break inheritance (under the *Default* directory).
3. When you have found the desired folder, click the name of the folder to display the detail page.
4. Click **Add** in the Access Controls table and choose the desired group or user from the list.
5. Choose the desired permissions for the group or user by highlighting the appropriate entries and click the **OK** button to add the new ACL to the folder.
6. Now that a valid ACL exists for the folder, click the **Disable Inheritance** button under the Folder heading. The value of the "Inherit ACL" field is changed to "false" and the **Disable Inheritance** button changes to **Enable Inheritance**.
7. Click **Access Controls** in the breadcrumb trail to return to the Access Controls folder list.
8. Repeat this procedure for each business entity folder.

Note: Do not forget to modify the business entity folders under each object type in the ICDocumentation tree.

Task 2: Nesting Your User Groups

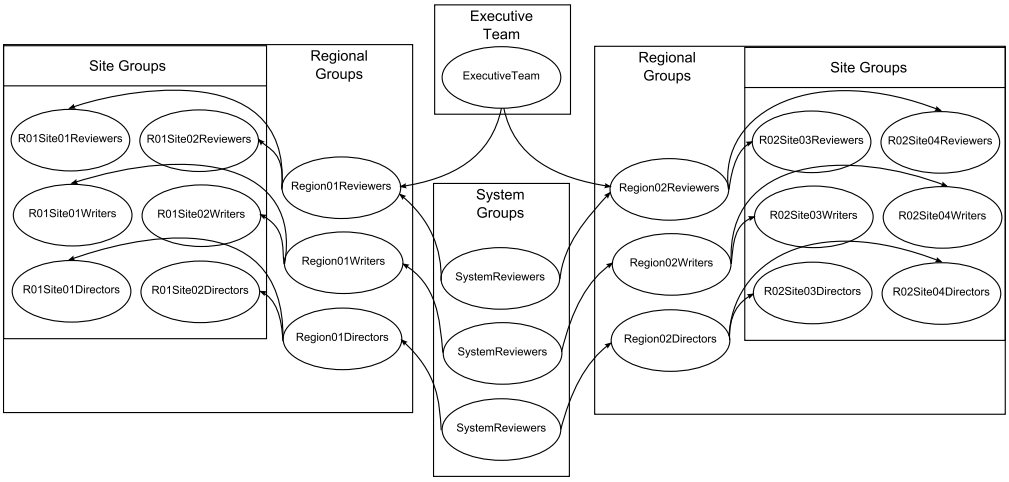
Now you have a lot of groups with users assigned to them according to their role. In this step, we will add groups to other groups in order to properly restrict their area of effect.

The way groups with users nest seems backwards at first glance - the most general groups (the System and Executive groups) have to be added to the more limited ones (the Regional groups), while the Regional groups have to be added to the most limited ones (the Site groups).

If the Region01Writers group belonged to the SystemWriters group, which can read, write, and associate to all regions, they would also be able to read and write to all Regions, which is not the desired behavior. We are trying to limit user scope, not enhance it. So adding smaller groups to larger groups doesn't work out correctly.

If you add the larger Regional groups to the smaller Site groups beneath them, you don't increase the smaller group's scope beyond its boundaries, but the Regional groups extend their vision downwards into all of the sites in their own Region. (Remember, since we broke inheritance at each level of the business entity, Regional groups don't automatically get to see the Sites underneath their Region.)

Here's a diagram that shows the way this works:



Let's follow one use case shown in the preceding diagram. The SystemWriters group becomes a sub-group to the Region01Writers group (and the Region02Writers group, and so on). Then, the Region01Writers group becomes a sub-group of the R01Site01Writers group (and the R01Site02Writers group, etc.). The sub-groups of Region01Writers also become sub-groups of R01Site01Writers through group inheritance. The effective members list of R01Site01Writers is now:

```
R01Site01Writers
    <writer1>
    <writer2>
    ...
    Region01Writers
       (SystemWriters)
```

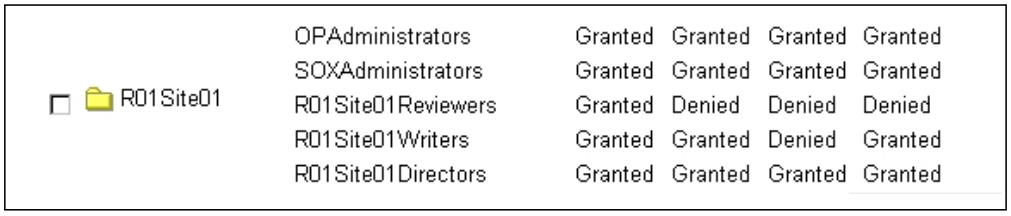
In the above example, SystemWriters is in parenthesis, because it isn't explicitly added to the group - it's included as a sub-group of the RegionalXXWriters groups. The same goes for the ExecutiveTeam group; it is added to each of the RegionXXReviewers groups. Executives only need Read access, so we don't need to add them to any other ACL classification.

Note: If you are using the Library paradigm, you do not want to add the ExecutiveTeam group to the Library group. You don't want empty Library data included into the executive level reports.

Now let's explore how we can use our nested groups to set our ACLs.

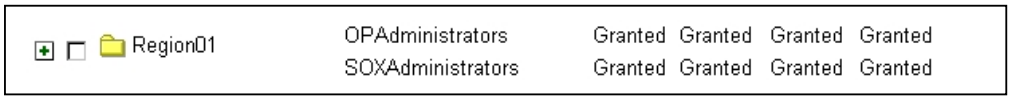
Task 3: Setting Folder Access Control Lists

Now that we have user groups with different permission needs for each site, we can start creating our ACLs. For each Site, we create an ACL for each R##Site## group and give them the necessary permissions. For example, in R01Site01, the ACLs for the business entity folder would look like this:



We don't need to specify the Region01Reviewers, Writers, or Directors - they are already included as members of the R01Site01 groups!

In general, you only need to specify ACLs for different access control levels (Read, Write, Delete, Associate) for business entity folders that contain non-business entity objects. For example, in our hierarchy, Regions only contain the sub-entity Sites - there are no accounts, processes, etc. directly associated with a Region. Therefore, we don't have to create ACLs for Region01Reviewers and the other ACL-specific groups at the Region level. In our current example, here's the ACL list for Region01:



Here's are some general guidelines for whether or not to create an ACL for a user group on a business entity:

- If the business entity has accounts or processes associated with it, you need to create an ACL for each entity-specific group (such as R01Site1Writers, etc.) with the correct permissions.
- When you create ACLs for a business entity, you must replicate the ACL for each business entity folder underneath the ICDocumentation folder structure. For example, you must create the same ACL list for the ICDocumentation/Accounts/Region01/R01Site01 folder that you created for the BusinessEntities/Region01/R01Site01 folder, and so on through each sub-folder structure under ICDocumentation (Accounts, Processes, Risks, Controls, etc.).

Note: If no folder with the correct name exists, either there is no object of that type currently in the business entity's hierarchy, or a parent folder's ACLs do not include a group that contains the current user, preventing you from seeing the folder.

- If a business entity only has sub-entities associated with it, you should not create individual ACLs for the business entity's Reviewer, Writer, and Director groups. We will deal with this in the next section,

Only one step remains - we've created the ACLs for our business entities, but when you log in, you can only see the first level of your business entities! We now need to establish read permissions in the business entities above our Site user groups, so that we can browse down to the Site level and view our objects.

Using Group ACLs to Traverse Business Entities

Even though we have successfully created a nested series of groups that successfully limits the scope of our site users, we seem to have gone a little too far - we can't browse through the business entities to get to our site! We need to create a group that will allow site users to browse through the entities, without granting anything but Read.

To allow Read access to lower-level user groups, follow these steps.

Procedure

1. Access the **Users, Groups and Domains** page (see "Accessing Users, Groups and Domains" on page 7).
2. Create a new group at the Region level (actually, at any level above the lowest, if you have more than two levels). Call the new group Region01Browsers, because that's what its purpose will be - to allow users from the entities below it to browse down to their site.
3. Create a similar group for each business entity above the lowest level (Site, in our example).
4. Access the Access Control page (see "Accessing the Access Control Page" on page 620).
5. Navigate into your business entity folder structure (under *\Default\BusinessEntities*).
6. Create an ACL on Region01 and grant Region01Browsers Read access. Repeat this with Region02Browsers in the Region02 business entity folders, and so on in any other Regions you've created.

   In order to not make the Browsers groups unwieldy, we'll need to "roll-up" each site's users into a single group that can be added to the Region01Browsers group.
7. Add the R01Site01Directors and R01Site01Writers group to the R01Site01Reviewers group.
8. Add the R01Site01Reviewers group to the Region01Browsers group. This has the effect of adding all of the R01Site01 groups to the Browsers group, even though you only added one.
9. Repeat the process for the rest of the business entities.
10. If you have more than one level above your lowest level, you will need to link the Browsers groups together, creating a chain to the highest level of business entity.

    For example, if we had top-level business entities called "Country01," etc., we would create a group called Country01Browsers, and add the

Region01Browsers group to it. However, if Region02 was not a child of Country01, you would not add Region02Browsers to the Country01Browsers group.

11. Once the groups have been added, log out and log back in with a Site level user and test that the ACLs are working correctly.

Appendix E. Using the DataMart Reporting Schema

Overview

The IBM OpenPages application contains a new real-time reporting schema that allows you to regenerate the reporting schema as soon as changes to the IBM OpenPages repository are implemented.

For information on the real-time reporting schema, see "Administering the Reporting Schema" on page 59.

OpenPages still supports the use of the original "data-mart" reporting schema implementation, where the schema must be manually generated and exported to an external reporting database instance.

The exportation of data to the reporting database must be repeated each time you wish to update the data available to the third-party reporting tools.

In order to use the reporting capabilities of a reporting tool such as CommandCenter with the datamart reporting system, you must configure and populate the reporting schema with your current IBM OpenPages data. The following sections will explain how to configure and populate that database instance using the tools provided with Oracle and IBM OpenPages .

Configuring the Reporting Metadata

Before the dynamic part of the IBM OpenPages reporting schema can be created, the configuration tables must be populated. Populating the configuration tables is a manual process. To simplify the configuration process, an Oracle package named OP_REPORT_MGR is included with the IBM OpenPages product, along with two SQL scripts. The SQL scripts demonstrate how to load a reporting configuration that corresponds to the standard IBM OpenPages schema shipped with the IBM OpenPages product.

Note: If you have customized your IBM OpenPages schema you will have to customize the SQL scripts to reflect the changes you have made in your schema.

Configuration Tables

The IBM OpenPages reporting schema includes a set of permanent tables that store the configuration tables used by the OP_REPORT_MGR package to dynamically generate and populate the rest of the reporting schema. The following tables are used to store configuration information for the IBM OpenPages reporting schema.

- RPT_OBJECTS

  The RPT_OBJECTS table is used to register the names of the database objects that represent resources corresponding to registered content types. It also defines that physical types of the database objects - views, materialized views, or tables. It allows specifying tablespaces to store the database objects and their indices.

- RPT_OBJ_COLUMNS

  The RPT_OBJ_COLUMNS table is used to define the mapping between the properties associated with a content type and the database object columns representing them, column aliases, and their physical order. It also allows the

defining of function-based columns by specifying the data transformation of the property values by means of the supported macro keywords or a user-supplied function.

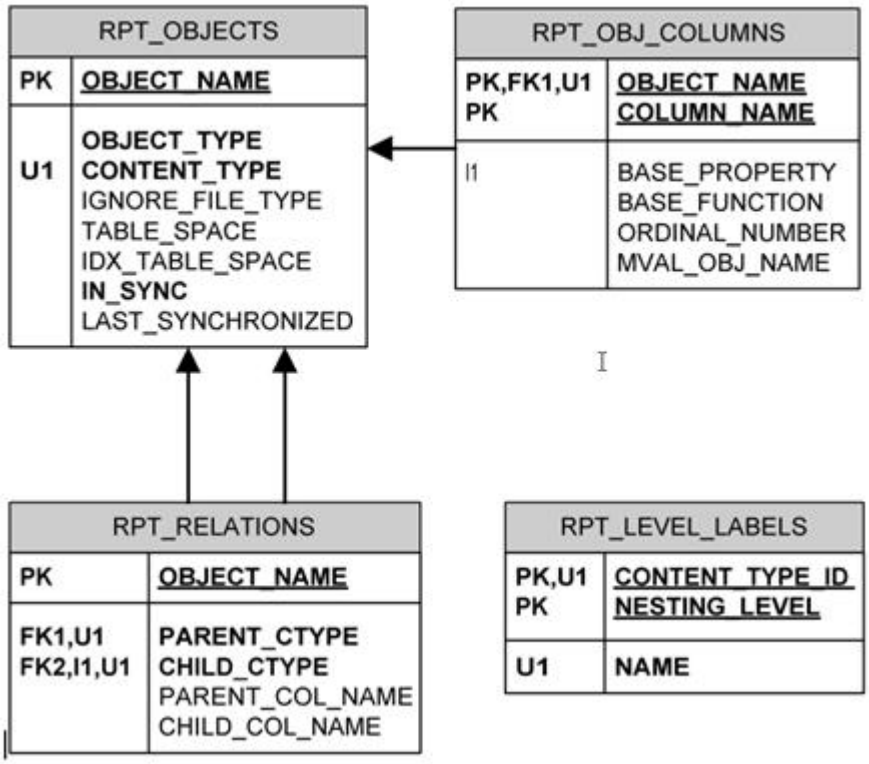
- RPT_RELATIONS

  The RPT_RELATIONS table is used to register object-to-object relationships. Database objects representing relationships can be either materialized views or tables, depending on the type of the "master" object. It can also specify column aliases for the parent and child identifiers.

- RPT_LEVEL_LABELS

  The RPT_LEVEL_LABELS table is used to assign a string label to a particular level in the hierarchy of jobects of the same type. For example, business entities can be nested, and assigning a label to each level of nesting (Division, Department, Workgroup, etc.) allows a better sense of level than "Level 3 Entity".

  The diagram represents the relationship of the configuration tables.



Reporting Schema Scripts

The IBM OpenPages product ships with two SQL scripts that demonstrate how to use the OP_REPORT_MGR package to load the reporting configuration. By default, the scripts are configured to support the default SSS (the IBM OpenPages Standard Schema) shipped with the IBM OpenPages product.

The supplied scripts are:

`ReportingSchema_Core.sql`

- Cleans up the reporting schema configuration tables
- Registers the database objects to represent the IBM OpenPages -specific content types and sets their properties. The default database object is a materialized view.

- Registers the columns that represent the core (system) attributes common to resources of all content types in the system.
- Registers the relationships between the various tables.
- Registers the level labels for the content types that can be nested.

`ReportingSchema_ProcessCentric_Delta.sql`

- Registers the remaining extended attributes defined in the SSS.

Note: The `ReportingSchema_ProcessCentric_Delta.sql` script only needs to be run the first time you load the configuration into the reporting schema. Subsequently, it will only need to be run if the schema of the IBM OpenPages application is modified in some way.

Executing the Configuration Scripts

To configure the reporting schema, log in as the openpages user and manually run both scripts in SQL*Plus on the Oracle server machine in the following order:

```
sqlplus> ReportingSchema_Core.sql;
sqlplus> ReportingSchema_ProcessCentric_Delta.sql;
```

Customizing the Reporting Schema Configuration

To modify the reporting schema configuration, you can use any of the following methods:

- Changing the supplied scripts

  You can edit the supplied scripts and do a complete reload of the configuration data. You can repeat this process as many times as necessary, as long as you run both scripts - first loading the core attributes, and then the extended attributes.
- Incrementally adding new content types and attributes

  You can create additional scripts using the existing ones as a reference to register additional content types or additional attributes for already registered content types.
- Editing data directly in the database

  In some cases, it might be easier to make minor changes or test new settings by editing the contents of the configuration tables directly. Only experienced DBAs should attempt this procedure, however, as the risk of user error is prominent.

Naming Restrictions

When customizing your schema configuration or contents, the following naming restrictions must be followed: Object (table, view, or materialized view) and column names must be 30 characters or less and must be valid Oracle names (containing only alphanumeric characters, dollar sign($), hashes(#), and underscores(_).

Mixed case names, names containing spaces, and international characters are not supported. Object names must be unique in the application user schema. Column names must be unique within the scope of a single object.

Supported Macro Keywords

Currently, the following macro keywords can be used to specify the data transformation of the property values inside the configuration tables.

- [FriendlyName] - applies to the resource name, resulting in the original resource name with the extension removed.

- [SoxUrl<;hostname:port>] - applies to the resource ID, resulting in the URL to view the resource properties (the "Details" page) in the IBM OpenPages user interface.

  Note: If the hostname and port information is omitted, the SoxUrl defaults to "localhost:7009". If you are using CommandCenter reports, you must modify the macro to explicitly specify the host server name and port of the IBM OpenPages application server. For load-balanced configurations, you can specify different values in the "hostname" and "port" for different content types.
- [DelimitedList] - applies to the multi-valued properties, resulting in a comma-separated list of values.
- [LockStatus] - applies to the resource ID, resulting in an indication whether there is a specific lock on the resource. This does not include checked-out locks.
- [NestingPath] - applies to the resource ID of the nested content types (business entities, sub-accounts, and sub-processes), resulting in a concatenated string of the "friendly names" of the resource and all its subordinate objects of the same type.
- [NestingLevel] - applies to the resource ID, resulting in a numeric value representing the object level in the hierarchy of nested objects of the same type.
- [NestingLabel] - applies to the resource ID, resulting in a value that represents the nesting level.

If any of the columns for a given content type use one of the "Nesting*" macros, the resulting database object will contain a level-based hierarchy representation, where each level of nesting is represented by a column. The extra columns are named according to the level labels defined for the corresponding content type.

If no level labels were defined for a given level, the column will be named as "LEVEL<#>" (for example, LEVEL1, LEVEL2, etc.)

Note: It is strongly recommended that you define level labels to accommodate the expected depth of object nesting for a given implementation, because the algorithms that populate the reporting schema rely only on the configuration data and do not validate whether the real data has additional levels of nesting than were originally declared.

The following picture shows a table with the "nesting" and level-based hierarchy columns:

ENTITY_ID	EN_NAME	EN_EXPORTLABEL	EN_NESTINGLEVEL	EN_NESTINGPATH	CORPORATE	DEPARTMENT	DIVISION	WORKGROUP
172	Corporate	Corporate	1	Corporate	Corporate	[NULL]	[NULL]	[NULL]
174	Canada	Department	2	Corporate/Canada	Corporate	Canada	[NULL]	[NULL]
176	Mexico	Department	2	Corporate/Mexico	Corporate	Mexico	[NULL]	[NULL]
182	United States	Department	2	Corporate/United States	Corporate	United States	[NULL]	[NULL]
181	Eastern Region	Division	3	Corporate/United States/Eastern Region	Corporate	United States	Eastern Region	[NULL]
180	Boston Office	Workgroup	4	Corporate/United States/Eastern Region/Boston Office	Corporate	United States	Eastern Region	Boston Office
170	Library	Corporate	1	Library	Library	[NULL]	[NULL]	[NULL]

Populating the Reporting Schema

After loading the reporting schema configuration, you can create and populate the dynamic portion of the reporting schema by executing the supplied command file (`Refresh-Reporting-Schema.cmd`) and providing the required input parameters.

Note: For the Refresh-Reporting-Schema.cmd file to work correctly, the Refresh-Reporting-Schema.sql file must be located in the same directory as the command file.

To populate the reporting schema:

1. Open a command window on the Oracle database server.
2. Navigate to the directory containing the Refresh-Reporting-Schema.cmd batch file.
3. Execute the Refresh-Reporting-Schema.cmd file using the following syntax:

```
Refresh-Reporting-Schema.cmd
     <OracleUserName> <OracleUserPassword> <OracleAlias>
     <ReportingPeriodValue> [<AddReportingPeriodColumn>
     [<ReportingPeriodColumnName> [<BackwardCompatibilityMode>]]]
```

Where:

< OracleUserName > is the name of the Oracle user account used by the IBM OpenPages application to connect to the database. This is a required parameter.

< OracleUserPassword > is the password of the Oracle user account. This is a required parameter.

< OracleAlias > is the Oracle Net Alias, a "friendly" Oracle instance system identifier or connection string. Usually this is the same as the SID. This is a required parameter.

< ReportingPeriodValue - is a value to be inserted into the "Reporting Period" column. This is a required parameter. Can be any arbitrary string. If the string contains spaces, it must be enclosed with double quotes. The special keyword "auto" can be used to populate the reporting period column with a timestamp representing the time that execution of the Refresh-Reporting-Period.cmd was started. Specifying a value of "no", "none", "null", or "nothing" will cause the default value of <AddReportingPeriodColumn> to flip to "no", and a reporting period column will not be added unless the <AddReportingPeriodColumn> is explicitly set to "Yes".

< AddReportingPeriodColumn > - indicates whether the "reporting period" column should be added to all objects created during the reporting schema refresh. Allowed values are "yes" and "no". This is an optional parameter that defaults to "yes" if it is not included in the parameter list. The reporting period column can be used to uniquely identify data produced by different reporting schema refresh sessions, if the user chooses to load the data into a dedicated data warehouse.

< ReportingPeriodColumnName > - specifies a physical name for the reporting period column. Defaults to "none". When the default value is used, the reporting period column is named "REPORTING_PERIOD". This is an optional parameter.

Note: When the Refresh-Reporting-Schema.cmd is run, it will automatically turn on Oracle Statistics for the following tables: all tables beginning with SX_, and the EFFECTIVE_RIGHTS table.

Checking the Results of the Reporting Schema Refresh

On every execution, the command line utility creates a new log file named in the format of Refresh-Reporting-Schema-YYYY-MM-DD#HH-MM-SS.log.

After the command executes, review the file for any possible errors and to get information about what input parameters were used for a given execution session, as well as the time it took to refresh the reporting schema.

Below is a sample of a successful reporting schema refresh:

```
Refreshing Reporting Schema...
Execution started at 2004-10-13 16:25:03.53
Input parameters:
     Add reporting period column: [yes]
     Column name: [Default/Not specified]
     Column value: [Auto generated/not specified]
     Backward compatibility mode: [Not requested]
Execution finished at 2004-10-13 16:52:02.73
Elapsed time: +000000000 00:26:59.209000000

PL/SQL procedure successfully completed.
```

The sample log below illustrates the errors logged when the reporting schema configuration was not loaded or was incomplete:

```
ERROR at line 1:
ORA-20100: Reporting schema metadata are not loaded
ORA-06512: at "OPENPAGES.OP_EXPORTER", line XXXX
ORA-06512: at line 1
```

This sample log corresponds to a situation where a reporting schema refresh is attempted, but another schema refresh session or object reset event is in progress:

```
ERROR at line 1:
ORA-20100: Another reporting schema refresh operation in progress
ORA-06512: at "OPENPAGES.OP_EXPORTER", line XXXX
ORA-06512: at line 1
```

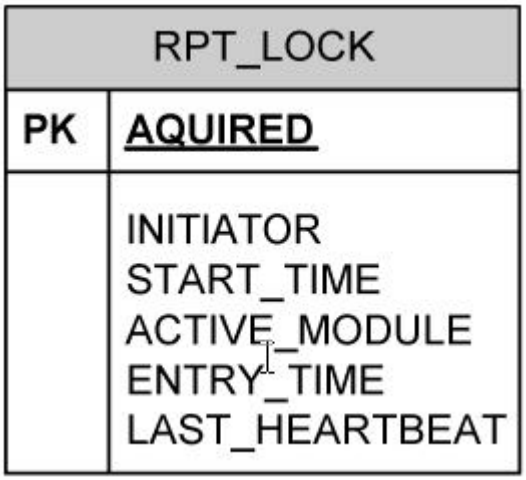
Synchronization Control:

Because during the reporting schema refresh database objects can be dropped and created, this operation is implemented as a single instance task. To enforce that no more than one refresh operation can be executed at any given time, the RPT_LOCK table is used.

As the reporting schema refresh and the object reset operations both use and modify a common subset of the database objects (namely the NODES table and the EFFECTIVE_RIGHTS materialized view), those operations cannot be executed at the same time.

The RPT_LOCK table can be used to verify if reporting schema refresh is in progress and its current status. If refresh is being executed, the table will contain a single record, otherwise the table will be empty. For more information about the

table layout and usage sample refer to the diagram below:



The following is an example of checking for the currently running reporting schema refresh jobs and their status using SQL*Plus:

```
column initiator format a40
column active_module format a40
column start_time format a30
column entry_time format a30
column last_heartbeat format a30

select * from rpt_locks;
```

Exporting Data to the Reporting Database Instance

After the contents of the reporting schema are created (refreshed), it must be copied to a dedicated reporting instance. This is a two-step process - first the data must be exported outside the live application instance, and then loaded into the dedicated reporting Oracle instance.

Important: It should be noted that these procedures will need to be repeated each time you want to update the data contained in the reporting datamart. The data will NOT update automatically.

The following sections will explain the procedures required to export the reporting schema to the reporting instance.

Note: To run the `Export-Reporting-Schema.cmd` command file, the `Generate-Export-Params.sql` script must be located in the same directory as the command file.

Exporting the Reporting Schema Contents

To export the required reporting schema database objects:

1. Open a command prompt on the database server machine and navigate to the location of the `Export-Reporting-Schema.cmd` command file.
2. Execute the `Export-Reporting-Schema.cmd` file with the following syntax:

   ```
   Export-Reporting-Schema.cmd
        <OracleUserName> <OracleUserPassword> <OracleSID> <NLS_LANG>
   ```

   Where:

   < `OracleUserName` > is the name of the Oracle user account used by the IBM OpenPages application to connect to the database. This is a required parameter.

< OracleUserPassword > is the password of the Oracle user account. This is a required parameter.

< OracleSID > is the Oracle instance system identifier or service name. This is a required parameter.

< NLS_LANG > is the national language setting to be used for the data export session. This is a required parameter.

Note: In order to run the export command successfully, SQL*Plus and the Oracle EXP utility must be installed on the Oracle database server.

After completion, the command line utility creates four files:

- reporting-schema-exp-parameters1.txt - contains the export parameters used by the EXP utility.
- reporting-schema-exp-parameters2.txt - also contains the export parameters used by the EXP utility.
- rpt-exp_YYYY-MM-DD#HH-MM-SS.log - provides statistics about the data exported and any error information.
- rpt-exp_YYYY-MM-DD#HH-MM-SS.dmp - export file containing data and object definitions for the reporting schema.

Importing the Reporting Schema Contents

Importing the data is a two-step process. First, you must import the contents, constraints, and indexes for all of the reporting schema tables, except for the RPT_OBJECTS, RPT_RELATIONS, EFFECTIVE_RIGHTS, ACTORINFO, and FOLDERS tables.

Then import the contents and indexes for the above-mentioned tables.

Note: The constraint definitions for those tables should not be imported, as foreign keys on those tables reference other tables which are not part of the reporting schema and are not exported.

To simplify the importing process, you can use a copy of the reporting-schema-exp-params.txt file to create a parameter file for the Oracle IMP utility.

For information about the format of Oracle parameter files for the EXP/IMP utilities consult your Oracle product documentation.

Note: It is possible to import the entire data dump file and review the reported errors. However, only the foreign key creation errors for the above-mentioned tables can be safely ignored.

Currently, in order to load updated data, the existing database objects have to be dropped. As part of the IBM OpenPages installation, the AuroraDbDelete.sql script is supplied, which can be used to drop all the objects in the user schema. This script can be executed in SQL*Plus.

Note: Exercise caution when executing the script, as the script removes all objects owned by the currently connected user.

Once the contents are imported successfully, the reporting schema data source is ready to be accessed by the third-party query engine.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service. This document may describe products, services, or features that are not included in the Program or license entitlement that you have purchased.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Location Code FT0
550 King Street
Littleton, MA 01460-1250
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only. This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Copyright

Licensed Materials - Property of IBM Corporation.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written.

These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Trademarks

IBM, the IBM logo, ibm.com, OpenPages, AIX, ReportNet, WebSphere, and Cognos are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide.

The following terms are trademarks or registered trademarks of other companies:

- Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
- Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
- Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Other product and service names might be trademarks of IBM, OpenPages, Inc., or other companies. A current list of IBM trademarks is available on the Web at " Copyright and trademark information " at www.ibm.com/legal/copytrade.shtml.

Glossary

access control list (ACL)
A concept in computer security used to determine the permissions (Read, Write, Delete, and Associate) a user or group can have on the folder structure of an object type (such as, an Entity, Risk, or Test). ACLs provide a means to control who has access to what and with which permissions. ACLs can be assigned to groups and users via a Role Template.

Action Menu
The menu bar that is always displayed at the top of a page. To reveal menu items, hover your mouse pointer over a menu name. Your permissions determine which menus and items are available.

Actor ACLs
These are a set of administrator access rights (Manage, Lock, Unlock, Reset Passwords, Assign Roles, Browse) defined on users and groups. These access rights control the operations an administrator can perform on a particular user or group.

administrator
A user that is granted special permission to manage a Business Entity, including the assignment of Roles to users and groups.

application permissions
A list of permissions that allow groups and users to access certain activities, including administration, within the application (such as the ability to view, lock, or unlock objects, or create and delete reporting periods).

associations
Relationships that exist among objects, or between objects and attached files. Example: A sub-entity may be directly associated with a process or business function.

business unit
One or more Entities, Processes or Sub-Processes.

CSV Comma separated values. A type of file that uses a comma-delimited format.

group A generic term that encompasses both organizational and security domain groups.

listing pane
The pane on an object's Detail View page that is displayed when you click the name of an associated object type. It lists all the names of objects for that type that are associated with the current object, and has an Actions Menu for adding new objects, or associating and copying existing objects of the same type.

object Any item that contains or receives information, such as Business Entities, Processes, Risks, Controls, Issues, Tests and so forth. In a security context, an object is the piece of data to which access control is applied (such as, Business Entity, Process, Sub Process, Risk Assessment). Also called “resource”.

object type
A category or type of object, such as a Risks, Controls, Issues and so forth. In a hierarchy of objects, each object type has a set of allowed relationships with other object types.

organizational group
A group that is created by an administrator to organize users within an organization. Organizational groups are typically associated with security domain groups and other organizational groups.

pane A section or component of an object view, usually rectangular in shape. For example, a Detail View page typically consists of several panes, such as a Details pane, Context pane, Associations pane, Listing pane, and an Attachments pane.

resource
See “object”.

Resource ACLs
These are a set of access rights (Read, Write, Delete and Associate) defined on the parent folder of an object. These access rights control the operations a user can perform on the folder and any objects under that folder.

role An instance of a Role Template that is applied to a set of Users/Groups for a specific security context. Roles are granted to Users/Groups which allows them access to objects with certain permissions. Some examples of roles are: 'Process Owner', 'Control Owner', and 'Tester'.

Role Template
A security object that you can use to define all aspects of application security for various groups and users within a business unit. It contains access control definitions on folder structures for object types and application permissions. Role Templates generally reflect the usual or expected function that a user or group plays within an organization. Some examples or Role Templates that can be defined are 'Process Owner', 'Control Owner', and 'Tester'. The template can then be applied to different Users/Groups for a specific security context.

security context point
A point defined in the OpenPages security model that you can use to assign roles to users and groups for controlling access and application permissions to objects under that security point.

security domain group
A group that is automatically created by the system when a business entity or subentity is created. Business entity security domain groups are located under the top level (root) **Security Domains** folder on the **Users, Groups and Domains** page.

Index

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

W

X