IBM OpenPages GRC
Version 7.4.0

Administrator's Guide

Note

Before using this information and the product it supports, read the information in “Notices” on page 805.

Product Information

This document applies to IBM OpenPages GRC Version 7.4.0 and may also apply to subsequent releases.

Contents

Introduction

IBM® OpenPages® GRC is an integrated governance, risk, and compliance platform that enables companies to manage risk and regulatory challenges across the enterprise.

Audience

The *IBM OpenPages GRC Administrator's Guide* is intended for use with OpenPages GRC on Platform and OpenPages GRC on Cloud. The content contains instructions for maintaining, configuring, and administering the OpenPages GRC application. It is intended for use by administrators who have a background in Systems Management. Topics include user and group administration, database backup and restoration, customizing the application's look and feel, and using the data loader capabilities.

Please read the following important information regarding IBM OpenPages GRC documentation

IBM maintains one set of documentation serving both cloud and on premise IBM OpenPages GRC deployments. The IBM OpenPages documentation describes certain features and functions which may not be available in OpenPages GRC on Cloud. For example, OpenPages GRC on Cloud does not include integration with IBM Business Process Manager and certain administrative functions.

If you have any questions about the functionality available in the product version that you are using, please contact IBM OpenPages Support via the IBM Support Community.

Finding information

To find product documentation on the web, including all translated documentation, access IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter).

Accessibility features

Accessibility features help users who have a physical disability, such as restricted mobility or limited vision, to use information technology products. OpenPages GRC documentation has accessibility features. PDF documents are supplemental and include no added accessibility features.

Forward-looking statements

This documentation describes the current functionality of the product. References to items that are not currently available may be included. No implication of any future availability should be inferred. Any such references are not a commitment, promise, or legal obligation to deliver any material, code, or functionality. The development, release, and timing of features or functionality remain at the sole discretion of IBM.

Database tool information

IBM OpenPages GRC Platform supports both the IBM DB2® database and the Oracle database.

- To run OpenPages GRC Platform SQL scripts, you must use CLPPlus with IBM DB2, and SQL*Plus with Oracle database.

- To run queries, you can use any SQL tool that is compatible with the database. For example, you could use CLPPlus or Optim™ Development Studio to run queries on the IBM DB2 database.

Installation locations

The installation directory is the location of product artifacts after a package, product, or component is installed. The following table lists the conventions that are used to refer to the installation location of installed components and products:

Important: Directory locations that contain spaces are not supported. IBM OpenPages GRC Platform or any software that is used by it must not be installed into a directory with spaces. For example, do not install database server, database client, or application server software into the `Program Files` directory.

Table 1: Variable notations for installation directories

Directory	Description
<installation_server_home>	The directory where the IBM OpenPages GRC Platform installation server is installed. For example: • On Windows: `c:\IBM\OPInstall\OP_<version>_Installer` • On AIX® and Linux: `/home/opuser/IBM/OPInstall/OP_<version>_Installer`
<agent_home>	The directory where the IBM OpenPages GRC Platform installation agent is installed on a remote server. For example: • On Windows: `c:\IBM\OPAgent` • On AIX and Linux: `/home/opuser/IBM/OPAgent`
<OP_HOME>	The directory where OpenPages GRC Platform is installed. For example: • On Windows: `c:\OpenPages` • On AIX and Linux: `/opt/OpenPages`
<ORACLE_HOME>	The installation location of the Oracle database server. For example: • On Windows: `C:\app\Administrator\product\12.1\client_1` • On AIX and Linux: `/home/oracle/app/oracle/product/12.1/client_1`
<DB2_HOME>	The installation location of the IBM DB2 software. For example: • On Windows: `C:/IBM/SQLLIB` • On AIX and Linux: `/home/db2inst1/sqllib`

Table 1: Variable notations for installation directories (continued)	
Directory	**Description**
<WAS_HOME>	The installation location of IBM WebSphere® Application Server. For example: • On Windows: `C:\IBM\WebSphere\AppServer` • On AIX and Linux: `/opt/IBM/WebSphere/AppServer`
<COGNOS_HOME>	The installation location of Cognos Analytics. For example: • On Windows: `C:\IBM\cognos\analytics` • On AIX and Linux: `/usr/IBM/cognos/analytics`
<JAVA_HOME>	The installation location of your Java™ Runtime Environment (JRE) or your IBM Java Software Development Kit (SDK). SDK example on an application server where IBM WebSphere is installed: • On Windows: `C:\IBM\WebSphere\AppServer\Java\8.0` • On AIX and Linux: `/opt/IBM/WebSphere/AppServer/Java/8.0` JRE example on a reporting server where Cognos Analytics is installed: • On Windows: `C:\`*<COGNOS_HOME>*`\jre` • On AIX and Linux: */*<COGNOS_HOME>*`/jre`
<CC_HOME>	The installation location of OpenPages GRC Platform CommandCenter. For example: • On Windows: `C:\OpenPages\CommandCenter` • On AIX and Linux: `/opt/OpenPages/CommandCenter`
<SEARCH_HOME>	The installation location of global search. The *<SEARCH_HOME>* directory contains the `opsearchtools.jar`, Apache Solr, and other global search files. The global search indexing directory is also stored in the *<SEARCH_HOME>* directory. For example: • On Windows: `c:\OpenPages\OPSearch` • On AIX and Linux: `/opt/OpenPages/OPSearch` In the installation app, you specify the *<SEARCH_HOME>* directory in the **Search Home Directory** field on the **Search Server** card.

IBM OpenPages GRC Platform

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 Financial Controls Management, Operational Risk Management, IT Governance, Policy and Compliance Management, and Internal Audit, 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.

OpenPages GRC Platform solutions

The IBM OpenPages GRC Platform consists of the following solutions:

- Financial Controls Management (FCM) provides automated assessment, testing, and certification processes to standardize and manage Sarbanes-Oxley (SOX) compliance enterprise-wide.
- 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.
- Policy and Compliance Management (PCM) provides an integrated solution for reducing the complexity of complying with numerous industrial, ethics, privacy, and government regulatory mandates.
- IT Governance (ITG) provides a risk-based, policy-driven approach to managing risk and compliance initiative for the IT organization.
- Internal Audit Management (IAM) provides an integrated audit management solution to manage the full life cycle of internal audits.

How IBM OpenPages GRC Platform can help

The OpenPages GRC Platform application provides many capabilities to simplify and centralize compliance and risk management activities.

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 Cognos

- 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 (both UK and US), 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

- 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 1. What's new?

New and changed features affect the administration of IBM OpenPages GRC Platform.

For information about all new features for this release, see the *IBM OpenPages GRC Platform New Features Guide*.

For an up-to-date list of environments that are supported by OpenPages GRC Platform, see the IBM Software Product Compatibility Reports (http://www.ibm.com/support/docview.wss?uid=swg27039467).

New and changed features in version 7.4.0

The new and changed features in IBM OpenPages GRC Platform version 7.4.0 are described in the following sections. For more information, see IBM OpenPages GRC New Features Guide.

Platform enhancements

New and changed features in version 7.4.0 related to IBM OpenPages platform are described in the following tables.

Cognos Analytics V11.0 enhancements

Table 2: Cognos Analytics V11.0 enhancements	
For information about...	**See topic...**
Adding Cognos Analytics dashboard and story pages to OpenPages by using the new `Cognos Analytics Dashboard Redirect` page template.	"Manually creating an instance of a Cognos dashboard or story" on page 121
The predefined reports that are supplied with OpenPages that have been updated to work with Cognos Analytics V11.0.	Chapter 7, "Managing reports," on page 109
The new application permission: All/SOX/ CommandCenter Studios/Cognos Analytics	"Reporting framework permissions" on page 684

Additionally, the **Reporting** menu now contains **Reporting** > **Cognos Analytics**. The following menu items were removed:

- **Cognos Analysis Studio**
- **Cognos Connection**
- **Cognos Query Studio**
- **Cognos Report Studio**
- **Cognos Workspace**
- **Cognos Workspace Advanced**

Reporting framework enhancements

Table 3: Reporting framework enhancements	
For information about...	**See topic...**
Configuring multiple framework models and by using the new standard and basic framework models.	“Framework models” on page 659
The new All Models and Selected Models options on **Administration** > **Reporting Framework** > **Generation**.	“Choosing update options in the reporting framework” on page 685
The new templates, Template_Model and TEMPLATE_NAMESPACE, that you can use to quickly create new framework models and namespaces.	“Creating a framework model and namespace using a template” on page 669
The new **Package Name** field on computed fields.	“Defining a computed field” on page 155
The new settings in the **Administration** > **Settings** > **Platform** > **Reporting Framework V6** folder:	
Configuration > **Concurrent Models**	“Configuring the number of models that can be concurrently generated” on page 665
Configuration > **Sort Order Locale**	“Defining the sort order locale ” on page 666
Models > **[model name]** > **Format**	“Defining the format for a framework model” on page 670
Models > **[model name]** > **Is Enabled**	“Enabling a framework model ” on page 670
Models > **[model name]** > **Mode**	“Defining the query mode for a framework model ” on page 671
Models > **[model name]** > **Profile**	“Defining whether a framework model uses profile filtering” on page 671
Models > **[model name]** > **Namespaces** > **[namespace name]** > **Is Facts and Dimensions Enabled**	“Defining whether facts and dimensions are enabled for a namespace ” on page 674
The **Administration** > **Settings** > **Platform** > **Reporting Framework V6** > **Models** setting has been changed.	“Defining a name for a framework model” on page 670

Administration and serviceability enhancements

New and changed features in version 7.4.0 related to IBM OpenPages administration and serviceability are described in the following tables.

Administration and serviceability enhancements

Table 4: Administration and serviceability enhancements	
For information about...	**See topic...**
The new **New Folder Name** field that you can use to give a folder a name when you select a folder under the **Administration** > **Settings** menu and click **Copy to**.	“Copying settings and folders ” on page 341

Table 4: Administration and serviceability enhancements (continued)	
For information about...	**See topic...**
The new **Administration** > **Manage System Files** menu item that allows you to manage system files and folders.	Chapter 8, “System file management,” on page 131
The new ready-to-use OpenPages Platform 3 profile that administrators need to access system files and folders using **Administration** > **Manage System Files**.	Chapter 8, “System file management,” on page 131 “Associating users and groups to a profile” on page 217
The new **Administration** > **Settings** > **Applications** > **Common** > **Disable the files of OPX** setting that can temporarily enable the OPX interface.	“Disabling the Files of OPX” on page 327
The new **Administration** > **Settings** > **Applications** > **GRCM** > **Environment Migration** > **Allow ObjectManager XML** setting that controls whether ObjectManager XML files can be imported through **Administration** > **Import Configuration**.	“Settings that apply to environment migration” on page 575
The **Administration** > **Settings** > **Applications** > **Common** > **Configuration** > **Force Internet Explorer Compatibility Mode** registry setting has been removed. Internet Explorer 11 in native mode is supported. Internet Explorer 9 and 10 and Internet Explorer compatibility mode are no longer supported.	

User provisioning enhancements

Table 5: User provisioning enhancements	
For information about...	**See topic...**
The new **Users** menu item on the **Administration** menu.	Chapter 3, “Users, groups, and domains,” on page 19
Tasks that you should complete before creating, modifying, or copying users and changes to the way delegated administration works in 7.4.0.	“Planning user administration” on page 19
Administrative permissions that are required for each of the user provisioning tasks.	“Administrator permissions for user-provisioning functions” on page 22
LDAP server integration for creating new user accounts.	“LDAP and user provisioning” on page 25
The new method of adding new user accounts with the Create User wizard.	“Creating user accounts” on page 27
The new method of modifying and managing existing user accounts.	“Modifying user accounts” on page 28
The new functionality that allows you to copy a user's locale, profiles, group memberships, and direct role assignments.	“Copying access from one user to another” on page 30

Table 5: User provisioning enhancements (continued)	
For information about...	**See topic...**
The new registry settings for configuring the behavior of user provisioning functionality.	"User provisioning settings" on page 312
The new default password expiry behavior that uses the **Applications** > **Common** > **Administration** > **User Provisioning** > **Default User Password Expiration** setting rather than the **OpenPages** > **Platform** > **Security** > > **Password** > **Policy** > **Default Expiry Days** setting.	"Default User Password Expiration" on page 313
When you configure user and group selector display types for simple strings, you can now leave the **Starting Group** value blank. A blank value used in combination with an **Include Disabled** value of true can result in improved search performance.	Table 89 on page 267

New features in version 7.3.0.2

The new features in IBM OpenPages GRC Platform, version 7.3.0.2, are described in the following sections.

Cognitive services

Administrators can configure the cognitive services to support decision making when users associate objects.

- Added **Type** and **Field Association** fields to **Administration** > **Cognitive Services** > **Natural Language Classifiers**. For more information, see Chapter 31, "Configuring cognitive services," on page 723.

Integration with IBM Regulatory Compliance Analytics

Administrators can configure how IBM Regulatory Compliance Analytics data is imported into IBM OpenPages GRC Platform.

Added **RCA Integration** to the **Administration** menu. It has two menu items:

- **Configure Import from RCA**
- **Import from RCA**

Added the application permission, RCA Integration, which controls whether these menu items are displayed. It is located in **SOX** > **Adminstration**. Administrators who work with IBM Regulatory Compliance Analytics integration need to have this application permission. For more information, see "Types of application permissions" on page 32.

For more information about the feature, see Chapter 33, "Importing IBM Regulatory Compliance Analytics data," on page 737.

Registry settings for third-party SMTP providers

Added registry settings:

- **Applications** > **Common** > **Email** > **SMTP Port**
- **Applications** > **Common** > **Email** > **SMTP Security Type**

Define these settings if you use a third-party SMTP provider. For more information, see "Set the mail server address" on page 322.

Auto-naming setting for SOXDocument objects

You can use the new Auto Remediate Duplicate File Names setting to control auto-naming for SOXDocument objects if file names are not unique in a folder. For more information, see "SOXDocument object auto-naming settings for duplicate file names" on page 320.

Copy views to profiles

Administrators can now copy object and creation views from one profile to one or more other profiles. For more information, see "Copy views for an object from one profile to one or more other profiles" on page 244.

Configuring user-friendly URL link names by using the rich text display type for simple strings

You can use the rich text display type to display a user-friendly link name as a field's default value. For example, you can configure a field's default value to display as **My Company** rather than **http://www.mycompany.com**. This existing feature is described in the new topic, "Configuring URL link names by using the rich text display type for simple strings" on page 265.

Compare environments

You can find differences between two environment configuration XML files by using **Compare Environments**. Use Compare Environments to identify and resolve issues before you migrate configurations from one environment to another. For more information, see Chapter 21, "Comparing IBM OpenPages GRC Platform environments," on page 563.

New features in version 7.3.0.1

The new features in IBM OpenPages GRC Platform, version 7.3.0.1, are described in the following sections.

Cognitive services

- Added the data type, Classifier. A classifier field must have this data type.

  For more information, see "Data types" on page 143.
- Added the menu item, **Administration** > **Cognitive Services** > **Natural Language Classifiers**. Use this task to create a classifier configuration. For more information, see Chapter 31, "Configuring cognitive services," on page 723.

UCF connector integration

Use IBM OpenPages GRC SDI Connector for UCF Common Controls Hub to import data from UCF Common Controls Hub into IBM OpenPages GRC Platform.

For more information, see "IBM OpenPages GRC SDI Connector for UCF Common Controls Hub integration" on page 694.

IBM OpenPages Regulatory Compliance Management Theme Deployer

The RCM Theme Deployer is a tool that users can use to lay the foundation for business entities to complete regulatory compliance assessments.

For more information, see "RCM Theme Deployer" on page 731.

IBM OpenPages Regulatory Compliance Management configuration tool

You can use the IBM OpenPages Regulatory Compliance Management tool to configure the RCM solution, including the RCM Theme Deployer.

For more information, see Chapter 32, “Configuring IBM OpenPages Regulatory Compliance Management,” on page 731.

New X-XSS-Protection response header setting

The new **X-XSS-Protection** setting enables XSS filtering on server responses. Using this setting is preferred to using the **IE XSS Filter** setting. If there is a conflict between the **IE XSS Filter** and **X-XSS-Protection** settings, the one that enables the header is used. For more information about **X-XSS Protection**, see “Configure the HTTP response headers” on page 353.

New features in version 7.3.0

The new features in IBM OpenPages GRC Platform Version 7.3.0 are described in the following sections.

Enable or disable file attachment search

From the global search administration page, you can now toggle between enabling and disabling the file attachment search component for all search-enabled file types.

For more information, see “Enabling and disabling file attachment searching” on page 362.

Specify which file types are enabled for file attachment search

From the SOXDocument object type administration page, you can specify which MIME (Multipurpose Internet Mail Extensions) types are enabled or disabled for file attachment global search.

In a new installation of OpenPages 7.3, some MIME types are enabled for searching and others not. When you upgrade to OpenPages Version 7.3.0 from an earlier version, the same set of MIME types are enabled. However, the Search Files switch is off so that existing customers can continue to use global search with the existing functionality.

For more information, see “Enabling attachment file types for global search” on page 362.

Show an additional custom field in the search results

You can now configure one additional custom field to be displayed in the search results for each object type. As administrator, you can customize global search results to contain one additional field in the search results to help the user determine whether the record that is returned is the record for which they want the details.

For more information, see “Displaying a custom field in global search results” on page 366.

Legacy option for the new copy and associate functionality

You can use a registry setting to revert to using the legacy copy and associate features in Activity Views and Detail Views only. This is to allow time to ensure that the new implementation meets your needs before you retire the old implementation. The interface that is used for copy tasks and for associate tasks from Grid Views is always the new interface.

For more information about the legacy copy setting, see “Set copy operations” on page 324.

For more information about the legacy associate setting, see “Common folder settings” on page 341.

Dashboard tab for the user's home page

The Dashboard tab allows users to create their own dashboard for the Home Page. Users can now make their workflows more efficient by creating quick access to the tasks and information that they use most often. Users can tailor their dashboards to suit the way that they work.

Users and administrators can add as many of the following types of widgets as needed to the Dashboard tab:

- Filter Count widget
- Object Global Search widget
- Static Web Link widget
- Add New widget, which creates a **Add New** button that is preconfigured for a specific object type.

For each profile, administrators can create a default Dashboard tab that is displayed for users who log on to OpenPages for the first time. Administrators can specify that a panel is either locked or unlocked. When a locked panel is saved by an administrator, it is automatically pushed to the Dashboard tab of all users in the profile the next time those users log on. When an unlocked panel is saved by an administrator, it becomes part of the default Dashboard tab for users who are opening the application for the first time, but the panel is not pushed to the Dashboard tab of users. Users can edit or delete unlocked panels but cannot edit or removed locked panels.

For more information, see "Configuring users' Dashboard tabs" on page 233.

Integration with IBM Business Process Manager

Added the following registry settings in the **Administration** > **Settings** > **Platform** > **Workflow Implementations** > **IBM BPM** folder:

- **Enable Login SSO**
- **Portal Page Path**
- **Server URL**

For more information, see "Workflow implementations settings" on page 353.

Added the following menu items to the **Administration** menu:

- **IBM BPM Process Center**
- **IBM BPM Process Inspector**
- **IBM BPM Process Admin**

Added the new application permission, IBM BPM, which controls whether these menu items are displayed. It is located in **SOX** > **Adminstration**. Administrators who work with IBM BPM need to have this application permission. For more information, see "Types of application permissions" on page 32.

To profiles, added **Process Portal** to the `Home Page Tab Configuration` setting. When this setting is set to `Visible`, the **Process Portal** tab is displayed on the Home Page.

Personalizations are now maintained

Some personalizations to OpenPages are now maintained when you clear your browser cache or switch to another browser or device. For example, if you rearrange the panels on your home page dashboard and then switch to another browser, your dashboard looks the same in the new browser window. The changes that you made to the panels are preserved. Previously, personalizations were lost because they were stored in the browser.

In version 7.3, the following personalizations are stored in the database:

- The home page tab that was last selected: **My Work** or **Dashboard**
- **My Work** tab
  - Hidden and shown panels
  - Collapsed and expanded panels
  - Panel sequence
- **Dashboard** tab
  - Hidden and shown panels
  - Panel sequence
  - Widgets added and removed from the dashboard

- Analytics bar:
  - The default filter
  - The filters that are displayed on the analytics bar
  - The order of the filters
  - The expanded or collapsed state of the analytics bar
- Grid views
  - Column widths
  - Sequence of fields
  - Compact mode or full mode, and the fields shown or hidden for each mode

Enhanced export functionality

Using new registry settings, you can:

- allow users to choose which object types and fields to export. For more information, see "Enable object type and field export choices in the Filtered List View" on page 338.
- exclude object types from an export unless they are included in the Filtered List View. For more information, see "Exclude object types to export in the Filtered List View" on page 339.
- determine how many total levels of object types the user can choose to export, including the top-level object that is exported. For more information, see "Number of levels to export in the Filtered List View" on page 339.

FastMap import performance improvements

The performance of FastMap imports has been improved by a significant amount. The improved performance applies to objects being created or updated.

Note: The total time it takes to modify objects with a FastMap import can be affected by the time it takes for the triggers to operate. The improvements made to FastMap import performance do not impact the portion of time spent evaluating and executing the triggers.

Disable Add New capability

You can now disable the **Add New** capability from several launch points within the product by using one or more new registry settings. This is useful if users find it difficult to select the most appropriate parent information for particular object types.

For more information, see "Disable the Add New wizard from various launch points" on page 309.

Collect and view logs

The new LogCollector tool provides a command-line interface that you can use to collect log files and diagnostic data from the IBM OpenPages GRC Platform environment.

With the LogCollector tool, you can collect log and diagnostic files from the IBM OpenPages GRC Platform environment and from the IBM OpenPages GRC Platform database.

New features in version 7.2.0.4

The new features in IBM OpenPages GRC Platform, version 7.2.0.4, are described in the following sections.

Collect and view logs

The new LogCollector tool provides a command-line interface that you can use to collect log files and diagnostic data from the IBM OpenPages GRC Platform environment.

With the LogCollector tool, you can collect log and diagnostic files from the IBM OpenPages GRC Platform environment and from the IBM OpenPagesdatabase.

For more information, see “Collect log files and diagnostic data” on page 539.

New features in version 7.2.0.2

The new features in IBM OpenPages GRC Platform, version 7.2.0.2, are described in the following sections.

OpenPages Loss Event Entry

You can use the new optional, chargeable component, IBM OpenPages Loss Event Entry, to enable users across an organization to quickly create loss events. It is easy to use and task focused for users with no experience with OpenPages.

For more information, see Chapter 29, “Configuring OpenPages Loss Event Entry,” on page 709.

Business Entity Selector

You can use the new Business Entity Selector display type in IBM OpenPages Loss Event Entry and in most OpenPages views. This display type enables users to quickly identify the role a business entity plays.

For more information, see “Configuring the Business Entity Selector display type for simple string fields” on page 263.

New features in version 7.2.0.1

The new features in IBM OpenPages GRC Platform, version 7.2.0.1, are described in the following sections.

Approval app

The approval app is an optional feature that leverages the power of IBM OpenPages GRC Platform and provides an easy-to-use interface for quickly taking action on a review, approval, or attestation request with confidence and full knowledge of the context surrounding the request. The approval app works with objects that are set up for the configurable lifecycle.

For more information, see Chapter 28, “Configuring the approval app,” on page 701.

New features in version 7.2.0

The new features in IBM OpenPages GRC Platform, version 7.2.0, are described in the following sections.

Hyperlink to Add New wizard

You can now open a hyperlink URL, for example, one you received in an email, and go directly to the Add New wizard to create an object of a specific type. If you are not logged in and not using single sign-on, you must log in. OpenPages will open in a new browser window or tab and display a page with the Add New wizard.

After the Add New wizard is open, functionality is the same as from other access points.

For information about how to set up the hyperlinks, see “Task-oriented hyperlinking” on page 801.

Personalized home page

You can now control the display and order of the panes on the **My Work** tab on the home page.

The **My Work** tab contains numerous panes with predefined lists, filtered lists, and reports that have been set up for you by an administrator. This enhancement allows you to personalize the **My Work** tab to be more specific to your role and to rearrange the panes so you can easily and quickly access what you work on everyday.

Administrators use the new **My Work Home Page Can Be Personalized** setting to globally control whether users are allowed to use this feature. For more information, see "Home page settings" on page 333.

Global search

You can now configure and use global search, an optional component that enables users to search easily for objects across the entire application.

Administrators can set up global search for first time, customize which object types and fields can be searched, and tune global search by using registry settings and other properties.

For more information, see Chapter 16, "Configuring the global search feature," on page 357.

QRadar integration package

QRadar® integration is an optional project that you can use to import Offenses from IBM QRadar to IBM OpenPages GRC Platform as Incident object types.

You can configure the IBM Tivoli® Directory Integrator (TDI) included with IBM OpenPages GRC Platform version 7.2 to work with QRadar or other third-party solutions. You can run TDI assembly lines on demand by the command line, or schedule them to run at regular intervals. You can also use filtering so that only the relevant subset of data that impacts your business is imported.

For more information, see Chapter 26, " IBM OpenPages GRC Platform connectors," on page 689.

Equation editor

You can now add mathematical equations that support IBM OpenPages Model Risk Governance and other solutions.

Administrators use the new **CodeCogs Equation Editor with the Enable CodeCogs(r) Equation Editors** setting to globally control whether users are allowed to use this feature.

For more information, see "Common folder settings" on page 341.

Changed features in version 7.2.0

The following features are changed in IBM OpenPages GRC Platform version 7.2.0.

FastMap and new objects related to questionnaire assessments

You can now use FastMap to import and export the new questionnaire template objects and the content in sections, subsections, and questions. You can also use it to import and export the standard fields for questionnaire assessment instances. For more information see "Using FastMap with questionnaire template and assessment objects" on page 656.

Changed features in version 7.1.0.1

The following features have changed in IBM OpenPages GRC Platform version 7.1.0.1.

The validate command replaces the verify command in ObjectManager tool

The ObjectManager tool `verify` command used in OpenPages GRC Platform version 7.1 has been deprecated and replaced by the `validate` command. For more information, see "Validating or verifying configuration changes" on page 619.

New features in version 7.1.0

The new features in IBM OpenPages GRC Platform are described in the following sections.

Field level security and encryption

You can specify access rights and enable data encryption at the individual field level. These new security capabilities provide more granular control over access to data and enforce segregation of duties across an organization.

With the new security capabilities, a chief compliance officer can be assured that access to corporate GRC data is controlled at the required granularity, based on employees' roles, and that confidential or sensitive information is not overexposed. A business user, such as an owner, a reviewer, or an approver on a specific GRC object instance, can view and edit a set of fields, depending on his or her role and the state of the associated object. A database administrator who performs IBM OpenPages GRC Platform backups cannot access confidential or sensitive data. All of these benefits are achieved with minimal administrative impact.

Field level security is enforced at all levels of the system, including the application user interface, Cognos reports, Risk APIs, data export and import (FastMap), and data load.

When you apply this type of security, the fields are rendered proactively based on the users' access rights. Read-only fields are displayed as non-editable. The values in the inaccessible fields are displayed as **Confidential** for users who do not have the required access rights.

For more information, see "Field level security" on page 69 and "Field level encryption" on page 81.

New method for adding objects

Administrators and users can now easily add new object instances on a single page from anywhere in the system.

Using the **Add New** wizard, the users can create and save an object by entering only the minimum, most important information based on the user's profile. When **Auto Naming** and **Save as Draft** are enabled, new objects can be added with only two clicks.

Where possible, the system leverages context to simplify input for the users. The users can leverage a library of object templates to simplify input requirements and to drive corporate standards when they create objects.

The **Add New** wizard can be used to add a row to a grid view and to add file attachments, which makes it possible for the user to stay on the grid view and get more work done without leaving the page. The user can associate the new object to multiple parents of different object types, eliminating the need for extra navigation and tasks in the user interface after the object is created.

A confirmation message with a hyperlink to the new object appears after the object is saved. Users can access the object with one click if they choose to specify additional information.

For more information, see "Configuration settings for the Add New wizard" on page 202.

Control over the object parent information when exporting data

You can configure the FastMap export template to optionally include the object parent information when you export data in IBM OpenPages GRC Platform.

The resulting FastMap format worksheet can be used to load the objects and their associations to another system that does not contain these object and association instances, but has the same configured object types and associations, fields, and profiles. The data on the loaded target system will be the same as on the source system from which the content was exported.

For more information about the new FastMap parameters, see "FastMap parameters for importing and exporting data" on page 644.

The OpenPages folder is opened automatically in the Administration Settings folder hierarchy

To speed navigation in the user interface, the OpenPages folder is automatically opened in the **Administration** > **Settings** folder hierarchy.

The folder is hidden in the user interface; however, it is still part of the settings path. To author an XML settings path, you still include the OpenPages folder after the Settings folder in the path. For example: **Administration** > **Settings** > **OpenPages** > **Applications**.

Task-oriented hyperlinks

You can now add hyperlinks that point directly to views and filters in IBM OpenPages GRC Platform where users need to perform tasks. The hyperlinks can be added from internal or external locations, and can also include filters.

For example, in a notification email to a risk owner, you can include a hyperlink to the **Rate This Risk** Activity View if the risk is ready to be rated, but a hyperlink to the **Assess the Controls for Risks** Activity View if the risk controls need to be assessed. Additionally, an email to a person responsible for collecting KRI values could contain a hyperlink to the **Enter KRI Values** Grid View with the **My KRIs with Values to be Entered** public filter applied.

This new capability allows you to create hyperlinks that are task focused and applicable to the object lifecycle stage.

You can create hyperlinks that include the following target views:

- The Detail View for a specific object instance, in read-only mode.
- A specific activity view for an object instance.
- The Filtered List View for a specific object type with a public filter applied.
- A specific grid view for an object type with a public filter applied.

You can add hyperlinks from the following locations:

- OpenPages reports.
- Notification emails.
- OpenPages JSP helper applications.
- Within the IBM OpenPages GRC Platform application, using computed fields or URL link fields.

For more information, see "Task-oriented hyperlinking" on page 801.

Task focused home page

Home page filtered lists can now be made task focused.

Using new configuration settings, administrators can control the fields that are displayed, specify the detail or activity view to be used for the Name hyperlink target, and specify the filtered list view or specific grid view to be used for the **Show All** hyperlink target. This is intended to direct users to a view that is appropriate for the task for which the list was generated rather than to the generic user interface.

For more information, see "Home page settings" on page 333.

Changed features in version 7.1.0

The following features are changed in IBM OpenPages GRC Platform version 7.1.0.

Default folder for adding new child objects
When you create a new object, the system uses the default folder setting to determine in which folder to create child objects.

In previous releases, when the **parent_entity** folder was set as the default folder, child objects were added to the next level parent folder.

In this release, when the **parent_entity** is set as the default folder, new child objects are added to the **parent_entity** folder.

For more information, see "Controlling the default folder for new child objects " on page 207.

Marking fields as read-only on user profiles
Administrators can define field-level settings in various areas of the system.

In previous releases, the read-only setting was defined at the user profile level. This configuration is no longer available through the administrative user interface. If you upgrade from an older version, the Add New view no longer honors the read-only setting defined at the profile level.

New features in version 7.0.0

The following features are new in IBM OpenPages GRC Platform version 7.0.0.

Visualizations

As a Risk analyst or Compliance manager, you can graphically render your business process and communicate it to other users of risk analysis.

You can create interactive visualizations to communicate information about the process flows and the Business Entity hierarchical structure.

The following are the new visualization object types:

- Process Diagram
- Data Input
- Data Output

For more information, see Chapter 6, "Business process visualizations," on page 95.

Security rules

Use security rules to define a more granular control over the access to individual objects in a folder. For example, two GRC domains share a common organizational hierarchy. They share some common object instances, such as processes, but they do not want to share other object instances, such as risks and controls. If you do not create security rules on objects, folder-based security applies.

For more information, see Chapter 4, "Security," on page 43.

Grid view

The grid view allows you to select how information about an object is displayed by selecting an option from the View selector. Options include the ability to display objects that match the selected filter or the folder view of an object. Select a grid view to display information about more than one object. From the grid view, you can add a new item and update one or more items.

You can use the Bulk Update feature to update multiple objects in the grid view during one editing session. For example, you can update all objects assigned to User A and assign them to User B.

Filtered List views and Folder views have been consolidated with the new grid views.

For more information, see “Grid views” on page 238.

Info Card

The Info Card is displayed when you hover over an object. The card allows you to quickly understand and review an object definition.

The Info Card is available from the grid view.

New multi-selector actor field types

New field types allow you to select multiple actors when selecting users, user groups, or both users and user groups.

Orphan system field

The new Orphan system field allows you to see and filter on the objects with no parents. You can also filter on objects that have parents but do not have a path to a business entity.

IBM OpenPages Software Development Kit

A new OpenPages SDK allows users to access and manipulate OpenPages platform data programmatically. This offering includes a REST API and Java API working samples that demonstrate typical use cases and reference documentation to help you understand and use the APIs.

The following API documents were added in this release and they are available from your installation.

- *IBM OpenPages GRC Platform API Javadoc*
- *IBM OpenPages GRC Platform REST API Reference Guide*
- *IBM OpenPages GRC Platform Trigger Developer Guide*

Changed features in version 7.0.0

This section lists are features that are changed in version 7.0.0 of IBM OpenPages GRC Platform.

Changes to the user interface

Improved icons make it easier for you to identify the commands that you need. To view the updated icons, users must clear their web browser's cache after upgrading to version 7.0.0.

Changes to menus

The contents of the **Administration**, **Reporting**, and **MyOpenPages** menus have been reorganized.

The **Workflow Console** is available on the **Administration** menu. The **Workflow Console** was formerly called the IBPM Console.

Changes to the configuration of the menu bar do not take effect immediately. The next time that you log in, you will see the changes that you have made to the menus.

Page size setting for Filtered List views

The **Page Size** setting for Filtered List views is no longer required to be used and is ignored. Instead, rows are loaded as you scroll through the Filtered List view.

Actor fields

Actor fields can now be Field Dependency controllers.

Object views

You can now change the order of Detail and Activity object views.

Filters

Quick Filter and Advanced Filter have been consolidated. When you press **Enter**, the Quick Filter is applied.

Some actions take effect immediately

Some actions, such as View Selection and Reporting Period, take effect immediately when you select them. You are no longer required to click Go or View.

Paginate Actor Tables and Use Actor Search Only settings are no longer required

There are no longer two possible interfaces used for selecting user lists and group lists in the administration user interface. Where the type-ahead search and filterable listing of users or groups were available, you have the option of selecting users or groups.

The **Paginate Actor Tables** and **Use Actor Search Only** settings under /OpenPages/Applications/Common/Administration/Users and Groups are now ignored and are treated as though their values are always **true**.

To control the number of rows listed per page, use the **Page Size** setting under /OpenPages/Applications/Common/Administration/Users and Groups.

Chapter 2. System Administration Mode (SAM)

Use System Administration Mode (SAM) to restrict user access to when you apply configuration changes or other updates to the system.

When System Administration Mode (SAM) is enabled, the following conditions are enforced:

- 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 “Asynchronous background jobs and administrative functions” on page 385).

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, Chapter 5, “Managing the reporting schema ,” on page 89.
- 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 “Data types” on page 143 for multi-value conversion details).
- Set up field level security.

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 Administration Mode

You can enable and disable the system admin mode.

You must have the **System Administration Mode** application permission set on your account to view the **System Admin Mode** link and the **System Admin Mode** menu item from the **Administration** menu.

Table 6: Settings for System Administration Mode

If Link...	**Use to...**
Enable	enter System Administration Mode
Disable	exit and terminate System Administration Mode

The link switches between **Enable** and **Disable** depending on which mode it is in.

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

Procedure

1. Log on to the IBM OpenPages GRC Platform user interface as a user with the **System Administration Mode** permissions.
2. Do one of the following:
   - Click the **Enable** or **Disable** link.
   - From the menu bar, select **Administration** and click **System Admin Mode** and click **Enable** or **Disable**.

Chapter 3. Users, groups, and domains

Access within the IBM OpenPages GRC Platform application is administered through the use of users, groups, and domains.

To create and administer users and groups, you must have administrative privileges.

- To access the **Users** menu item, you must have **Browse** permission on any security domain or any user group.
- To access the **Users, Groups and Domains** menu item, you must be a Super Administrator or a delegated administrator with any administrator permission. For information about delegating and assigning administrator permissions, see “Delegate administrator permissions” on page 21.
- For information about the administrative permissions that are required for specific user-provisioning functions, see “Types of administrator permissions” on page 21.

Users and groups are organized under the following top-level groups:

-  Security Domains - this group is 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 administrators with appropriate permissions. For an overview of security domains, see “Security domains” on page 48.

  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.

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

-  Workflow, Reporting and Others - this group is 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 groups under the Workflow, Reporting and Others group, and later associate them to different security domains. For upgrade customers, this top-level group also includes the groups that existed in prior releases of OpenPages GRC Platform.

  To navigate to a group detail page, you must be a super administrator or a delegated administrator of that group with at least **Browse** administrative permission. For information on delegating administrator permissions, see “Delegate administrator permissions” on page 21.

Note: The term group includes both organizational and security domain groups, unless otherwise specified.

Planning user administration

There are numerous things to consider before you create, modify, or copy a user account.

The following list outlines the tasks that you should perform before you begin creating, modifying, or copying users:

1. Determine whether you want to integrate IBM OpenPages with your LDAP servers to allow prepopulation of user information when you create a new user in IBM OpenPages. If so, then perform one or both of the following actions:
   - If you are using LDAP over SSL/TLS, setup your certificates.
   - Configure access to your LDAP servers from IBM OpenPages.
2. Determine whether you want to allow the creation or updating of users based upon existing users. The user will have the same attributes, such as locale, profiles, group memberships, role assignments, and reports access, as another user. If so, then perform the following actions:

- Determine which users can be used as source for the Copy Access From operation.
- Determine whether you want to allow inactive users to be the source for the Copy Access From operation.
- Configure the default behavior for the Locale, Profiles, Group Memberships, Direct Role Assignments, and Direct Reports Access attributes during the Copy Access From operation.
- Determine whether the Copy Access From operation adds to or replaces a user or group's existing attributes.

3. Determine the default values for the following settings:
   - The default value or values for the Allowed Profiles.
   - The default value for the locale.
   - The number of rows that are listed per page in the Reports Access table.
4. Determine the password behavior for users by performing the following actions:
   - Configure the default change password behavior when you create a new user.
   - Configure the default password expiration behavior.
5. If user provisioning is configured in your system to allow copying attributes from inactive users, determine whether you want to create template users as inactive users. The inactive template users should have similar attributes that you want to copy to other users. The administrator can modify attributes after the copy operation.
6. Determine whether you want to add administrators who can perform user provisioning tasks beyond the super user. For example, you can create administrators who perform only password management tasks for users, while other administrators can create users.

   Note: As of version 7.4, you must now assign delegated administrators rights at the top-level security domain and the top-level user group to perform some user-provisioning functions. For more information, see “Administrator permissions for user-provisioning functions” on page 22. For these functions, you can separate out the tasks the delegated administrators can do but can no longer separate out which places they can perform them.
7. Determine whether you want to primarily manage administrative rights, such as managing profiles, role assignments, and reports access, directly at the user level or by making users members of user groups. You can use a combination of methods. It is strongly recommended that you manage administrator rights via user groups.
8. Determine the groups and security domains that you want each user to belong to. By default, when you create a new user from scratch, that user belongs to a special group called Standalone Users and Groups. Only the Super Administrator has administrative access to this group. 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, the system makes that user or group a member of Standalone Users and Groups.

   For more information about group memberships, see “Associating and disassociating a group” on page 31.
9. Determine the profiles that you want the users to have.

   For more information about choosing profiles, see Chapter 11, “Profiles,” on page 213.
10. Determine the role assignments that you want the user to have.

    For more information about role-based security and role templates, see “Role-based security model” on page 43.
11. Determine the reports that you want the users to have access to.

    For more information about modifying reports access, see Chapter 7, “Managing reports,” on page 109.

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 installation, the Super Administrator is the only user in the system. In an upgrade installation, you 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. A Super Administrator can delegate administration activities by assigning roles to users through the use of Role Templates (for more information see "Role templates" on page 51) and group administrator permissions (for more information, see "Delegate administrator permissions" on page 21).

Delegate administrator permissions

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 one administrator who would only have the ability to reset passwords for users, another who could lock and unlock users, and a third who could create users and associate them to user groups and assign them role templates.

For more information about entity groups, see "Security context points" on page 45). 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

You want to designate Mary Smith as an administrator who can reset passwords for any users. You would assign the **Reset Password** permission to Mary Smith.

Note:

- When 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 25.
- Security domain groups are not displayed in the User/Group selector list.

Note: Administrators with **Settings** application permission can configure the behavior of some user-provisioning functions. For more information, see "User provisioning settings" on page 312.

Types of administrator permissions

There are six security management permissions that you can delegate to a security domain or user group administrator.

Table 7: Administrator permissions	
Permission	**Description**
Manage	Allows the delegated administrator to create, modify, and associate users and groups.
Lock	Allows the delegated administrator to lock a user account, which prevents logon to the IBM OpenPages GRC Platform application from that account. With this permission, a **Lock** link can be clicked in the **User Information** section of the **View, Edit, or Disable User** page.
Unlock	Allows the delegated administrator to unlock a previously locked user account. With this permission, an **Unlock** link can be clicked in the **User Information** section of the **View, Edit, or Disable User** page.
Reset Password	Allows the delegated administrator to reset passwords for users.
Assign Role	Allows the delegated administrator to assign one or more roles to users and groups and to revoke a role from a user or group. This permission applies to security domains only.
Browse	Allows the delegated administrator to view users and groups within that group. This permission is selected by default.

Administrator permissions for user-provisioning functions
You must have the appropriate administrator permissions to perform each user-provisioning function.

Table 8: Permissions required for user provisioning functions	
To do the following...	**You must have these permissions...**
View the **Users** menu item on the **Administration** menu and the **View, Edit, or Disable User** field on the **Users** landing page	**Browse** on any security domain or any user group.
View the **Create User** button on the **Users** landing page and create new users	**Manage** on any security domain or any user group. If LDAP Server integration is configured, there is an additional field that you can use to search for user in LDAP Server and prepopulate their user information. For more information, see “LDAP and user provisioning” on page 25.
Edit user information	**Manage** on any security domain or any user group that includes the user account.

Table 8: Permissions required for user provisioning functions (continued)	
To do the following...	**You must have these permissions...**
Enable and disable user accounts	**Manage** on any security domain or any user group that includes the user account. To clear direct role assignments when you disable a user account, you must have **Assign Role** on the root security domain. To clear group memberships when you disable a user account, you must have **Manage** on the top-level user group. To clear direct reports access when you disable a user account, you must belong to the OPAdministrators group. Note that an administrator cannot disable their own account. For information about the difference between disabling and locking user accounts, see “Modifying user accounts” on page 28.
Lock user accounts	**Lock** on any security domain or any user group that includes the user account. Note that an administrator cannot lock their own account.
Unlock user accounts	**Unlock** on any security domain or any user group that includes the user account.
Edit user passwords This includes the **Password** and **Confirm Password** fields.	**Reset Password** on any security domain or any user group that includes the user account.
Configure password options and edit configured password options This includes the following options: **User must change password at next log on**, **User cannot change password**, **Password never expires**, **Password expires in <n> days**, and **Force Password Change**.	**Manage** on any security domain or any user group that includes the user account. Note that an administrator can force a password change for their account and reset their password.
Edit a user's locale and profile information	**Manage** on any security domain or any user group that includes the user account.
Modify a user's group memberships	**Manage** on the top-level user group.
Add role assignments to a user	**Manage** and **Assign Role** on the root security domain.
Remove role assignments from a user	**Assign Role** on the root security domain.
View a user's reports access	OPAdministrators group membership. Information is read-only.

Table 8: Permissions required for user provisioning functions (continued)	
To do the following...	**You must have these permissions...**
Copy access from one user to a new or existing user This includes locale, profiles, group memberships, and direct role assignments.	**Manage** on the top-level user group and **Manage** and **Assign Role** on the root security domain.
Copy direct reports access from one user to a new or existing user	**Manage** on the top-level user group, **Manage** and **Assign Role** on the root security domain, and OPAdministrators group membership. Information is read-only.

Example

Figure 1 on page 24 shows a diagram with a sample security administration structure.

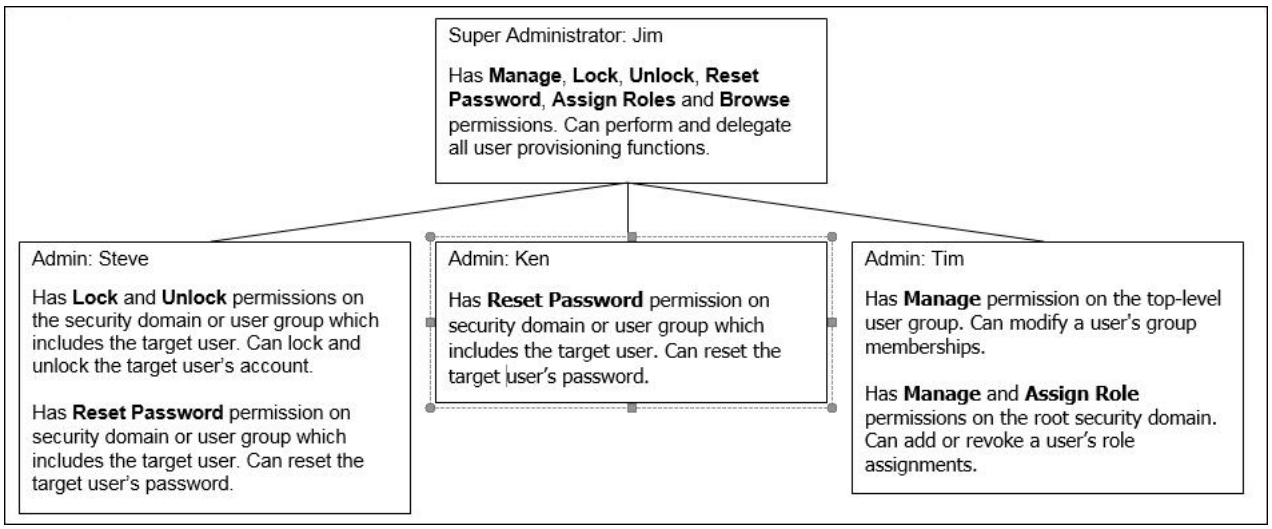


Figure 1: Sample security administration

Assigning administrator permissions

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

Procedure

1. Click **Administration** > **Users, Groups and Domains**.
2. On the **Users, Groups and Domains** page, click the name of the group for which you want to assign administrative permissions to selected users.
3. On the detail page of the selected group, go to the **Administrators & Permissions** tab.
4. Click **Assign**.
5. Select (user icon) or search for a user (magnifying glass icon).
6. From the **Permissions** column, select the administrative permissions that you want to assign to this user (see "Types of administrator permissions" on page 21 for a list of permissions). To select all permissions, select the **Permissions** box in the column heading.
7. When finished, click one of the following icons:
   - **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 that are assigned to a user at any time.

Procedure

1. Click **Administration** > **Users, Groups and Domains**.
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, go 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 (see "Types of administrator permissions" on page 21 for a list of permissions).
6. Click **Save**.

Revoking administrator permissions

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

Procedure

1. Click **Administration** > **Users, Groups and Domains**.
2. Click the appropriate group, and on the **Users, Groups and Domains** page, select the check box next to the name of each user in the **Adminisrators** list for whom you want to revoke administrative permissions.
3. Click **Revoke**. The name of the user is removed from the list of group administrators.

LDAP and user provisioning

You can configure access to your LDAP server or servers from IBM OpenPages GRC Platform so that you can access user information from your LDAP server or servers when creating users in IBM OpenPages.

Through an LDAP server integration with IBM OpenPages, you can search your company's LDAP servers for a list of people who meet the search criteria. You can then select a user from the list and the information fields in the **Create User** wizard will be pre-populated with the user's information from the LDAP server.

Note: LDAP configuration for user provisioning does not affect LDAP user authentication.

This video demonstrates how to configure access to your LDAP server or servers from OpenPages so that you can access user information from your LDAP server or servers when creating users in OpenPages:

https://youtu.be/GfGNCSIakQI

Importing an LDAP certificate to the local trust store

If you are using LDAP over SSL/TLS, you must import an LDAP certificate to the local trust store before you can configure LDAP for user provisioning. It is needed to build an SSL communication between the OpenPages GRC Platform servers and your LDAP over SSL/TLS server.

Before you begin

The target secure server application from which you are going to retrieve the certificate must be running and listening on the port.

About this task

You can use the **Retrieve from port** option in the IBM WebSphere administrative console to retrieve the certificate. The root certificate contains the public key and has been verified by the certificate authority (CA).

Procedure

1. Log on to the IBM WebSphere administrative console.
2. Expand **Security** and click **SSL certificate and key management**.
3. Under **Related Items**, click **Key stores and certificates** and click the **CellDefaultTrustStore** keystore.
4. Under **Additional Properties**, click **Signer certificates** and **Retrieve from port**.
5. Enter the host and port information.
   - **Host**: This is the name of your LDAP server.
   - **Port**: This is the port where your LDAP server is running, for example, 636.
   - **Alias**: Enter a descriptive name for the certificate, for example, `ldap1`.
6. Click **Retrieve signer information**.
7. Verify that the certificate information is for a certificate that you trust.
8. Click **Apply** and then click **Save**.
9. Restart the OpenPages GRC Platform services.

Configuring LDAP access for user provisioning

You can configure access to your LDAP server to import LDAP user information when creating users in IBM OpenPages GRC Platform.

Before you begin

To configure LDAP access for user provisioning, you must be a member of the OPAdministrators user group and have the following application permission; **All Permissions** > **SOX** > **Administration** > **LDAP Server**.

If you are using LDAP over SSL/TLS, make sure you have completed the preconfiguration task.

Procedure

1. Click **Administration** > **User LDAP Configuration**.
2. Click **Add New**.
3. Type a name for the LDAP configuration and click **OK**.

   Note: You can configure multiple LDAP servers so that the **Create User** wizard shows the search results from all LDAP servers at once. The maximum number of search results, is the sum total of the maximum results of each LDAP server configured.
4. In the **Provider URL** field, type the LDAP service provider that you want to use.

   The value should contain a URL string, such as `ldap://<hostname>:389`.

   Note: If you are using LDAP over SSL/TLS, there are some additional preconfiguration steps that you must perform. An example for the **Provider URL** when using LDAP over SSL/TLS is the following string: `ldaps://<hostname>:636`.
5. In the **First name attribute** field, **Middle name attribute** field, and **Last name attribute** field, type the attribute names that you want to map to the IBM OpenPages user's first name, middle name, and last name respectively.

   Note: The middle name is not displayed in IBM OpenPages by default. To display the middle name in the search results of the **Create User** wizard so that you can differentiate users who have the same first and last name, you can add the following code to the **Singular Label** box of the **com.display.name.format** entry under the **Formats** folder on the **Application Text** page: `%MN`. For

more information, see “Modifying the user name format” on page 283. The middle name is not stored in IBM OpenPages.

6. Click **Validate** to ensure you have filled out the form correctly.

   If you have missed a required field or entered incorrect information, an error message is displayed at the top of the screen.

7. After you have successfully validated the information, click **Save**.

Provisioning users

Your ability to create a new user, modify user accounts, and copy access from one user to another is based on your administrative permissions and the way user provisioning is configured in your system. The user-provisioning options that you see in the product are determined by your permissions and configuration.

You can delegate administrative capabilities to specific administrators to give them the ability to perform certain user-provisioning functions. For example, you could delegate permission to two administrators to manage user passwords, and delegate permission to three other administrators to create users and update group memberships.

For information about which administrator permissions are required for each of the user-provisioning functions, see Table 8 on page 22.

Creating user accounts

You create new user accounts with the **Create User** wizard.

Before you begin

Before you create a new user, see “Planning user administration” on page 19.

About this task

Depending on your permissions and user provisioning configuration, you can copy access from an existing user to a new one. You can also copy access from one existing user to another. For more information, see “Modifying user accounts” on page 28.

Depending on your delegated administrator permissions, you can perform certain functions when you create a user account, such as associating group memberships and assigning roles. For information about which permissions you need for each operation, see “Administrator permissions for user-provisioning functions” on page 22.

This video demonstrates how to create new user accounts:

https://youtu.be/YGeSsw5PszU

Procedure

1. Click **Administration** > **Users**.
2. Click **Create User**.

   Note: If LDAP is configured with your IBM OpenPages GRC Platform application, a **Search** field is displayed. This allows you to search for an LDAP user whose information you want to copy to create the new IBM OpenPages user. You can type a user name, first name, last name, or email address into the **Search** field. Select the LDAP user from the list to access the **Create User** page. For information about configuring access to an LDAP server, see “Configuring LDAP access for user provisioning” on page 26.

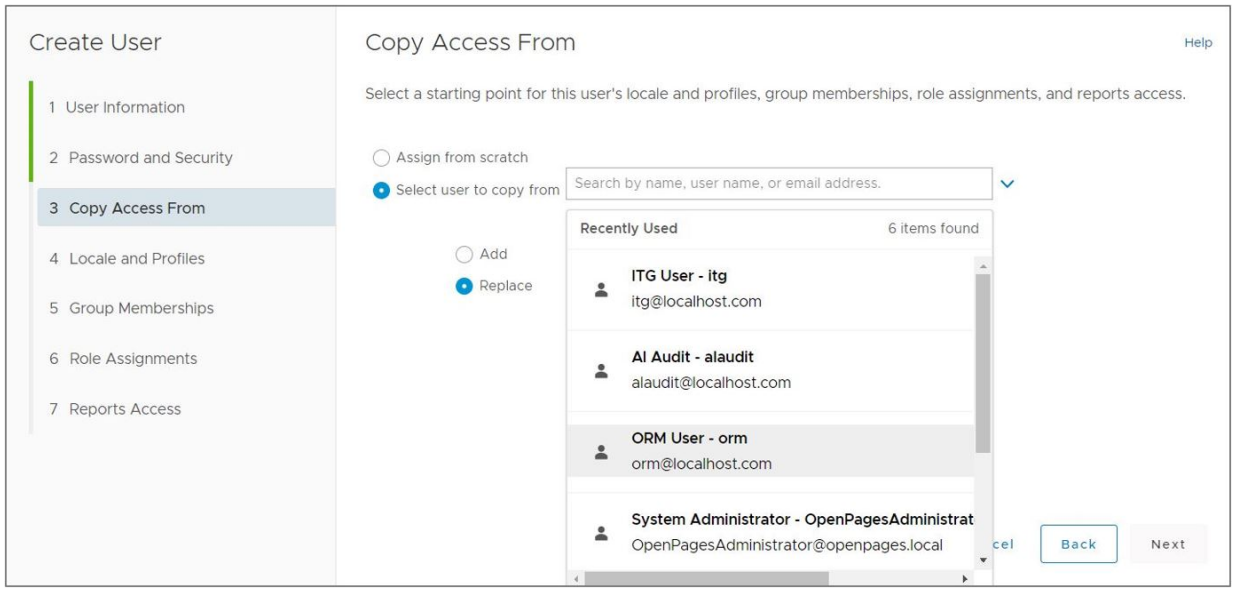
3. Complete the information on the **User Information** and **Password and Security** pages of the **Create User** wizard.

   When you create user names and passwords, the following rules apply:

- User names are case-sensitive. For example, `MyName` and `myname` would be two unique users.
- User names can be up to 256 characters.
- User names can contain alphanumeric characters and any of the following special characters: `@-!._/:*\"#%?<>`

  To exclude characters, including special characters, from user names, specify these characters in the **Illegal Characters** setting. For more information, see “Exclude characters from user names” on page 341.
- Passwords can contain up to 32 characters and cannot contain spaces.

4. If you have the necessary permissions, you can copy access from another user to determine the starting point for a new user's attributes, such as group memberships, role assignments, and reports access. On the **Copy Access From** page, perform one of the following actions:
   - Click **Assign from scratch**, and then click **Next**.
   - Click **Select user to copy from**.
     - Search for the user that you want to use as source for the copy operation. You can type a user name, first name, last name, or email address to find a user.
     - Click **Next**. The following pages of the **Create User** wizard reflect the locale, profiles, group memberships, role assignments, and reports access of the source user. Personal filters are not copied.



5. On the **Locale and Profile** page, you can specify the user's locale, choose one or more profiles to associate with the user, and select a **Current Profile**.
6. On the **Group Memberships** page, perform the following actions to assign group memberships:
   - To select group memberships, click **Associate Groups** and select the check boxes next to the groups to which you want the user to be a member.
   - To delete group memberships, click the **X** next to the membership that you want to remove.
7. On the **Role Assignments** page, you can view the user's role assignments.

   You can assign roles after the user is created.
8. On the **Reports Access** page, you can view the user's reports access.
9. Click **Finish**.

Modifying user accounts

You can view and modify the details of an existing user account, such as all the user's group memberships, role assignments, and profiles.

Before you begin

Before you modify user information, see “Planning user administration” on page 19.

About this task

Depending on how user provisioning was configured in your system, you might be able to copy access from one user to another. For information about copying access, see “Copying access from one user to another” on page 30.

Depending on your delegated administrator permissions, you can perform certain functions when you modify a user account, such as editing user information, enabling or disabling a user account, and changing group memberships. For information about which permissions you need for each editing operation, see “Administrator permissions for user-provisioning functions” on page 22.

There are some constraints on your ability to make changes. For example, you cannot disable or lock yourself or the super user (OpenPagesAdministrator) or the OPSystem user. You cannot remove a user from special user groups that contain all users, or all users who are not associated with any other user group.

Procedure

1. Click **Administration** > **Users**.
2. In the **View, Edit, or Disable User** field, search for the user account that you want to modify.

   When you click in the **View, Edit, or Disable User**, a list of users that you recently worked with is displayed. You can select one of these users or search for a different user.
3. In the **User Information** section of the **View, Edit, or Disable User** page, you can perform one or more of the following actions:
   - Edit user details, such as email, first name, and last name. You cannot change a user name.
   - Disable and enable a user account. When an account is disabled, the user of that account is prevented from logging in, and the user is displayed as inactive and grayed out in user selector lists. If necessary, you can re-enable a disabled user account. User accounts cannot be deleted through the user interface in IBM OpenPages. Depending on how your system is configured, in addition to disabling the user, you can choose to remove their locale, profile, group membership, role assignment, or reports access.

     Tip: If you want to prevent a user from logging in, but you still want the user to appear in user selectors, disable the user and then update the user selectors to set **Include Disabled** to **True**. For more information, see “Configure user and group selectors display types for simple strings” on page 266.
   - Lock and unlock a user account. Depending on your configuration, users might be locked automatically if they exceed a set number of unsuccessful login attempts. When an account is locked, the user of that account is prevented from logging in. The user is displayed as active but locked in user selector lists, and they can be selected. If you do not want the user to appear as active and selectable in user selector lists, disable the user account instead.
   - Reset the user's password or force the user to change the password the next time they log on. Passwords can contain up to 32 characters and cannot contain spaces.

     Important: If you use IBM OpenPages Loss Event Entry, do not change the dedicated users' passwords by using OpenPages. Always use the Loss Event Entry Configuration tool to change the passwords. If you change the passwords in OpenPages, users cannot use Loss Event Entry because the passwords are out of sync.
4. In the **Locale and Profile** section, you can change the user's locale, change the **Allowed Profiles**, and select a different **Current Profile**.
5. In the **Group Memberships** section, you can add and remove group membership assignments by clicking **Associate Groups**.
6. In the **Role Assignments** section, you can add role assignments by clicking **Assign Roles**.

You can remove role assignments that were assigned directly to the user. You cannot remove role assignments that are inherited from group memberships.

When you remove a role from a user or group, the role assignment is explicitly removed from the user or group on a given entity.

7. In the **Reports Access** section, you can view the reports folder access that was assigned directly to the user and inherited from group memberships.

Copying access from one user to another

You can copy a user's locale, profiles, group memberships, and direct role assignments. You can also copy direct reports access attributes to another user.

Before you begin

Before you copy access from one user to another, see "Planning user administration" on page 19.

To copy access from one user to another, you must be granted **Manage** permission at the top-level group and **Assign Role** and **Manage** permissions at the root security domain. If you do not have these permissions, you cannot see the **Copy Access From** option.

Administrators with **Settings** application permission can use the user provisioning registry settings to establish the following copy access behavior:

- Determine whether the copy operation is allowed and which users, including inactive users, can be used as sources for the copy operation. For more information, see "Users Can Copy Access From" on page 313 and "Copy Access From Inactive" on page 312.
- Specify which attributes are copied by the copy operation. For more information, see "Copy User Info Attributes" on page 312.
- Determine whether the copy operation adds to or replaces the user's existing attributes. For more information, see "Copy User Info Choice" on page 312.

Procedure

1. Click **Administration** > **Users**.
2. In the **View, Edit, or Disable User** field, search for the user account that you want to modify.

   Note: You can also copy access from an existing user when you are creating a new user. For more information, see "Creating user accounts" on page 27.
3. From the left pane, click **Copy Access From**.
4. Search for the user that you want to use as source.
5. Click **Copy**.

   Note: This does not include copying personal filters.

Creating an organizational group

Users with the correct permissions can create groups by 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. Click **Administration** > **Users, Groups and Domains**.
2. Expand the list and click the name of the group to which the new group belongs. If no higher-level group for the new group exists, select the **Workflow, Reporting and Others** group.
3. On the detail page of the selected group, go to the **Groups** tab and click **Add New**.
4. Complete 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 **Groups** section.

5. If you want to add users to the group or modify the group permissions, click the name of the new group to view the detail page.

Associating and disassociating a group

You can associate and disassociate groups from other groups.

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

When you add an existing group to another group, the disassociated group is still available in the group selector list.

Procedure

1. Click **Administration** > **Users, Groups and Domains**.
2. Expand the list and click the name of the group to which you want to associate another group, or to which the soon-to-be-disassociated group belongs.
3. Go to the **Groups** tab and select the check box next to each group to be associated or disassociated.
4. Click **Associate** or **Disassociate**.

Defining application permissions

You can define access permissions for IBM OpenPages GRC Platform in the application user interface.

The following methods of defining permissions are available:

- 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 information, see “Role templates” on page 51.
- 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 information, see “Creating an organizational group” on page 30.

Setting 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 users in that group can lock objects, view audit trail information, and create reporting periods.

To delegate group security management permissions to administrators, see “Delegate administrator permissions” on page 21.

To assign application permissions for a role, see “Accessing the role templates page” on page 51.

Procedure

1. Click **Administration** > **Users, Groups and Domains**.
2. Expand the list and click the name of the group whose application permissions you want to view or modify.
3. On the detail page of the selected group, go to the **Permissions** tab.

   Tip: Most of the application permissions in IBM OpenPages GRC Platform 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 "Types of application permissions" on page 32 and "Application permissions not contained under the SOX heading" on page 35.
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 "Delegate administrator permissions" on page 21.

Types of application permissions

Administrators can use a set of application permissions to limit the activities of the various users and user groups that can access the IBM OpenPages GRC Platform application. The application permissions reside under the SOX permissions heading and can be applied to OpenPages GRC Platform user groups.

Important: If the changes to application permissions result in changes to menus, the menu changes do not appear until users log out and then log back in to the application.

Users are generally granted the applicable permissions by being assigned to role templates that include those permissions.

Administration permissions

When you create an administrative-level group, you must grant them Administration permissions. If a user or user group possesses any of these permissions, they see the **Administration** menu on the menu bar.

Table 9: Administration application permissions

Permission	Description
Access Control Lists	Allows super administrators to view, edit, and remove the access control listings for objects through the **Custom Security** menu item on the **Administration** menu. For more information on Access Control Lists (ACLs), go to "Role-based access control permissions" on page 49.
Application Text	Allows users and members of user groups to view and edit locale-specific application label values through the **Application Text** menu item on the **Administration** menu.
CompareEnvironments	Allows users and members of user groups to use the Compare Environments tool through the **Administration** > **Compare Environments** menu item.
Currencies	Allows users and members of user groups to administer currencies.
ExportConfiguration	Allows Super Administrators to access the environment migration tool to export configuration items for import into another system. See Chapter 22, "Migrating OpenPages GRC Platform environments," on page 575.

Table 9: Administration application permissions (continued)	
Permission	**Description**
Field Groups	Allows users and members of user groups to view and manage the configuration of field groups with their related field definitions through the **Field Groups** menu item on the **Administration** menu.
IBM BPM	Allows users and members of user groups who work with IBM Business Process Manager to access the following menu items on the **Administration** menu: **IBM BPM Process Center**, **IBM BPM Process Inspector**, and **IBM BPM Process Admin**.
ImportConfiguration	Allows Super Administrators to access the environment migration tool to import configuration items that are exported from another system. See Chapter 22, "Migrating OpenPages GRC Platform environments," on page 575.
Object Profiles	Allows users and members of user groups 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 users and members of user groups to reset objects for a new reporting period. For information on governing reset behavior, see Chapter 14, "Reporting periods, object resets, and rulesets," on page 289.
Object Text	Allows users and members of user groups to view and edit locale-specific object label values through the **Object Text** menu item on the **Administration** menu.
Object Types	Allows users and members of user groups 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.
RCA Integration	Allows users and members of user groups who work with IBM Regulatory Compliance Analytics to access the following menu items on the **Administration** menu: **RCA Integration** > **Configure Import from RCA** and **RCA Integration** > **Import from RCA**.
Reporting Framework	Allows users and members of user groups to generate and manage the reporting framework through the **Reporting Framework** menu item on the **Administration** menu.
Reporting Framework Configuration	Allows users and members of user groups to administer and configure the reporting framework through the **Reporting Framework** menu item on the **Administration** menu.
Reporting Periods	Allows users and members of user groups to finalize and reapply Reporting Periods through the **Reporting Periods** menu item on the **Administration** menu. **Finalize** allows users and members of user groups to finalize the active Reporting Period. **Reapply** allows users and members of user groups to reapply the active Reporting Period.
Reporting Schema	Allows users and members of user groups to manage the Reporting Schema through the **Reporting Schema** menu item on the **Administration** menu.

Table 9: Administration application permissions (continued)	
Permission	**Description**
Role Templates	Allows users and members of user groups to view, add, and manage roles through the **Role Templates** menu item on the **Administration** menu.
Search	Allows users and members of user groups to manage and maintain global search operations through the **Global Search** menu item on the **Administration** menu.
Security Rules	Allows users and members of user groups to manage and maintain security rules through the **Security Rules** menu item on the **Administration** menu.
Settings	Allows users and members of user groups to view and manage settings through the **Settings** menu item on the **Administration** menu.

IBM CommandCenter Studio permissions

This application permission allows users and members of user groups to access Cognos Analytics by launching the **Cognos Analytics** menu item on the **Reporting** menu.

Table 10: IBM Command Center Studio permission	
Permission	**Description**
Cognos Analytics	This application permission enables the Cognos Analytics portal through the **Reporting** > **Cognos Analytics** menu item. Use the Cognos Analytics portal to access your Cognos software and corporate data. Depending on your access permissions, you can create, update, run, and distribute reports, dashboards, stories, and cubes, create and run agents, or schedule entries.

Change History permission

Change History application permission allows users and members of user groups to review the selected Reporting Period to view historical information about objects.

With this permission enabled, a **Change History** option can be selected on the object's detail page.

For more information, see “Reporting period interactions” on page 290.

Note:

- When you copy objects, change histories are not copied with the object. The copy of the object has no change history because it is a new object.
- When you add new fields to an object type, the OpenPages GRC Platform administrators might see a blank to blank change in the change history because the fields were not previously available.

Browse Files permission

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

Folders permission

This application permission enables users and members of user groups 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 permission

This application permission allows users and members of user groups 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 to the role-based security model. For new first-time installations, this permission is not honored.

Project Management permission

If your system is configured to enable Project Management, this application permission allows users and members of user groups who are assigned role templates that include the permission to use the Milestone and Milestone Action Item Project Management capabilities available through the **Project** menu item on the **My OpenPages** menu.

View Locks permission

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.

Application permissions not contained under the SOX heading

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

Users are generally granted the applicable permissions by being assigned to role templates that include those permissions.

All permission

Grants users and members of user groups all permissions and access to every functional and administrative area within OpenPages GRC Platform (web and server).

Administration permissions

The Administration permissions grant users and members of user groups the ability to archive and restore document versions and to enable and disable System Administration Mode.

Table 12: Administration permissions

Permission	Description
Archive Management	Allows group members to archive and restore document versions.

Table 12: Administration permissions (continued)	
Permission	**Description**
System Administration Mode	Allows group members to enable and disable System Administration Mode and perform certain administrative functions. For details see, "Enabling and disabling System Administration Mode" on page 17.

Files permissions

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

Table 13: Files permissions	
Permission	**Description**
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. **Restriction:** This permission applies only to file attachments (of the SOXDocument object type).
Lock	Allows group members to lock objects, 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** icon 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 subtrees.
Unlock	Allows group members to unlock objects.

Publishing permissions

The **Add Pages** permission grants administrative permissions to make Cognos and jsp reports available from the OpenPages GRC Platform application user interface.

Table 14: Publishing permissions	
Permission	**Description**
Add Pages	Allows group members to add reports.

Configure password requirements

IBM OpenPages GRC Platform 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: Configuring password behavior in OpenPages GRC Platform does not apply if you use single sign-on (SSO), such as LDAP or Microsoft Active Directory. Your internal IT policies dictate password behavior within the product.

Configuring password policies

The IBM OpenPages GRC Platform allows administrators who can access the Settings administrative section to modify the password policies 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 in **Administration** > **Settings** > **Platform** > **Security** > **Password**) as described in Table 15 on page 37:

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Table 15: Password Settings

Setting	Description
Encryption Administrator	The user name who is allowed to change the password encryption algorithm and the encryption key.
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 is required to contain at least one character from each group. If a group is empty, that group is ignored. **Important:** You cannot include the comma as a required character in a strong password.
Strong Policies - Enabled	If the value is set to: • `true` - then users are required to enter strong passwords when they specify their user password. • `false` - then users are not required to enter strong passwords when they specify their user password. This value is set by default.
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.

Configuring password encryption

You can modify the encryption algorithm, and change the key that is used by the encryption algorithm to encrypt passwords in IBM OpenPages GRC Platform.

The Update Password Encryption Algorithm (UPEA) tool is used to modify the encryption algorithm and encryption key.

The UPEA tool can be used to:

- Change the AES encryption key - this is the default encryption algorithm.
- Change the encryption algorithm from 3DES to AES.

Modifying password encryption

To modify password encryption, you use the Update Password Encryption Algorithm (UPEA) tool.

Before you use the UPEA tool, ensure that you complete the following tasks:

- "Verifying the current encryption algorithm" on page 38
- "Verifying the environment" on page 38
- "Configuring the security provider in the java.security file" on page 39
- "Preparing passwords in the aurora.properties file and the op-backup-restore.env file for reencryption" on page 39
- "Updating the users table to change passwords" on page 40

You run the tool from the command line as follows:

OP_Home\bin\UpdatePasswordEncryptionAlgorithm.cmd (Windows)

OP_Home/bin/UpdatePasswordEncryptionAlgorithm.sh (UNIX)

Verifying the current encryption algorithm

If you have a legacy system, verify the name of the current encryption algorithm before you run the UPEA tool to change the algorithm to AES 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 you are finished, log out of SQL*Plus.

Results

If the SQL statement returns the name:

- 3DES, then run the UPEA tool to change the encryption algorithm to AES.
- AES, then you already have the AES encryption algorithm. If you want, you can use the UPEA tool to change the AES encryption key.

Verifying the environment

The following tasks must be completed before you run the UPEA tool.

- An IBM OpenPages GRC Platform system must be properly installed and functioning on the machine.
- A full backup of the OpenPages GRC Platform database must be completed. For more information, see Chapter 18, "Using IBM OpenPages GRC Platform utilities with Oracle databases," on page 419.
- Ensure that all OpenPages GRC Platform servers are started and that no users are logged on to the system during the password encryption update.

  Note: For details on starting and stopping servers for Windows, AIX and Linux environments, see "Starting application servers" on page 549.

Configuring the security provider in the java.security file

The security provider must be specified in the `java.security` file.

Procedure

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

a) Open a command or shell window on the application server.

b) Navigate to:

```
<Java_Home>|jre|lib|security
```

Where:

<Java_Home> is the installation location of the Java Runtime Environment.

- Windows: `C:\IBM\WebSphere\AppServer\java\jre\lib\security`
- Linux and AIX: `IBM/WebSphere/AppServer/java/jre/lib/security`

c) Make a backup copy of the `java.security` file before you modify it.

d) Open the `java.security` file in a text editor of your choice.

e) Locate the following property in the file:

```
security.provider.<#>=
```

Where: The number sign, *<#>* is one increment above the last number in the list (for example, 9).

f) If the `BouncyCastleProvider` security provider is not present, modify the value after the equal sign so it matches this:

```
security.provider.<#>=org.bouncycastle145.jce.provider.BouncyCastleProvider
```

g) When you are finished, save and close the file.

Preparing passwords in the `aurora.properties` file and the `op-backup-restore.env` file for reencryption

You can reencrypt the passwords that are in the `aurora.properies` and `op-backup-restore.env` files. By default, the files are in the *<OP_Home>* directory.

For Microsoft Windows operating systems, the default installation directory of OpenPages GRC Platform is `C:\OpenPages`.

For AIX and Linux operating systems, the default installation directory of OpenPages GRC Platform is `/opt/OpenPages`.

Procedure

1. Open a command or shell window on the application server.
2. Go to the *<OP_Home>* | `aurora` | `conf` directory.
3. Edit the `aurora.properties` file in the `conf` directory.
   a) Make a backup copy of the file.
   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 after the equal sign to plain text.
   e) Save and close the file.

   Note: The passwords are encrypted when you restart the servers.
4. Edit the `op-backup-restore.env` file in the *<OP_Home>* | `aurora` | `bin` directory.
   a) Make a backup copy of the file.

b) Open the file in a text editor of your choice.

c) Search the file for these two properties: DB_OP_PWD and DB_WF_PWD.

d) Change each password value after the equal sign to plain text.

e) Save and close the file.

Note: The passwords are encrypted when you restart the servers.

Updating the users table to change passwords

Updating user tables to change passwords with the UPEA tool applies only to upgraded databases.

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

The UPEA tool defines the parameters of the password encryption algorithm.

UPEA syntax

The syntax of the UPEA tool is detailed in the following section:

```
UpdatePasswordEncryptionAlgorithm
   -Mode [CA|CK]
   -AlgorithmName [AES]
   -Host <hostname>
   -ProviderName CAMCryptoBC
   -ProviderClass org.bouncycastle145.jce.provider.BouncyCastleProvider
   -Username <OpenPagesAdministrator>
   -Password <OpenPagesAdministrator password>
   [-Port <portnumber>]
   [-KeySize <128>]
   [-?]
```

The following table describes the UPEA parameters.

Table 16: 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 3DES to AES. • CK (for Change Key) — used to change the AES encryption key.
-AlgorithmName	Required. Use to specify the type of encryption algorithm to use. The only valid value is AES.

Table 16: UPEA parameters (continued)	
Parameter	**Description**
-Host	Required. Use to specify the host name of the application machine. Default value: `localhost`
-ProviderName	Required. Use when you change algorithms to the AES encryption algorithm only. Has only one valid value: `CAMCryptoBC`.
-ProviderClass	Required. Use only in conjugation with `-ProviderName` to specify the class for the new encryption algorithm. Has only one valid value: `org.bouncycastle145.jce.provider.BouncyCastleProvider`
-Username	Required. Use to specify the user name to use when you modify 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. Default value: `10101`
-KeySize	Optional. Use to specify the length of the AES encryption key. The only valid value is 128. If an invalid value is given, or no value is provided, the default value of 128 is used.
-?	Optional. Displays the on-screen help for the UPEA tool.

Changing the password encryption algorithm to AES

You can run the UPEA tool to change the password encryption algorithm from 3DES or OP-CUSTOM to AES, which is more secure.

Procedure

1. Edit the <OP_root>/OpenPages/aurora/conf/aurora.properties file and the <OP_root>/OpenPages/aurora/bin/op-backup-restore.env file and change any encrypted passwords to plain text.
   - If you are using 3DES, look for lines that contain {3DES}.

     For example, suppose the `aurora.properties` file contains the following line: `database.PASSWORD=`**`{3DES}`**`Rj+steg+3eU7kb80+\=\=`. The database password is encrypted with the 3DES algorithm. Replace the encrypted password with the password in plain text, for example, `database.PASSWORD=db_password`.
   - If you are using OP-CUSTOM, the lines do not have an algorithm indicator. Look for encrypted passwords and change each of them to the password in plain text.

   The passwords are encrypted with the AES algorithm when you restart the OpenPages GRC Platform services in step 3.
2. Open a command or shell window on the OpenPages GRC Platform server.

   Go to the *<OP_HOME>*`/bin` directory.
   - For Microsoft Windows operating systems, the default installation directory of OpenPages GRC Platform is `C:\OpenPages`.
   - For AIX and Linux operating systems, the default installation directory of OpenPages GRC Platform is `/opt/OpenPages`.

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

```
UpdatePasswordEncryptionAlgorithm.sh|.cmd -Mode CA -Host localhost
   -Port <port> -AlgorithmName AES -ProviderName CAMCryptoBC
   -ProviderClass org.bouncycastle145.jce.provider.BouncyCastleProvider
   -KeySize 128 -Username <OpenPagesAdministrator>
   -Password <OpenPagesAdministratorPassword>
```

- *<port>* is the bootstrap port number. If you do not specify a value, `10101` is used.
- *<host>* is the host name of the application server. If you do not specify a value, `localhost` is used.

3. Restart all OpenPages GRC Platform services.
4. If you are using OpenPages to authenticate users, 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.

   Note: If you are using Single Sign-On (SSO), LDAP, or another external system to authenticate users, passwords are not reset.

Changing the AES encryption key

At certain times, you might want to change the encryption key that is used by the AES encryption algorithm. You can change the encryption key by using the UPEA tool.

Procedure

1. Log on to the IBM OpenPages GRC Platform server as a user with administrative privileges.
2. Open a command or shell window and change directory to the *<OP_Home>*`/bin` directory.
   - For Microsoft Windows operating systems, the default installation directory of OpenPages GRC Platform is `C:\OpenPages`.
   - For AIX and Linux operating systems, the default installation directory of OpenPages GRC Platform is `/opt/OpenPages`.
3. From the command or shell window, run the following command on a single line:

   Windows

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

   AIX and Linux

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

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

   Note: If you changed the default port for OpenPages GRC Platform to a port other than 10108, add the `-Port` parameter to the end of the command with the new port number.
4. Restart OpenPages GRC Platform services for the changes to take effect.

Chapter 4. Security

Most of your security requirements can be handled in IBM OpenPages GRC Platform with folder-based security, either role-based security or custom security. If you need to refine folder-based security, use security rules.

Role-based security
Use role-based security to define application permissions for each role and to set access control (Read, Write, Delete, Associate) for each object that is included in that role. All users in each role inherit the same security access controls.

Custom security
Use custom security to set access control (Read, Write, Delete, Associate) on folders for Project Milestones and Project Action Items. All objects in the folder inherit the same security access controls.

Security rules
You can define two types of security rule:

- Record level security rules

  Use record level security rules to control access to individual objects in a folder. For example, two GRC domains share a common organizational hierarchy. They share some common object instances, such as processes, but they do not want to share other object instances, such as risks and controls. If you do not create security rules on objects, folder-based security applies.

  Record level security rules have the following access controls: Create, Read, Update, Delete, and Associate. The Write access control in folder-based security is split into Create and Update for security rules, which gives you more control over what users can and cannot do.

- Field level security rules

  Use field level security rules to control access to individual fields within an object.

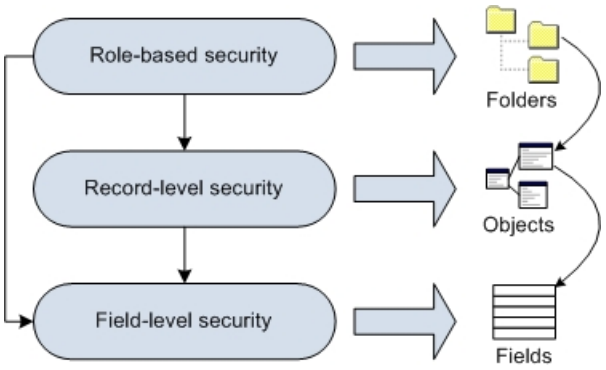


Figure 2: Levels of security

Role-based security and security rules differ from profiles and field dependencies because security is applied everywhere rather than in the OpenPages GRC Platform application only.

Role-based security model

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 3 on page 44 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.

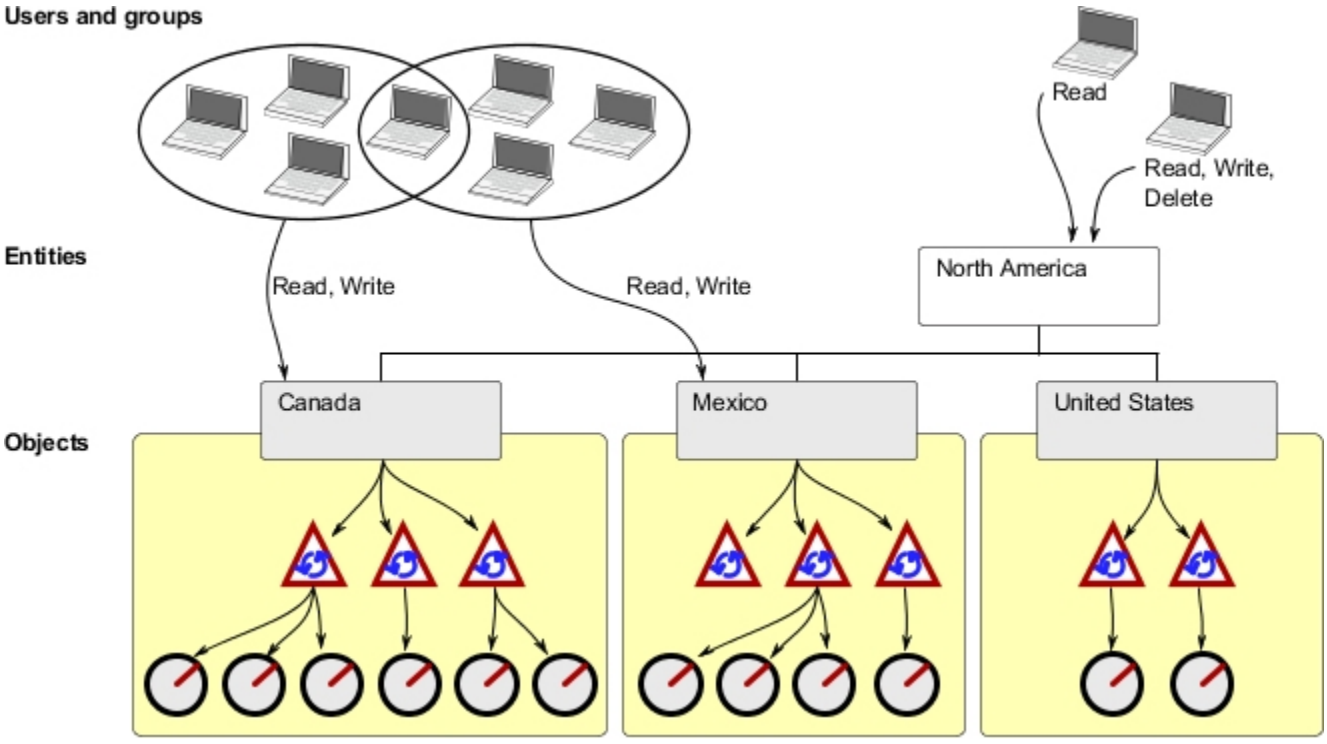


Figure 3: Security concepts in a hierarchy

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 "Role-based access control permissions" on page 49.
- Application permissions for the role. For information about the various application permissions, see "Defining application permissions" on page 31.

  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 "Delegate administrator permissions" on page 21.

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. *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 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 110.

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

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.

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 4 on page 46 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.

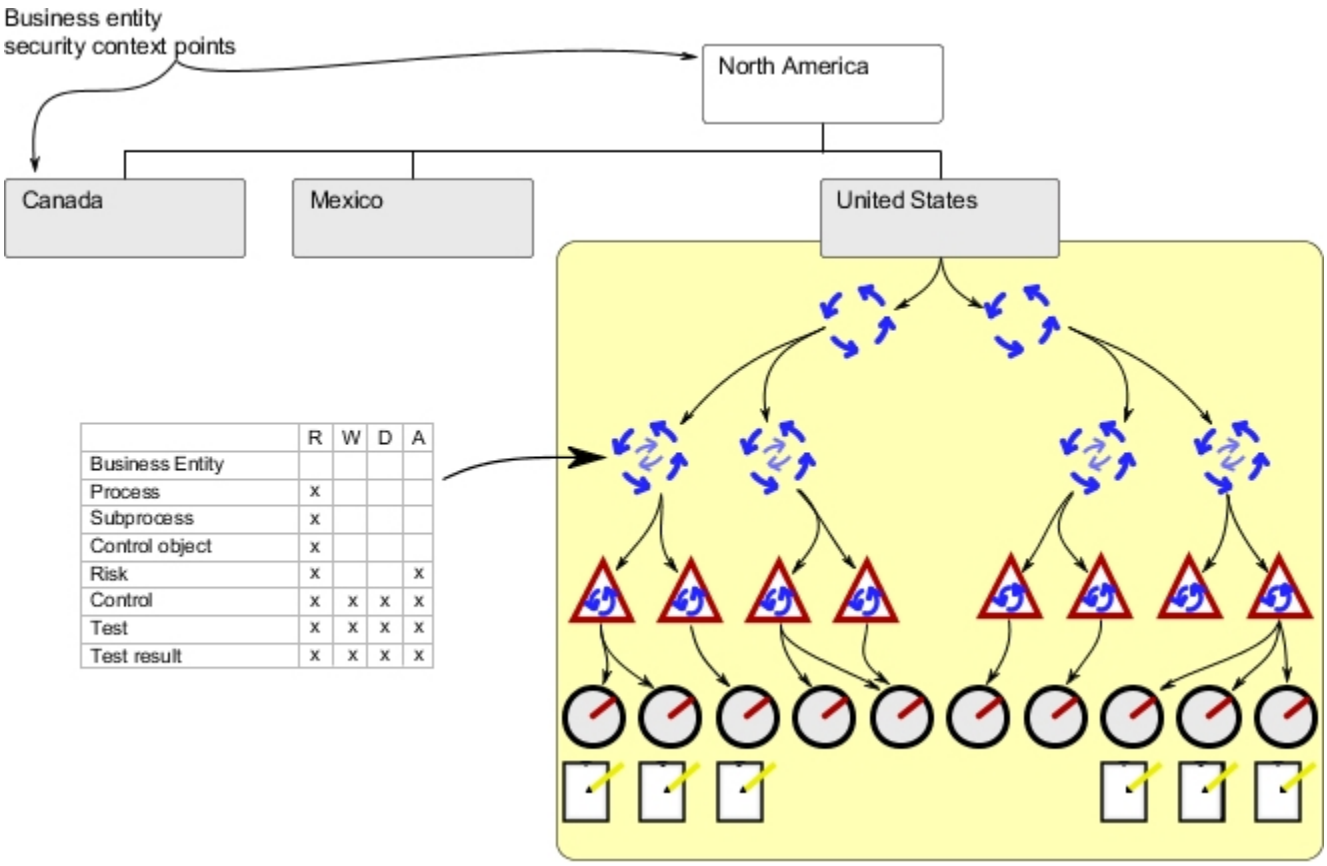


Figure 4: Business entity security context points

For details on assigning security management permissions to security domain group administrators, see “Delegate administrator permissions” on page 21.

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).

To achieve more control, change the Model setting. For more information, see “Set the system security model” on page 342).

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 IBM OpenPages GRC Platform 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

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 within 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 user interface in OpenPages GRC Platform 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 5 on page 47 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.

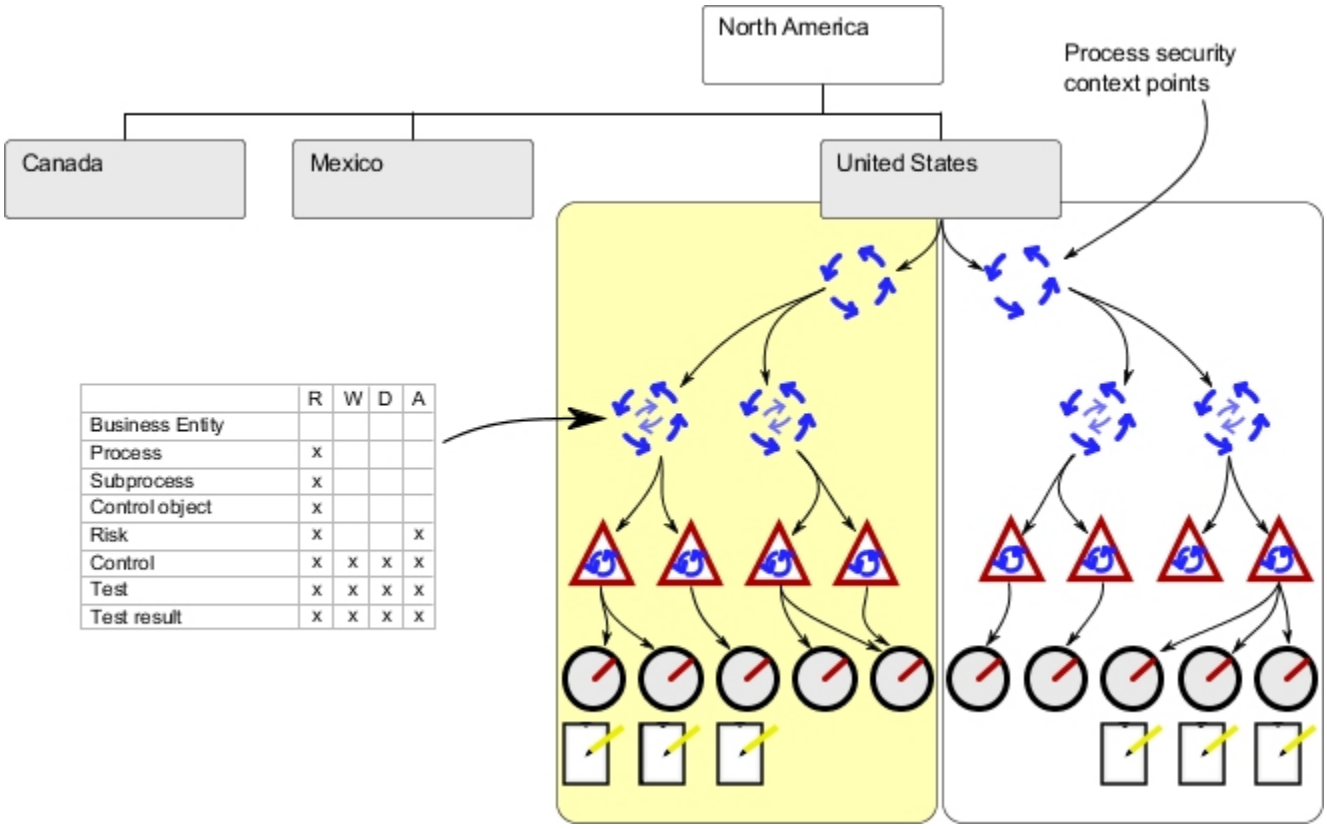


Figure 5: Business entity and process extended context points

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 6 on page 48 shows an example of a triangle relationship between a child Risk and parent Process and Sub-Process object types.

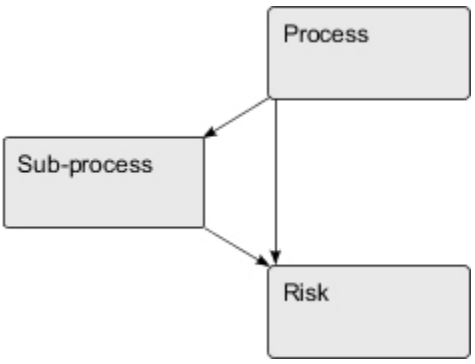


Figure 6: Triangle relationship between different object types

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, 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 "Triangle object relationships" on page 663.

Sample scenario

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 SUBPR0CESSES and PR0CESSES reside in the same Query Subject).

Security domains

In IBM OpenPages GRC Platform, 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

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.

Moving business entities

On occasion, you may need to reorganize 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.

Note: If you are planning on moving a large object hierarchy, consider using the Entity Move/Rename utility that is included with IBM OpenPages GRC Platform. This utility allows batch processing of multiple Business Entities for overnight or weekend execution without running the risk of operations timing out. You can run the utility interactively or as a scheduled job. See the *Entity Move/Rename Utility ReadMe* for details.

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 “Delegate administrator permissions” on page 21.

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 “Role templates” on page 51.

Role-based access control permissions

When you create a Role Template, you can specify the type of security access control that 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 “Custom security for projects” on page 79.
- Any new object types that are added to the system are excluded from all existing Role Templates.

Access control permissions for role-based security
For each object type that you want to include in a Role Template, you can set 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 read and 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 read, modify, and 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 “Scenarios: Using access control settings” on page 50.

- **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.

Scenarios: Using access control settings
The following 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.

For example, 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.

For example, 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.

For example, 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.

Role templates

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.

Because the **Assign Roles** permission is a global permission, it is not constrained by the hierarchy of the role. Users who are granted this permission can manage any role in the system.

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. After you save your changes (or cancel the operation), the Role Template is 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.

Accessing the role templates page

You can define application permissions by using role templates.

Only a Super Administrator or a delegated administrator with the **Role Templates** permission can access the **Role Templates** menu item.

Procedure

1. Log on to the IBM OpenPages GRC Platform application user interface as a user with the **Role Templates** application permission set.
2. Click **Administration** > **Role Templates**. From the **Role Templates** page, you can add, view, and modify role templates.

Adding a role template

You can add a role template to define application permissions.

The Role Template wizard guides you through 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 within 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.
2. Click **Administration** > **Role Templates**.
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 is 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 “Role-based access control permissions” on page 49.
   c) Click **Next**.
6. On the **Specify Permissions** page:
   a) Select the application permissions that you want to assign to this Role Template. For a description of the various application permissions, see “Types of application permissions” on page 32.
   b) 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 54.

Modifying a role template

When you modify a Role Template after you assign 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, does not have **Assign Roles** administration permission on higher-level entities and hence is not able to successfully edit, disable, or delete a template.

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

Procedure

1. Click **Administration** > **Role Templates**.
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. Click **Save**.

Enabling and disabling a role template

You can make a role inactive and keep it for future use by disabling the role. You can also enable a role that was previously disabled.

Procedure

1. Click **Administration** > **Role Templates**.
2. From the list on the **Role Templates** tab, click the name of the role you want to enable or disable. The detail page of the selected role is displayed.
3. On the **Role Information** tab, click **Disable** or **Enable**.

Results

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, 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.
- 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.

When you enable a role, the following occurs:

- Any users or groups who are assigned that role are able to perform activities on objects that are 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.

Deleting a role template

To automatically revoke all role assignments, you can delete a role template.

An administrator (or Super Administrator) with **Role Templates** application permission and the **Assign Roles** administrator permission can assign and/or revoke roles on any entity in the system. Only a Super Administrator or a top-level entity administrator is able to delete role templates, since this action automatically revokes all role assignments that were 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 are no longer able to perform the activities on objects that are 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 by revoking the role from the user or group.

Procedure

1. Click **Administration** > **Role Templates**.
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**.

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

You have a business entity with the following hierarchical structure:

Company ABC > North America > Boston

The business entity has the following 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
After Role Templates are created, 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.

About this task

You can assign a role to a user or group with the **Assign Roles** wizard. Alternatively for users, you can assign roles from the **View, Edit, or Disable User** page. For more information, see "Modifying user accounts" on page 28.

Procedure

1. Click **Administration** > **Users, Groups and Domains**.
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) Go to the **Role Assignments** tab.
   b) Click **Assign** to display the **Assign Roles** wizard.
4. On the **Select User(s)/Group(s)** page:
   a) Click **Add**.
   b) In the selection box, select the check box next to each group or user you want.

      Tip: To expand the group/user hierarchy, click the plus (+) sign.
   c) Click **Next**.
5. On the **Select Role Type and Role(s)** 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 is 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 Security Domain(s)** page:
   a) Optionally, in the **Name** box, 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 reduces the scope of the list by returning only those items that match the text you typed.
   b) In the **Security Domains** box, select one or more security context points from the list.
   c) Click **Finish**.

Revoking a role from a user or group

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.

Disassociating users from a security domain group does not result in removal of their role assignments on that entity.

About this task

You can revoke a role assignment from a user or group from the **Role Assignments** tab of the business entity security domain group. page. Alternatively for a user, you can remove roles from the **View, Edit, or Disable User** page. For more information, see "Modifying user accounts" on page 28.

Procedure

1. Click **Administration** > **Users, Groups and Domains**.
2. Under the **Security Domains** 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) Go to the **Role Assignments** tab.
   b) Select the check box next to the name of each group or user you want to revoke.
   c) Click **Revoke**. The name of the selected group or user is removed from the list.

Viewing roles assigned to users or groups

You can use several methods to view which roles are assigned to users and groups.

- Running reports
- Navigating to a user or group detail page and see the list of all roles that are 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 be only viewed from the detail page of that parent or child. Role assignments that are 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 subprocesses that are associated with the current security domain are also displayed.
- Selecting **Users** from the Administration menu and searching for a user in the **View, Edit, or Disable User** field. On the **View, Edit, or Disable User** page, click **Role Assignments** from the left panel. For more information, see "Modifying user accounts" on page 28.

Procedure

1. Click **Administration** > **Users, Groups and Domains**.
2. Under the **Security Domains** 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, go to the **Role Assignments** tab.
4. To view role assignments that are made directly to another business entity security domain group, repeat Steps 2 and 3.

Security rules

You can create two levels of security by using security rules:

- "Record level security" on page 57 allows administrators to control access to individual objects in a folder.
- "Field level security" on page 69 allows administrators to control access to individual fields within an object.

Security rules do not replace role-based security. Instead, they provide an extra level of security that can work with role-based security.

Consider this example of record level security. A folder contains 10 tasks. The role-based security grants the Read and Write access controls to all users in a certain role. You define a record level security rule to limit the access for one user who is in that role so that this one user has Read access for Task 1 and Task 8 only.

You can extend the example to field level security. Task 1 contains 10 fields. You can define a field level security rule to limit the access for one user in a certain role. This user has Read access for Field 3 and Field 7 only.

You define security rules for individual object types. After you have defined them, they are applied to all system components, including Reporting, FastMap, Triggers, Reporting Periods, and all available views.

A security rule comprises two parts:

- A formula that determines the conditions for granting the access controls.
  - The formula can be based on these field values: Actor fields, Enumerated fields, Text fields, Date fields, Numeric fields, and Currency fields.
  - The formula can be based on a user who is a member of particular user group or profile.

  - Complex formulae can be based on associations between objects.

    For example, a loss event is owned by the business unit where it occurred and is also shared with other business units that are impacted by the loss event. Selected users of the other business units should see its details.
  - The formula can support complex expressions that use terms such as AND, OR, NOT, and nested parentheses.
- The access controls that specify the object access permissions or field access permissions.
  - A record level security rule can specify Create, Read, Update, Associate, and Delete access to object instances.
  - A field level security rule can specify Read only, and Read and Update access to non-system fields within an object.

A security rule formula has the following restrictions:

- They do not support computed text fields or large text fields.
- They do not support NULL values.

  The NOT operator does not return objects that have an empty, blank, or null value in the selected field criteria.
- They do not support encrypted simple string or long string data type fields.

Note: Security rules are not applied to administrators. They have full permissions for all objects and fields.

Record level security

You can use record level security to control access to individual objects in a folder.

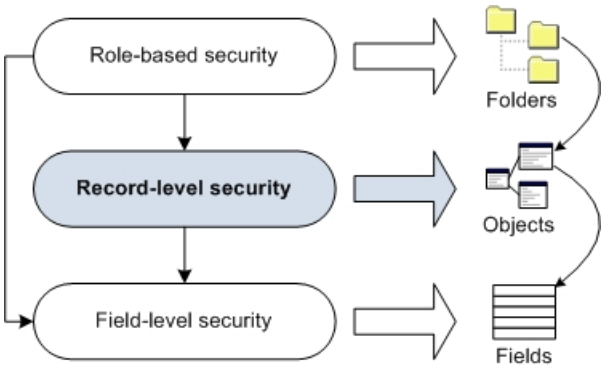


Figure 7: Record level security applies to objects

If no record level security is defined for an object, only role-based security is applied to the object.

When you define a record level security rule, the way that access is restricted depends upon whether the outcome of the formula is true or false when it is applied to an object:

- True: Access to the object is granted, and you can restrict or extend the existing role-based security for that object.
- False: Access to the object is not granted, and role-based security is applied.

When users open the Detail View for an object, they can see associated child objects only under the following circumstances:

- The associated child objects are included in a role template.
- The associated child objects are not included in a role template, but a record level security rule that extends role-based security is applied to the parent object.

RESTRICT and EXTEND rules

When you define a record level security formula, you define RESTRICT rules and EXTEND rules.

A RESTRICT rule is applied after role-based security (RBS). A RESTRICT rule further restricts access to an object. The following formula illustrates how a RESTRICT rule is evaluated:

```
If (RBS=True AND RESTRICT_RULE_RESULT=True), then grant access
```

Notice the AND operator. Role-based security must grant access, and the result of the RESTRICT rule must be true. The result is that users get access to the object if role-based security grants them access and the RESTRICT rule result is also true.

For example, suppose role-based security grants all users in the Finance group READ and UPDATE access on Control objects. But, you want users to be able to do an UPDATE only if they are also the owner of the control object. In this case, you can add a RESTRICT rule on UPDATE that checks the END_USER against the owner field of the object.

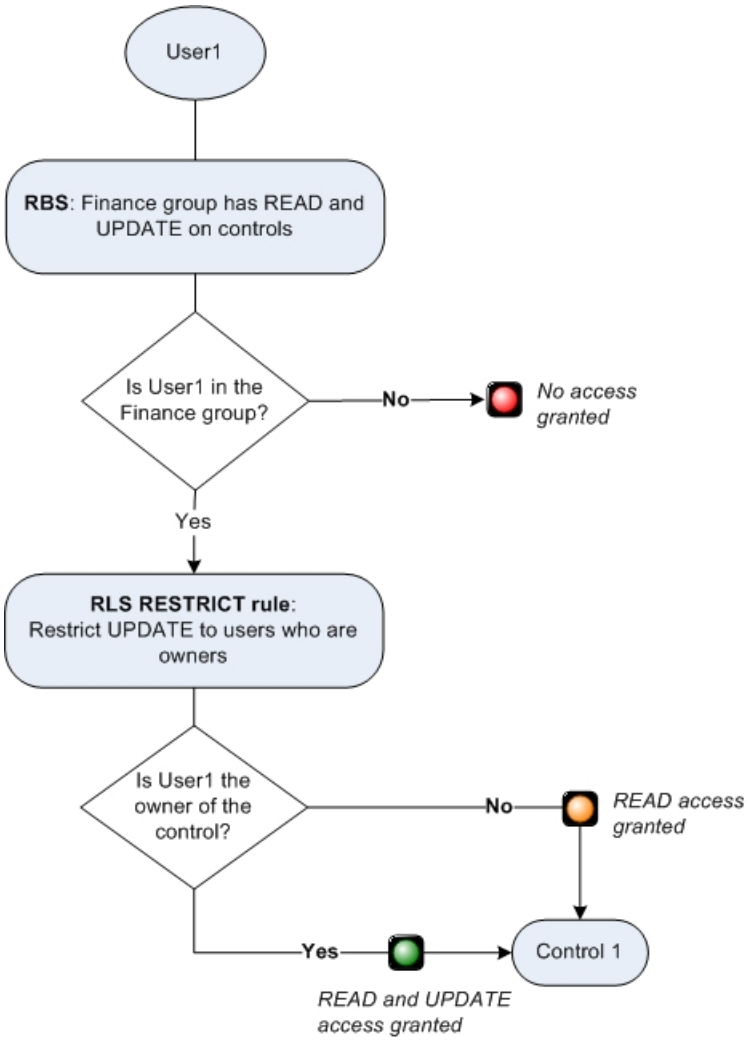


Figure 8: A RESTRICT rule grants UPDATE access if users are in the Finance group and are owners of the control

For a more detailed example, see the record level security scenarios, such as “Scenario: Objects that are shared across GRC domains” on page 64.

An EXTEND rule is applied in addition to role-based security. An EXTEND rule grants access to an object for which role-based security does not grant access. The following formula illustrates how an EXTEND rule is evaluated:

```
If (RBS=True OR EXTEND_RULE_RESULT=True), then grant access
```

Notice the OR operator. Either role-based security must give access or the EXTEND rule result must be true. The result is that users get access to the object if role-based security gives them access or if the EXTEND rule result is true. Which means users gain access to the object in all of the following scenarios:

- Role-based security is granted and the EXTEND rule result is true, OR
- Role-based security is granted and the EXTEND rule result is false, OR
- Role-based security is not granted and the EXTEND rule result is true.

For example, suppose role-based security grants all users in the Finance group READ and UPDATE access on Control objects. However, you also want users to be able to READ and UPDATE if they are the owner of the control object, regardless of whether they belong to the Finance group. In this case, you can add an EXTEND rule on READ and UPDATE that checks the END_USER against the owner field of the object.

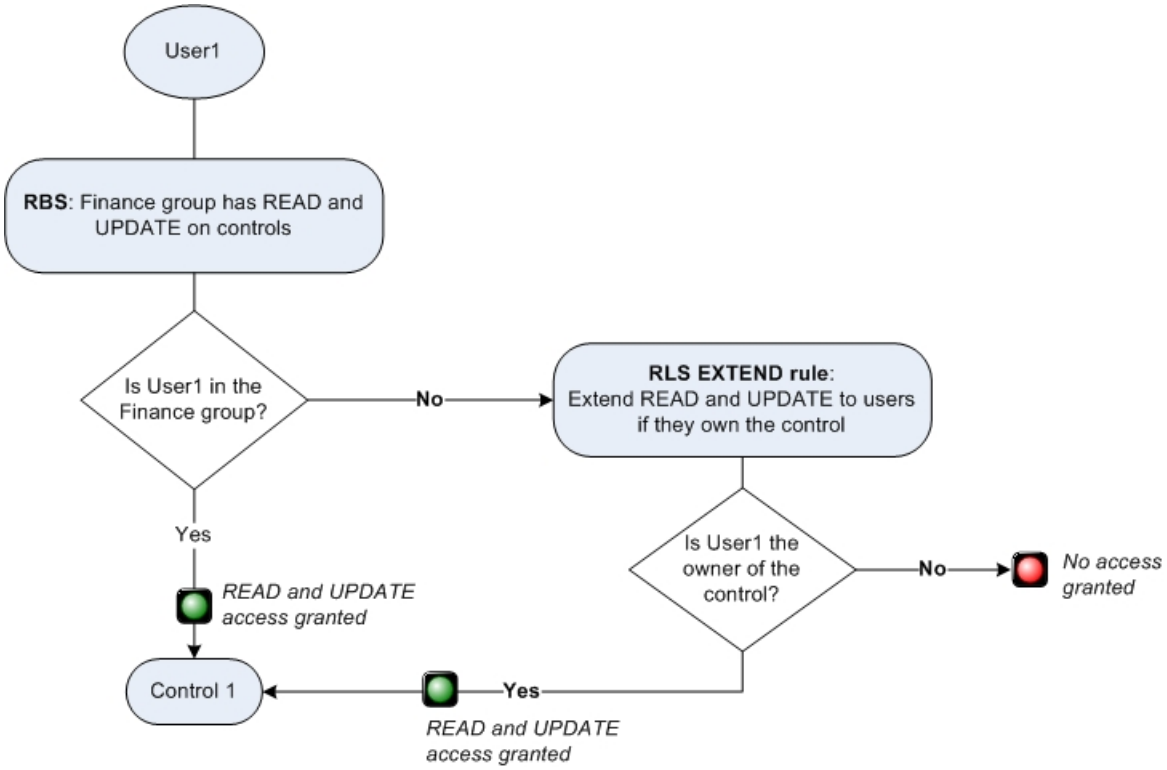


Figure 9: An EXTEND rule grants access to users who are owners of a control, regardless of their group membership

For a more detailed example, see the record level security scenarios, such as “Scenario: Access for business administrators” on page 69.

Whether you are using a RESTRICT rule or an EXTEND rule, the rule is evaluated within the context of role-based security.

Multiple security rules
You can use multiple RESTRICT and EXTEND rules. Before you combine rules, ensure that you understand how security rules work in combination with each other. Incorrect assumptions about the behavior of security rules can lead to insecure models.

Combining RESTRICT rules
When you have multiple rules on the same object type with the same access, the rules are combined by using an OR expression.

Here is an example of two RESTRICT rules combined:

```
Restrict Rule 1 - Grants READ
Restrict Rule 2 - Grants READ and UPDATE
```

Since each rule grants READ access, the two rules are combined whenever the READ access for a user needs to be determined. Each rule is evaluated on its own within the context of role-based security and access is granted if either of the rules evaluates to true. The means that the formula for this example is evaluated in the following manner:

```
If ((RBS=True AND RESTRICT_RULE_1_RESULT=True) OR
(RBS=True AND RESTRICT_RULE_2_RESULT=True)), then grant access
```

The result is that a user gets READ access in the following scenarios:

- Role-based security is granted and the RESTRICT rule 1 result is true, OR
- Role-based security is granted and the RESTRICT rule 2 result is true.

Combining RESTRICT and EXTEND rules
You can combine RESTRICT rules with EXTEND rules. Each rule is evaluated within the context of role-based security, and then an OR condition is applied. However, do not combine RESTRICT and EXTEND rules on the same object for the same privilege.

For example, you can combine a RESTRICT rule for READ and UPDATE with an EXTEND rule for DELETE:

```
Restrict Rule on READ, UPDATE
Extend Rule on DELETE
```

The rules are evaluated in the following manner:

If evaluating READ access:

```
If ((RBS=True AND RESTRICT_RULE_RESULT=True), then grant access
```

If evaluating UPDATE access:

```
If ((RBS=True AND RESTRICT_RULE_RESULT=True), then grant access
```

If evaluating DELETE access:

```
If (RBS=True OR EXTEND_RULE_RESULT=True)), then grant access
```

Attention: Do not use the same access privilege in both rules. This can lead to results that might not be-in-line with the behavior that you expect.

Here is an example of combined RESTRICT and EXTEND rules to help illustrate the point:

```
Restrict Rule on READ
Extend Rule on READ
```

The formula is evaluated in the following manner:

```
If ((RBS=True AND RESTRICT_RULE_RESULT=True) OR
(RBS=True OR EXTEND_RULE_RESULT=True)), then grant access
```

The result is that a user gets READ access in all of the following scenarios:

- Role-based security is granted and the RESTRICT rule result is true, OR
- Role-based security is granted and the EXTEND rule result is true, OR
- Role-based security is granted and the EXTEND rule result is false, OR
- Role-based security is not granted and the EXTEND rule result is true.

In other words, the user will have READ access with role-based security.

How combined security rules are evaluated
It is important to understand how RESTRICT rules and EXTEND rules are combined.

Many administrators assume that the EXTEND rule is evaluated after the RESTRICT rule, like this:

```
If ((RBS=True AND RESTRICT_RULE_RESULT=True) OR
EXTEND_RULE_RESULT=True), then grant access
```

The result would be that a user gets access in the following scenarios:

- Role-based security is granted and the RESTRICT rule result is true, OR
- The EXTEND rule result is true.

But this is not the case. Each rule is evaluated within the context of role-based security, and then an OR condition is applied:

Let's expand on this example to more clearly see the potential misunderstanding. Suppose that you have a user with the following set of circumstances:

- Role-based security access is granted to the user
- The RESTRICT rule for this user evaluates to FALSE
- The EXTEND rule for this user evaluates to FALSE

Using the formula from the assumed behavior the result of this scenario would be False:

```
((RBS=True AND RESTRICT_RULE_RESULT=True) OR EXTEND_RULE_RESULT=True) =
((True=True AND False=True) OR False=True) =
((True AND False) OR False) =
(False OR False) =
(False)
```

However, the formula that is actually being used is:

```
(RBS=True AND RESTRICT_RULE_RESULT=True) OR (RBS=True OR EXTEND_RULE_RESULT=True) =
(True=True AND False=True) OR (True=True OR False=True) =
(True AND False) OR (True OR False) =
(False OR True) =
(True)
```

Therefore, access would be granted for this user.

It is critical to understand how security rules work in combination with each other before you design your security framework. Incorrect assumptions on behavior can lead to insecure models.

Defining record level security rules
Use record level security rules to control access to individual objects in a folder.

Before you begin
You must enable System Administration Mode before you can define record level security.

Procedure

1. Click **Administration** > **Security Rules**.
2. Click the name of the object type for which you want to define a security rule.
3. Click **Add** next to **Record Level Security Rules**.
4. Add a name and description for the security rule.

5. Add the formula for the security rule.

   You can type the formula or use the **Path**, **Field**, and **Terms** to define parts of the formula. You can also use a combination of both. For more information, see "Grammar for security rules" on page 74.

   a) To reference another object, either a parent or child, complete the following actions.

      For more information, see "Paths for parent and child objects" on page 71.

      1) Click **Path**.
      2) In the **Parent or Child** field, specify whether the path follows parent objects or child objects.
      3) Select the object type that is the starting point for the path.
      4) Select the object type that is the ending point for the path.
      5) Click **Search** to view the possible paths.
      6) Select one or more paths. If you select more than one path, use the **Combine Paths** field to specify how to use the multiple paths. Select **Any Path** if you want to use any of the paths or select **All Paths** if you want all paths to be used for the rule to be applied.
      7) Click **Insert**.

   b) To define a field condition, complete the following actions.

      For more information, see "Terms for data types" on page 72.

      1) Click **Field**.
      2) Select an object type.
      3) Select the field that you want to use.
      4) Select an operator. The list of operators changes depending on the field data type.
      5) Enter the value of the field condition.
      6) Click **Insert** to add the field condition into the rule formula.

      If you type the field condition, ensure that you use system names. If you do not specify an object type, the rule uses the object type for the object to which the rule applies. If you specify an object type, the object type must be either the subject of the rule or be specified in a path expression that contains the field reference.

      Optionally, you can use square brackets to ensure that when elements of field references contain spaces or other special characters, these field references are parsed.

   c) To add operators or keywords, use the **Terms** menu.

6. In the **Security** property, specify how the security rule is combined with role-based security.

   - Select **Restrict** to apply both the role-based security and the security rule.

     This option configures more restricted security. For example, if role-based security is set to **Read** and the security rule is set to **Update**, the **Restrict** setting provides read only access.

   - Select **Extend** to bypass role-based security when the outcome of the formula is true.

     For example, if the role-based security is set to **Read** and the security rule is set to **Update**, the **Extend** setting allows a user to update information.

7. Specify the access controls.

   For more information, see "Minimum access controls for object operations" on page 63.

   Note: Security rules for **Create** access are defined separately from rules for **Read**, **Update**, **Delete**, and **Associate** access.

   Create
   Users can create objects.

   When a rule allows users to create objects, the formula cannot include fields within the object. It can include fields from the parent hierarchy, and other conditions that do not include fields. If you select **Create**, you cannot select any other access control for the rule.

Note: When you define record level security rules for the Create access control, use them only to further restrict role-based security.

You must use **Intended Parent** in the **Terms** field when you use **Create**.

Read
Users can view the object.

Update
Users can modify the object.

Delete
Users can delete the object.

Associate
Users can define associations or disassociations between objects.

When a rule allows users to associate objects, the formula cannot include fields within the target of the association. It can include fields from the child hierarchy, and other conditions that do not include fields.

8. Click **Save**.

Minimum access controls for object operations
Users can perform the following operations on objects: Create, Read, Update, Associate and Delete. Each of these operations requires certain minimum access controls.

Create operation

The following table shows the minimum access controls that a user requires to create an object. Access controls are required for both the parent object and the child object.

Some access controls must defined using role-based security rather than record level security (as indicated in the table). In these instances, the access control for the parent object can be defined using either type of security, but for the child object, it must be defined using role-based security.

Table 17: Access controls required to create an object

	Read	Write	Delete	Associate
Parent	Yes			Yes
Child	Yes (from role-based security)	Yes (from role-based security)		Yes (from role-based security)

Read operation

The following table shows the minimum access controls that a user requires to read an object.

These access controls can be defined in the role-based security or the record level security.

Table 18: Access controls required to read an object

	Read	Write	Delete	Associate
Object	Yes			

Update operation

The following table shows the minimum access controls that a user requires to update an object.

These access controls can be defined in the role-based security or the record level security.

Table 19: Access controls required to update an object				
	Read	**Write**	**Delete**	**Associate**
Object	Yes	Yes		

Associate operation

The following table shows the minimum access controls that a user requires to associate an object. Access controls are required for both the parent object and the child object.

Some access controls must defined using role-based security rather than record level security (as indicated in the table). In these instances, the access control for the parent object can be defined using either type of security, but for the child object, it must be defined using role-based security.

Table 20: Access controls required to associate an object				
	Read	**Write**	**Delete**	**Associate**
Parent	Yes			Yes
Child	Yes (from role-based security)			Yes (from role-based security)

Delete operation

The following table shows the minimum access controls that a user requires to delete an object. Access controls are required for both the parent object and the child object.

These access controls can be defined in the role-based security or the record level security.

Table 21: Access controls required to delete an object				
	Read	**Write**	**Delete**	**Associate**
Parent	Yes			Yes
Child	Yes		Yes	Yes

The following table shows the minimum access controls that a user requires to delete an object type that is self-contained or recursive, such as a Business Entity or Sub-Process. Access controls are required for both the parent object and the child object.

Some access controls must defined using role-based security rather than record level security (as indicated in the table). In these instances, the access control for the parent object can be defined using either type of security, but for the child object, it must be defined using role-based security.

Table 22: Access controls to delete a self-contained object				
	Read	**Write**	**Delete**	**Associate**
Parent	Yes			Yes
Child	Yes (from role-based security)		Yes (from role-based security)	Yes (from role-based security)

Scenario: Objects that are shared across GRC domains

Your company implemented the financial management and operational risk solutions. Because the teams that use these solutions share a common organizational hierarchy, they share some common object

instances, such as processes. But they do not want to share other object instances, such as risks and controls.

Role-based security means that all users in the financial management and operational risk teams have access to all objects and object instances in the folder. Access controls need to be set for each domain so that users work with only the objects that they are responsible for. As well securing objects, you are improving usability for your users.

For example, both of the financial management and operational risk teams use the Control object type but they use different instances of the Control object type. You want to enable users in the operational risk team to be able to update their instances of the Control object type. You also want to prevent users in the financial management team from viewing the instances that belong to the operational risk team.

You have two user groups for financial management and operational risk. Role-based security is already defined to grant **Read** and **Write** access controls to all users in the two teams. For example, a user in the SOXUsers group can update the controls that belong to the operational risk team.

Table 23: Permissions for each user group in the scenario

Domain	User Group	Permitted to work with	Not allowed to work with
Financial Management	SOXUsers	Compliance Controls	Operational Controls
Operational Risk	ORMUsers	Operational Controls	Compliance Controls

To satisfy the security requirements for these two user groups, role-based security is not changed. You add a security rule that further restricts the security that you already defined for the folder.

You define a security rule on the Control object type with the following information:

The formula is:

```
[SOXControl].[OPSS-Ctl].[Domain] IN ('Financial Management') AND END_USER IN
GROUP('SOXUsers'))
OR
[SOXControl].[OPSS-Ctl].[Domain] IN ('Operational Risk') AND END_USER IN
GROUP('ORMUsers'))
```

When the Security property is set to **Restrict**, both role-based security and the security rule are applied, and the Access controls are set to **Read** and **Update**.

Procedure

1. Click **Administration** > **Security Rules**.
2. Click the name of the Control object type.
3. Click **Add** adjacent to **Record Level Security Rules**.
4. Add a name and description for the security rule.
5. Add the formula:
   - Click **Field** and select the SOXControl object in the **Object Type** field.
   - In the **Field** box, select **Domain** and select the Financial Management domain for the compliance team.
   - Click **Insert**.
   - Click **Field** and select `AND`, then `END_USER`, and `IN GROUP` from the **Terms**.
   - Type `('SOXUsers')`.
   - Repeat for the Operational Risk domain.
6. In the **Security** property, select **Restrict** to have role-based security and the security rule both apply. **Restrict** prevents Compliance users from being able to view or work with the Operational Control.

7. Select the **Read** and **Update** access control check boxes.
8. Click **Save**.

Scenario: Lifecycle security

Security on an object can change during the lifecycle of that object. As an object moves through the lifecycle, its status changes and different users are allowed to change it. For example, users in different job functions, such as reviewers and approvers, work with the object at different times in the lifecycle. The same user can be an owner of one object and a reviewer of another object.

Security rules are evaluated before lifecycle triggers and actions modify an object. If an object's state before the lifecycle trigger meets the record level security criteria, you can update the object. The lifecycle trigger might modify fields so that the object state no longer meets the record level security rules.

In this scenario, the Process object is the primary parent. The Risk object is a child of the Process object because part of the process is to assess risk. As the Process object moves through the lifecycle, the status of the Process object affects the Risk object.

The following table shows who can update the object when the status changes for the object instance and its descendants.

Table 24: Lifecycle security based on the status of an object

Status of the object	**The role of the user who can update the object**
New	Only a level of administrative user, such as a business administrator, can change the object. The administrator assigns the object to an owner.
Under Development	Owner
Ready for Review	Reviewer
Ready for Approval	Approver

Role-based security is already defined to grant **Read** and **Write** access controls to all users in these roles. All users in these profiles have access to all objects in the folder. Access controls must be set on the status of the Process object so that users work with only the object when they are responsible for it.

You define the following security rule for the Process object type that restricts when users can update the Process object. When users who belong to a role login, they can update the Process object at the correct point in the lifecycle of the Process object.

The formula is:

```
[SOXProcess].[OPSS-Process].[Status] IN ('Under Development') AND END_USER
IN([SOXProcess].[OPSS-Process].[Owner])
OR
[SOXProcess].[OPSS-Process].[Status] IN ('Ready for Review') AND END_USER
IN([SOXProcess].[OPSS-Process].[Reviewer])
OR
[SOXProcess].[OPSS-Process].[Status] IN ('Ready for Approval') AND END_USER
IN([SOXProcess].[OPSS-Process].[Approver])
```

The Security property is set to:

Restrict

Both role-based security and the security rule are applied. For example, when the status of the object is set to New, only a user in the Administrator profile can work with the object.

The Access control is set to:

Update

Role-based security grants the Read access control.

Procedure

1. Click **Administration** > **Security Rules**.
2. Click the Process object type.
3. Complete the following actions to define the security rule that grants the **Update** access control:
   - Click **Add** adjacent to **Record Level Security Rules**.
   - Add a name and description for the security rule.
   - Use **Path**, **Field**, and **Terms** to define the formula.
   - Select the **Update** check box.
   - In the **Security** property, select **Restrict** to have role-based security and the security rule both apply.
4. Click **Save**.

Scenario: Access to Issue Action Items
Issues that are created under one business unit can cause action items to be assigned to other lines of business. You need to ensure that all action item owners, regardless of business unit, can view the related issue.

An issue can have multiple action items that resolve the issue. The action items can be assigned to different business units and each business unit needs access to the issue object.

In this example, the compliance team has an Issue object that has two action items. One action item is for the compliance team. The other action item is for another business unit to complete some systems work.

Role-based security is set for the compliance team. They have access to all the objects in the folder, including the Issue object. A security rule is not required for the compliance team.

The other business unit needs access to the Issue object that is associated to the action item that they are responsible for. If you add the other business unit to role-based security, the other business unit has access to all objects in the folder. A security rule extends access to the other business unit for their action item and prevents them from working with other objects in the folder.

You define a security rule for the Issue object type with the following information:

The formula is:

```
FOR (Any Child [SOXIssue]/[SOXTask] : [SOXTask].[OPSS-AI].[Assignee] =
END_USER)
```

When the Security property is set to **Extend**, security is extended beyond role-based security. Users in the other business unit who are the owner of an action item that is associated to this issue can view the issue; however, they cannot view other issues that do not meet the criteria in the formula. The Access controls are set to **Read**.

Procedure

1. Click **Administration** > **Security Rules**.
2. Click the name of the SOX Issue object type.
3. Click **Add** adjacent to **Record Level Security Rules**.
4. Add a name and description for the security rule.
5. Use **Path**, **Field**, and **Terms** to define the formula.
6. Select the **Read** check box.
7. In the **Security** property, select **Extend** to have the security rule extend the security that is set on the folder.
8. Click **Save**.
9. Click the name of the SOXTask object type.

10. Click **Add**.
11. Add a name and description for the security rule.
12. Use **Path**, **Field**, and **Terms** to define the formula.
13. Select the **Read** and **Update** check boxes.
14. In the **Security** property, select **Extend** to have the security rule extend the security that is set on the folder.
15. Click **Save**.

Scenario: Security by job function
All auditors on the same team have the same profile, role template, and security context points. However, each auditor can have a different function for each audit. As an administrator, you want more flexibility in the way you apply security at the field level for each auditor.

This scenario is a variant of the scenario called *Lifecycle security*.

An auditor can have a different job function on different audits. For example, in Audit A, Jim is the lead auditor and can edit more fields than the other auditors.

Table 25: Audit A scenario

Auditors	Job function	Permissions
Jim	Lead (In-charge)	Jim can edit the Audit A instance of the Audit object and its descendants, Audit Sections, and Audit Workpapers. Jim's access controls are Create, Read, Update, and Associate.
Susan	Field	Susan can read and update specific areas of the Audit Sections and Audit Workpapers in the Audit A instance. Susan's access controls are Read and Update for these areas.
Ellen	Field	Ellen can read and update specific areas of the Audit Sections and Audit Workpapers in the Audit A instance. Ellen's access controls are Read and Update for these areas.

However, in Audit B, Susan is the lead auditor while Jim is a field auditor.

Table 26: Audit B scenario

Auditors	Job function	Permissions
Susan	Lead (In-charge)	Susan can edit the Audit B instance of the Audit object and its descendants, Audit Sections, and Audit Workpapers. Jim's access controls are Create, Read, Update, and Associate.

Table 26: Audit B scenario (continued)		
Auditors	**Job function**	**Permissions**
Jim	Field	Jim can read and update specific areas of the Audit Sections and Audit Workpapers in the Audit B instance. Jim's access controls are Read and Update for these areas.
Ellen	Not involved in this audit	Ellen has no access controls set for her.

Scenario: Access for business administrators
Some users or groups need access to objects in a different way than most other users and groups in your organization. For example, business administrators need more access controls compared to other users, such as being able to update or delete an object.

This scenario is a variant of "Scenario: Objects that are shared across GRC domains" on page 64.

Exception management

One example is exception or waiver management.

In general, exceptions from a requirement, control, or process are granted on a project basis. The project is a child of a business entity and is implemented as a risk entity. The project can have secondary associations to a process, a subprocess, or a requirement. Exceptions are child objects of the project and define the requirement, control, or process from which the exception is seeking relief. The project is granted the exception. If no specific project is involved in the exception, the business entity is granted the exception

All users can create exceptions but they can view only the exceptions that they created. The exception process custodians in IT have the job of reviewing and approving exceptions. You must extend role-based security to grant the exception process custodians in IT the ability to read and update all exceptions.

Privacy incidents

Another example involves the employees who are responsible for privacy incidents.

Specific individuals across the enterprise have responsibility for entering and maintaining information about Privacy incidents. In addition to other access that they have, they are designated as Privacy users and they might be in a Privacy Group or a Privacy Profile. The Privacy users can see all privacy incidents regardless of where the Privacy users are in the business hierarchy. They have access to additional fields on privacy incidents.

Similar functionality can be provided on other object types, such as audit findings, incidents, and waivers.

Scenario: All users can view objects and some users can update objects
Objects can be stored in a common area and shared across GRC domains. In this scenario, only a few users are allowed to update the objects. All other users have read access only.

This scenario is a variant of "Scenario: Objects that are shared across GRC domains" on page 64.

Role-based security is defined for all users to be able to read the objects in the folder. You want a small group to be able to create and another group to be able to update and associate.

Field level security

You can use field level security to control access to individual fields within an object. Field level security is applied to the set of objects that the user is entitled to by either role-based security or record level security rules. If no field level security is defined for an object, security is applied at the object level (if security rules are defined) or at the folder level.

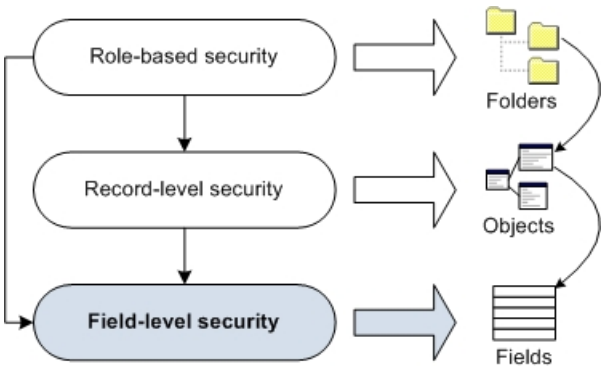


Figure 10: Field level security applies to object fields

When you define a field level security rule, you must consider all the scenarios that are required to access the field. If any scenarios are not defined, a user's access to the field is denied. This is known as redaction.

For example, one rule might specify that if a user is not an Owner, they have Read access only to a field. If a user is an Owner, they have Read and Update access. When the outcome of the formula is true, then Read access or Read and Update access is granted to a user. When the outcome of the formula is false, the field is redacted.

The way that access is restricted depends upon whether the outcome of a formula is true or false when it is applied to a field.

- True: The field is available to users as Read Only or Read and Update.
- False: The field is redacted. Users can see the field label, but not its value. Instead, the value is redacted, and the user sees some text, such as "Confidential" in place of the field value.

Restrictions:

- System fields are not supported.

  The system fields are "Name", "Description", "Location", "Creation Date", "Created By", "Last Modification Date", "Last Modified By", and "Comment".
- Computed fields are not supported.
- If more than one rule applies to a field, each is rule is combined by using an OR condition.
- If more than one rule is defined for the same field, and one grants Read access to the field and another grants Read and Update access, then a user is granted Read and Update access if the outcome of the formula for each rule is true.

Redacted fields
When you define a field level security rule, if the outcome of the formula is false, the field is redacted. Users can see the field label, but not its value. Instead, the value is redacted, and the user sees some text, such as "Confidential" in place of the field value.

You can change label of the text that is used to obscure the field value. For more information, see “Localizing application text” on page 281.

Defining field level security rules
Use field level security to restrict access to specific fields within an object.

Before you begin
You must enable System Administration Mode before you can define field level security.

Procedure

1. Click **Administration** > **Security Rules**.
2. Click the name of the object type for which you want to define a security rule.

3. Click **Add** adjacent to **Field Level Security Rules**.
4. Add a name and description for the security rule.
5. Add the formula for the security rule.

   You can type the formula or use the **Path**, **Field**, and **Terms** to define parts of the formula. You can also use a combination of both. For more information, see "Grammar for security rules" on page 74.

   a) To reference another object, either a parent or child, complete the following actions.

      For more information, see "Paths for parent and child objects" on page 71.

      1) Click **Path**.
      2) In the **Parent or Child** field, specify whether the path follows parent objects or child objects.
      3) Select the object type that is the starting point for the path.
      4) Select the object type that is the ending point for the path.
      5) Click **Search** to view the possible paths.
      6) Select one or more paths. If you select more than one path, use the **Combine Paths** field to specify how to use the multiple paths. Select **Any Path** if you want to use any of the paths or select **All Paths** if you want all paths to be used for the rule to be applied.
      7) Click **Insert**.

   b) To define a field condition, complete the following actions.

      For more information, see "Terms for data types" on page 72.

      1) Click **Field**.
      2) Select an object type.
      3) Select the field that you want to use.
      4) Select an operator. The list of operators changes depending on the field data type.
      5) Enter the value of the field condition.
      6) Click **Insert** to add the field condition into the rule formula.

      If you type the field condition, ensure that you use system names. If you do not specify an object type, the rule uses the object type for the object to which the rule applies. If you specify an object type, the object type must be either the subject of the rule or be specified in a path expression that contains the field reference.

      Optionally, you can use square brackets to ensure that when elements of field references contain spaces or other special characters, these field references are parsed.

   c) To add operators or keywords, use the **Terms** menu.
6. Click **Choose Fields**, and select the fields on which to apply the security rule, then click **Apply**.
7. For each field, specify the access controls.

   Read Only
   Users can read the field values, but not update them.

   Read and Update
   Users can read and update the field values.
8. Click **Save**.

Paths for parent and child objects

There can be several paths between objects. For example, there might be two paths between Object A and Object D: A-B-D and A-C-D. When you define a security rule, in the Path picker, you specify the starting point (Object A) and the end point (Object B). You are given a list of paths from which to pick.

To help you understand parent objects and child objects, consider the metaphor of a school. The students in the entire school can be thought of as having the role of any child. A classroom has a teacher, who can be thought of as the primary parent. The students in this classroom are the primary children of the

teacher. Other teachers have the role of any parent. If you want to use the path from a teacher to the students in the teacher's classroom, you use **Primary Parent** or **Primary Child** as the path qualifier.

Parent objects

You can use the following parent objects in the path.

Primary Immediate Parent
Paths follow only to the lowest level primary parent. Use **Primary Immediate Parent** for recursive object types only.

Primary Parent
Paths follow only to the primary parent. There can be only one primary parent.

If a primary parent is specified, the path follows only primary parent relationships.

Any Immediate Parent
Paths follow only to the lowest level parent. Use **Any Immediate Parent** for recursive object types only.

Any Parent
Paths follow to any level of parent, such as grandparent or parent, within recursive object types. For example, a control has a parent that is a subprocess and the subprocess has a parent. When you use **Any Parent** in the path for the control, the parent can be the subprocess or the subprocess's parent.

Child objects

You can use the following child objects in the path.

Primary Immediate Child
Paths follow only to the immediate, highest level child or to the immediate primary child. Use **Primary Immediate Child** for recursive object types only.

Primary Child
Paths follow only to the primary child, which is a child of a primary parent. A primary parent can have several primary children. A child can have only one primary parent.

If a primary child is specified, the path follows only primary child relationships.

Any Immediate Child
Paths follow only to the immediate, highest level children, if the child is a recursive object type. Grandchildren are excluded.

Any Child
Paths follow to any level of child, grandchildren or children, within recursive object types.

Terms for data types

This list contains the data types, operators, keywords, and other terms that are supported in a security rule formula.

The following data types are supported:

- Boolean
- Integer
- Decimal
- Date
- Currency
- Simple string including all display types
- Enumerated (single-valued and multivalued)

Terms that can be used with all data types

The following terms are used with all data types.

AND
Narrows the search for objects. The objects must meet all of the criteria.

OR
Broadens the search for objects. The objects must meet one of the criteria, not all of them.

NOT
Narrows the search by excluding all objects that match the specified criteria.

( ) (parentheses)
Groups criteria together to show the order in which the rule is applied.

If parentheses are not used, the precedence rules are:

1. **NOT**
2. **AND**
3. **OR**

Terms that are used with numeric data types

The following operators are used with numeric data types, such as decimal, integer, and currency data types. Security rules do not support field criteria on computed text fields or large text fields.

= (equal)
Compares the values in two fields and returns "true" if both contain the same value.

< (less than)
Compares the values in two fields and returns "true" if the second field is less than the first field. The two fields must be of the same data type. For example, both are decimal data types.

> (greater than)
Compares the values in two fields and returns "true" if the second field is greater than the first field. The two fields must be of the same data type. For example, both are decimal data types.

<= (less than or equal)
Compares the values in two fields and returns "true" if the second field is less than or equal to the first field. The two fields must be of the same data type.

>= (greater than or equal)
Compares the values in two fields and returns "true" if the second field is greater than or equal to the first field. The two fields must be of the same data type.

< > (not equal)
Compares the values in two fields and returns "true" if both contain different values.

Uses string variables.

Terms that are used with string data types

The following operators are used with data types that require strings, such as enumerated strings and simple strings. Security rules do not support long strings.

CONTAINS
Determines whether a multiple-select field contains a specific value or set of values.

ENDS WITH
Determines if the field value ends with the specified text.

LIKE
Determines if a field value matches the specified pattern string.

STARTS WITH
Determines if the field value starts with the specified text.

IN
Determines if the field value is in the specified field.

Terms that are used with date data types

TODAY
Returns today's date.

TOMORROW
Returns tomorrow's date.

NOW
Returns the current date and time.

You can specify a date in the future or in the past. For example:

- `NOW(5)` specifies a date five days from now.
- `NOW(2,'m')` specifies a date two months from now.
- `NOW(-5)` specifies a date five days ago.
- `NOW(-2,'y')` specifies a date two years ago.

You can use year, month, week, day, hour, minute, or second.

YESTERDAY
Returns yesterday's date.

DATE
Specifies the date and time as a string in the ISO format: `YYYY-MM-DD` and `hh:mm:ss.sTZD`.

You can also specify the date and its format as a string: `DATE('09/05/2013','MM/dd/yyyy')`

Terms that are used with other data types

END_USER
Returns the logged-in user.

END_USER_PROFILE
Returns the profile for the logged-in user.

IN GROUP
Returns the user group for the logged-in user.

IN PROFILE
Returns the specified field value that is in the specified profile.

INTENDED PARENT
Tests the parent under which a new object is to be created. It can be used only when you define a **Create** rule.

Use **INTENDED PARENT** when you want to control what a user or group can create. For example, you can allow specific users to create risks for subprocesses but not for issues.

When you use **INTENDED PARENT**, the condition can depend on the object type that is referenced as intended parent. The condition can also depend on the object type of the security rule's subject. A path expression that uses intended parent is considered false if the intended parent is not of the specified object type.

Grammar for security rules

As an administrator, you need to understand the grammar for a security rule formula so that you understand the potential impact of adding a rule.

`condition`

Condition is the basic building block for a security rule formula.

```
|--+-- predicate ----------------------+--|
   +-- NOT -- condition --------------+
   +--condition -- AND -- condition --+
   +--condition -- OR -- condition ---+
   +-- path-condition -----------------+
   '-- ( -- condition -- ) -----------'
```

The following rule applies to `condition`:

- If parentheses are not used, the precedence rules are:
  1. NOT
  2. AND
  3. OR

path-condition

```
                v------- AND ---------------.
>>-- FOR ( --+--- path-direction -- path --+--+-- : -- condition -- ) --<<
             | v-------- OR ---------------.  |
             +--- path-direction -- path --+--+
             '-- intended-parent -------------'
```

predicate

```
|--+-- scalar --+-- = ---+-- scalar --+--|
    |            +-- < ---+            |
    |            +-- > ---+            |
    |            +-- <= --+            |
    |            +-- >= --+            |
    |            '-- <> --'            |
    +-- like-predicate -----------------+
    +-- starts-with-predicate-----------+
    +-- contains-predicate--------------+
    +-- ends-with-predicate-------------+
    +-- in-predicate -------------------+
    +-- in-group-predicate--------------+
    '-- in-profile-predicate------------'
```

scalar-value

```
|--+-- field-reference -- +--|
    +-- end-user-profile --+
    +-- boolean ------------+
    +-- integer ------------+
    +-- decimal ------------+
    +-- date ---------------+
    +-- currency -----------+
    +-- simple string -----+
    +-- enum-value ---------+
    '-- function -----------'
```

field-reference

```
>>--+-----------------+-- . -- field-group -- . -- field-name --<<
    '-- object-type --'
```

The following rules apply to the `field-reference`:

- If no `object-type` is given, the object type is that of the object to which the rule applies.
- If an `object-type` is given, it must either be the subject of the rule or been specified in a path expression that contains the field-reference.
- All elements of the field reference must be system names.
- Optional square brackets can be used to assure parsing in case elements of field references contain spaces or other special characters.

end-user-profile

```
|-- END_USER_PROFILE ( --+-- field-reference --+-- ) --|
                         '-- string -----------'
```

function

```
|--+-- TODAY ------------------------------------------+--|
   +-- TOMORROW ---------------------------------------+
   +-- NOW --------------------------------------------+
   |         .-- ( 0, 'd' ) ---------------------------.  |
   |         |              .-- , ----- 'd' ---.       |  |
   '-- NOW --+-- ( -- offset +------------------+-- ) --+--'
                             '-- , --+-- 'y' ---+
                                     +-- 'm' ---+
                                     +-- 'd' ---+
                                     +-- 'h' ---+
                                     +-- 'mi' --+
                                     '-- 's' ---'
```

like-predicate

```
|-- field-reference -- LIKE -- pattern-string --|
```

The following rule applies to the `like-predicate`:

- The pattern string must be a string constant.
- For information on what is supported for the `like-predicate`, see “Limitations on special characters in filters for long string fields” on page 192 and “Using complex logic in a search filter” on page 195.

starts-with-predicate

```
|-- field-reference -- STARTS WITH -- string --|
```

contains-predicate

```
|-- field-reference -- ENDS WITH -- string --|
```

ends-with-predicate

```
|-- field-reference -- ENDS WITH -- string --|
```

in-predicate

```
|-- scalar-value -- IN --+-- scalar-value ----------------+--|
                         |      v--- , -----------.       |
                         '-- ( --- scalar-value --+-- ) --'
```

The following rules apply to `in-predicate`:

- If a single field reference is given, it must be a multivalued field.
- If multivalued fields are used in the list, they are unnested.

in-group-predicate

```
|-- scalar-value -- IN GROUP --+-- scalar-value ----------------+--|
                               |      v--- , -----------.       |
                               '-- ( --- scalar-value --+-- ) --'
```

The following rules apply to `in-group-predicate`:

- If a single field reference is given, it must be a multivalued field.
- If multivalued fields are used in the list, they are unnested.

in-profile-predicate

```
|-- scalar-value -- IN PROFILE --+-- string ----------------+--|
                                 |      v--- , -----.       |
                                 '-- ( --- string --+-- ) --+
```

The following rules apply to `in-profile-predicate`:

- If a single field reference is given, it must be a multivalued field.
- If multivalued fields are used in the list, they are unnested.

path

```
                   v----------------------.
 |-- object-type ----- / -- object-type --+--|
```

path-direction

```
    .-- ANY ------.                  .-- CHILD ---.
 |--+-- PRIMARY --+----------------+--+-- PARENT --+--|
                  '-- IMMEDIATE --'
```

intended-parent

```
 |-- INTENDED PARENT OF TYPE -- object-type -- |
```

Rules

- Combining multiple paths with AND or OR is semantically equivalent to specifying multiple path expressions with the same condition combined by AND or OR.
- For combined paths, the end point of all paths in the path expression must have the same object type. The condition can contain references only to the shared starting points and ending points as well as any references to outer paths that lead up to the subject.
- A path expression for a given path of object types is considered true if the condition is true for any instantiation of the path.
- Except for combined paths described earlier, the condition can depend on any object type along the path of the path-expression.
- The condition may also depend on object types along the path of containing path-expressions or the subject object type of the rule.
- When using `intended-parent`, the condition can depend on the `object-type` referenced as intended parent as well as the subject `object-type` of the rule. A path expression that uses the intended parent clause is considered false if the indented parent is not of the specified `object-type` or the operation is not Associate or Create.
- Depending on the path-direction specified, the path lists a connected series of object types relative to the current context either following parent or child relationships.
- The outermost path must start with the rule's subject type. Nested paths must start with the endpoint of the immediately containing path.
- If IMMEDIATE is specified and the end point of the path is a recursive object type, the path stops at the bottom most parent of that type or the top most child.
- If PRIMARY is specified, the path will follow only primary parent relationships.

Enabling or disabling a security rule

You can work on a security rule without making it available to your users. When the security rule is ready, you can enable it. Conversely, you can withdraw a security rule by disabling it so that you can make all required changes to it.

Before you begin

You must enable System Administration Mode before you can work with security rules.

Procedure

1. Click **Administration** > **Security Rules**.
2. Select the object type that contains the security rule that you want to enable or disable.
3. Enable or disable the security rule.

Validating a formula for a security rule

When you validate a formula for a security rule, IBM OpenPages GRC Platform checks the completeness of the formula that you entered and verifies that the syntax of the rule is correct.

Note: The validation is validating only whether the rule is syntactically correct. It does not validate whether the values are valid. The values that you provide are validated when you save.

For example, in the following expression, the left side of the equation shows an enumerated string field. The right side has a Boolean value. The syntax would be correct if the status field was Boolean. The validation does not recognize that the data types are different.

```
[SOXIssue].[OPSS-Iss].[Status] = FALSE
```

Before you begin

You must enable System Administration Mode before you can work with security rules.

Procedure

1. Click **Administration** > **Security Rules**.
2. Select the object type that contains the security rule that you want to validate.
3. Click on the security rule, and then click **Edit**.
4. Click **Validate** for the formula that you want to validate.
5. When you see a message that the formula has successfully validated, click **Save**.

Deleting a security rule

When a security rule is no longer required, you can delete it. You cannot undo the deletion.

Before you begin

You must enable System Administration Mode before you can work with security rules.

Procedure

1. Click **Administration** > **Security Rules**.
2. Select the object type that contains the security rule that you want to delete.
3. For the security rule that you want to delete, click **Delete**.

Best practices for security rules

When you configure security rules, consider the best practices.

Combining record level security rules for an object type

If you have a (Create) and (Read or Associate) rule for an object type, you must add an extra OR condition to the (Read or Associate) rule. This condition is required so that the (Create) and (Read or Associate) rules to can work together.

The OR condition looks like this:

```
(NOT(FOR (Any Parent [Rule_ObjectType]/PATH : 1=1))
    AND [Rule_ObjectType].[System Fields].[Created By] = END_USER)
```

Where:

Rule_ObjectType is the object type in which the Read rule is created.

PATH is the path of the Read rule, starting from the Rule_ObjectType.

The following example shows the security rule for LossEvent to control the Read operation for LossEvents under BusinessEntity.

```
OR (NOT(FOR (Any Parent [LossEvent]/[SOXBusEntity] : 1=1))
    AND [LossEvent].[System Fields].[Created By] = END_USER)
```

Custom security for projects

You can set custom security access control (Read, Write, Delete, Associate) on folders for Project Milestones and Project Action Items.

Use the **Custom Security Access Control** page to set custom security access control. 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 **Common** > **Custom ACL Object Types** setting in the **Settings** page. Add object names separated by commas.

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

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 of 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. 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.

Creating an Access Control List

You can control which users and groups can access Project Milestones and Project Action Items.

Before you begin

Before you can add an Access Control List (ACL), you must disable system admin mode.

Procedure

1. Log on to IBM OpenPages GRC Platform as a Super Administrator user with the **Access Control Lists** application permission set.
2. Click **Administration** > **Custom Security**.

3. Click **Default** > **Plan** and do the following:
   - For Project Milestones - click the **Milestone** link.
   - For Project Action Items - click the **Task** link.
4. On the **Access Control** tab, click **Actions** > **Add**.
5. On the access control entry page:
   a) Search for the user or group you want to add.
   b) For each permission (Read, Write, Delete, Associate), select a setting value (Granted, Inherited, Denied).
   c) Click **Add**.

   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.

Editing an Access Control List

You can edit an Access Control List for a user or group.

Before you begin
Before you can edit an Access Control List (ACL), you must disable system admin mode.

Procedure

1. Log on to IBM OpenPages GRC Platform as a Super Administrator user with the **Access Control Lists** application permission set.
2. Click **Administration** > **Custom Security**.
3. Expand the folder hierarchy and click the folder that has the Access Control List you want to modify.
4. 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) Click **Save**.

Deleting an Access Control List

You can delete an Access Control List for a user or group.

Before you begin
Before you can delete an Access Control List (ACL), you must disable system admin mode.

Procedure

1. Log on to IBM OpenPages GRC Platform as a Super Administrator user with the **Access Control Lists** application permission set.
2. Click **Administration** > **Custom Security**.
3. Expand the folder hierarchy and click the folder that has the Access Control List you want to modify.
4. 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 **Actions** > **Remove**.

Field level encryption

You can encrypt specific fields in the IBM OpenPages GRC Platform repository to prevent system administrators from viewing confidential data directly from the database. Data in encrypted fields is shown as a string of random characters.

Simple string and long string field data types are supported.

Note: Before encrypting long strings in OpenPages running on Oracle 12.1, refer to the following Technote: http://www.ibm.com/support/docview.wss?uid=swg22010106. The Technote describes a potential issue and how to resolve it by obtaining the appropriate patch from Oracle support and applying it to your environment. The IBM OpenPages GRC Platform reporting framework handles encrypted fields by running a database function to decrypt them. When a long string (CLOB) field is made encrypted, the framework must be regenerated to call this database function. For more information, see "Generating the reporting framework " on page 683.

Restrictions:

- The maximum size of long strings that can be encrypted is 2 MB.
- Do not include encrypted long string fields in the search criteria for a filter because they can return unexpected results.

Create a file for the encryption keystore and key pair

Before you can set up the encryption keystore in IBM OpenPages GRC Platform, you must create a file that contains the encryption keystore and key pair details.

The file must use the Java format (jceks). Although you can use any keytool to create the file, it must use the same format as a Java keystore.

The encryption key must use one of the following encryption algorithms. Any other algorithms are not supported.

Attention: You must obtain special files for key sizes greater than 128. For more information, see "Special encryption files for 192 bit and 256 bit encryption" on page 82.

Table 27: Supported encryption algorithms

Algorithm name	Key size
3DES	168
AES128	128
AES192	192
AES256	256

In the following example, the command generates a keystore that uses the supported Java format (jceks). The encryption key uses a 3DES encryption algorithm with a key size of 168.

```
keytool -genseckey -alias openpages -keyalg 3DES -keysize 168
 -storetype jceks -keystore keystore-3DES.jks
```

In the following example, the command generates a keystore that uses the supported Java format (jceks). The encryption key uses an AES encryption algorithm with a key size of 128.

```
keytool -genseckey -alias openpages -keyalg AES -keysize 128
 -storetype jceks -keystore keystore-AES128.jks
```

In the following example, the command generates a keystore that uses the supported Java format (jceks). The encryption key uses an AES encryption algorithm with a key size of 192.

```
keytool -genseckey -alias openpages -keyalg AES -keysize 192
 -storetype jceks -keystore keystore-AES192.jks
```

In the following example, the command generates a keystore that uses the supported Java format (jceks). The encryption key uses an AES encryption algorithm with a key size of 256.

```
keytool -genseckey -alias openpages -keyalg AES -keysize 256
 -storetype jceks -keystore keystore-AES256.jks
```

Special encryption files for 192 bit and 256 bit encryption

By default, applications that are based on Java technology include an IBM JRE that does not support Advanced Encryption Standard 192-bit (AES-192) or Advanced Encryption Standard 256-bit (AES-256) encryption.

The United States export administration regulations for strong cryptography prohibit including such software support. Administrators can enhance an IBM JRE to work with AES-256 and AES-192 encryption by obtaining the IBM Java Cryptography Encryption (JCE) unrestricted policy files from IBM Unrestricted SDK JCE policy files.

Note:

You must have a universal IBM ID to download the files. If you do not have an IBM ID, click the registration link on the page and perform the following steps:

1. Log in.
2. Select **Java 5.0 SR16, Java 6 SR13, Java 6 SR5 (J9 VM2.6), Java 7 SR4, Java 8 GA, and all later releases**.
3. Click **Continue**.
4. In the new page, check **I Agree** and select **I confirm**.
5. In the new page, click the **Download now** link.
6. Extract the download and copy the JAR files to the *<JAVA_HOME>*`/jre/lib/security` directory, overwriting those already there.

Attention: For the changes to take effect, you must restart the OpenPages application servers. For more information, see Chapter 20, “Starting and stopping servers,” on page 549.

Setting up the encryption keystore

The encryption keystore is a file that stores the key that you use to encrypt data in the IBM OpenPages GRC Platform repository.

The keystore file must be on the admin server.

In a horizontal environment, the keystore file must also be available to each application server There are two options:

- Each application server must have access to the file location on the admin server.
- The file must be available in the same location on each application server.

Before you begin

You must enable System Administration Mode before you can set up the encryption keystore.

Procedure

1. Click **Administration** > **Encryption Keystore**.
2. Click **Edit**.
3. Enter the name of the encryption key in the **Key Name** field.
4. Enter the alias in the **Key Alias** field.

   Important: Ensure the alias that you specify here is an exact match to the alias in the keystore file.
5. Enter the keystore location in the **Keystore Location** field.

   For security reasons, you cannot browse to the location, you must type it in manually.
6. Enter the password to access the **Keystore Password** field,

   Important: Ensure the password that you specify here is an exact match to the password in the keystore file.
7. Confirm the password in the **Re-enter Keystore Password** field.
8. Select the encryption algorithm that is used by the key in the **Algorithm** field.
9. Enter a description for the keystore in the **Description** field.
10. Click **Update**.

What to do next
You must now enable the key to encrypt the repository.

Enabling the encryption keystore

After you set up the encryption keystore, you must enable it to encrypt the IBM OpenPages GRC Platform repository. If required, you can disable the keystore later to decrypt the repository again.

When you enable the keystore, any fields that are currently marked for encryption are automatically encrypted in the repository. If there are no fields that are marked for encryption, the keystore is enabled, meaning that it is ready to automatically encrypt any fields that are marked for encryption from now. For information on marking fields for encryption, see "Encrypting field values" on page 151.

Procedure

1. Click **Administration** > **Encryption Keystore**.
2. Click **Enable**.

   Depending on the size of the repository, encryption can take a long time. Encryption runs as background event. You can view the progress by clicking **Refresh**.

Disabling the encryption keystore

After the IBM OpenPages GRC Platform repository is encrypted, you can disable the keystore to decrypt the repository again.

When you disable the keystore, any fields that are currently marked for decryption are automatically decrypted in the repository. If no fields are marked for decryption, the keystore is disabled, meaning that it is ready to automatically decrypt any fields that are marked for decryption from now. For information on marking fields for decryption, see "Decrypting field values" on page 152.

Procedure

1. Click **Administration** > **Encryption Keystore**.
2. Click **Disable**.

Depending on the size of the repository, decryption can take a long time. Decryption runs as background event. You can view the progress by clicking **Refresh**.

Updating the encryption keystore

Your company IT policy might require that you periodically change the encryption key. Whenever the encryption key details change, you must update the encryption keystore in IBM OpenPages GRC Platform.

If it is already encrypted, you do not need to disable the encryption keystore to update it.

Procedure

1. Click **Administration** > **Encryption Keystore**.
2. Click **Edit**.
3. Enter the current encryption keystore password to access it.
4. Update the details in the keystore.

   For more information, see "Setting up the encryption keystore" on page 82.
5. Click **Update**.

   Depending on the size of the repository, updating the encryption can take a long time. Encryption runs as background event. You can view the progress by clicking **Refresh**.

LDAP user authentication

IBM OpenPages GRC Platform supports the use of an LDAP (Lightweight Directory Access Protocol) authentication server to control user access.

To use LDAP user authentication, you integrate OpenPages GRC Platform with an LDAP data source.

Only one login module can be active at the same time. OpenPages GRC Platform supports a single namespace. All users must be authenticated through the same data source. Multiple authentication modules can be used in a multi-forested environment.

Users that are created or imported into OpenPages GRC Platform must also be defined in the LDAP authentication server. The administrator managing the OpenPages GRC Platform users is responsible for maintaining the correlation between the OpenPages GRC Platform user list and the external LDAP data source. If a user is disabled on the OpenPages GRC Platform server, the user must be manually disabled on the LDAP Directory server.

Note: If an LDAP Directory server is being used for user authentication, the **Change Password** option is disabled in OpenPages GRC Platform. When an LDAP server is used, passwords are not maintained in OpenPages GRC Platform. The password must be changed in the LDAP server.

You can also configure OpenPages GRC Platform to use an external LDAP user authentication server over SSL. For more information, see "Modifying the LDAP configuration file for LDAP over SSL" on page 514.

Configuring the LDAP Authentication Module

To successfully use an LDAP Directory Server with IBM OpenPages GRC Platform, you must configure the LDAP Authentication Module to recognize the presence of the LDAP server.

To configure OpenPages GRC Platform to work with an external LDAP authentication source, complete the following tasks:

- "Adding existing users to the LDAP server" on page 85
- "Changing the OPSystem password" on page 85
- "Modifying the LDAP configuration file" on page 85

Adding existing users to the LDAP server

You can add existing IBM OpenPages GRC Platform users to an LDAP server.

Make sure to refer to your LDAP Directory Server documentation for the steps required to add 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 20 characters. User names that exceed the 20-characters 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 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 "Changing the OPSystem password" on page 85 to change the OPSystem account password system-wide.
- The OpenPages GRC Platform Super Administrator (for more information, see "The Super Administrator" on page 21)
- OPAdministrator (only if you are using this account)

Changing the OPSystem password

If the OPSystem password on the LDAP server does not match the one installed by the IBM OpenPages GRC Platform 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.

   For Microsoft Windows operating systems, the default installation directory of OpenPages GRC Platform is `C:\OpenPages`.

   For AIX and Linux operating systems, the default installation directory of OpenPages GRC Platform is `/opt/OpenPages`.
4. Execute one of the following commands to open the `chng-sys-pswd` tool:

   For Windows, run `chng-sys-pswd.bat`

   For AIX and Linux, run `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. Restart all services to enable the new password.

Modifying the LDAP configuration file

You must modify the authentication configuration file to enable the LDAP Directory Server that you are using.

Note: If you are using LDAP over SSL, see "Modifying the LDAP configuration file for LDAP over SSL" on page 514.

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

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

The only module that the IBM OpenPages GRC Platform system pays attention to is the module that is named Openpages. Therefore, you need to make a backup of the Openpages module, rename the OpenpagesIP or OpenpagesAD to Openpages, and then change the settings to reflect the settings of your LDAP server.

Procedure

1. Stop all OpenPages GRC Platform 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 GRC Platform application.
3. Find the Openpages module and change its name to OpenpagesDefault.
4. Modify either the OpenpagesIP or OpenpagesAD module name to Openpages.
   - If you are using a Microsoft Active Directory server, change the name of the OpenpagesAD module to Openpages.
   - If you are using a Sun One Directory Server, change the name of the OpenpagesIP module to Openpages.
   - If you are using a different LDAP server, you can use either of these modules. Choose a module to use as a template and change its name to Openpages.
5. Specify the correct values for the following properties in the module that you named Openpages:

   provider.url
   Change the value to the hostname and port number for the LDAP authentication server. For LDAP, the protocol is ldap and the port is the LDAP port number (by default, 389).

   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, 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
   You can add additional custom parameters that are supported by the Java Naming and Directory Interface (JNDI). Precede a JNDI property with the ctx.env. prefix.

   For example, if you want to use the JNDI property com.sun.jndi.ldap.connect.timeout, use ctx.env.com.sun.jndi.ldap.connect.timeout="*<value>*" in the aurora_auth.config file.

   For information about JNDI properties, see the Java SE documentation (http://docs.oracle.com/javase/7/docs/technotes/guides/jndi/jndi-ldap.html#JNDIPROPS).

   For example:

   ```
   Openpages
   {
      com.openpages.aurora.service.security.namespace.LDAPLoginModule
            required debug=false
         provider.url="ldap://myserver.company.com:389"
         security.authentication="simple"
         security.search.user.dn="cn=Directory Manager"
         security.search.user.credentials="openpages"
         base.dn="ou=people,o=IBM,c=US"
         user.attr.id="uid"
   ```

```
      ;
};
```

6. When you are finished editing the file, save your changes and exit.
7. Restart all services.

Results

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

Setting up mixed-mode authentication

Use mixed-mode authentication when not all users can use a single namespace for authentication.

This solution should be used by customers who do not want to create the OPSystem, SOXAdministrator, OpenPagesAdministrator, or OPAdministrator user accounts on their LDAP server but do want all their users to be authenticated by LDAP. The following procedure creates a new namespace and modifies user names (such as OPSystem) to authenticate against the OpenPages GRC Platform authentication module rather than LDAP.

Procedure

1. To create the namespace modules in the `aurora_auth.config` file, log on to the application server.
2. Find and open the `aurora_auth.config` file.
3. Create or update the namespace modules in the file as follows:

```
OpenpagesDefault
{
com.openpages.aurora.service.security.namespace.AuroraLoginModule
required debug=false;
};


Openpages
{
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"
;
};
```

4. To create the namespace in the database, log into the database instance with the database id, such as OPENPAGES.
5. Run the following SQL to create the `OpenpagesDefault` namespace:

```
insert into namespaces (NAMESPACEID, NAME, JAASLOGINMODULE,
DESCRIPTION) values (namespaceidseq.nextval, 'Openpages Security',
'OpenpagesDefault', 'Default Openpages Security Namespace');
```

6. Run the following SQL to point an ID to the new namespace:

```
update actors set namespaceid = (select namespaceid from
namespaces where JAASLOGINMODULE = 'OpenpagesDefault') where actorid =
(select actorid from actorinfo where name = 'user_name');
```

   For example, the following SQL will have the OPSystem use the `OpenpagesDefault` namespace for authentication:

```
update actors set namespaceid = (select namespaceid from
namespaces where JAASLOGINMODULE = 'OpenpagesDefault') where actorid =
(select actorid from actorinfo where name = 'OPSystem');
```

7. Commit the changes to the database.

Configuring a multi-forested LDAP authentication

IBM OpenPages GRC Platform supports the use of multiple LDAP authentication servers in a multi-forested configuration. If the application 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 GRC Platform 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, OpenPages GRC Platform 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 5. Managing the reporting schema

The IBM OpenPages GRC Platform application supports the use of a real-time reporting schema model that allows reports to access information as it is entered into the system. Data does not have to be exported to an external reporting database repository.

See “Changes that require the reporting schema to be regenerated” on page 89 for a list of tasks that require the reporting schema to be recreated. The OpenPages GRC Platform application does not have be restarted after recreating the reporting schema.

The Reporting Schema page is used to control the creation and deletion of the reporting schema. Administrative-level users who have the Reporting Schema application permission can access the page.

Reporting schema permissions

Before performing any actions on a reporting schema, you must have specific application permissions set on your account.

For more information, see “Types of application permissions” on page 32).

Table 28: Reporting schema and framework permissions

This application permission...	**Is used to...**
Reporting Schema	access the **Reporting Schema** menu item.
System Administration Mode	enable and disable System Administration Mode.

Accessing the reporting schema

You can create, recreate, disable, drop, and view the status of a reporting schema from the Reporting Schema detail page.

Important: The system must be in System Administration Mode (see “Enabling and disabling System Administration Mode” on page 17) to modify the reporting schema.

Before you begin

Complete the following steps to access the reporting schema:

Procedure

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

Changes that require the reporting schema to be regenerated

Users can create a new or updated reporting schema when necessary.

The following table lists the changes that require you to regenerate the reporting schema and the reporting framework:

Table 29: Regenerating the reporting schema and the reporting framework.

This type of change...	**Requires this to be regenerated...**	
	Reporting schema	**Reporting framework**
Adding a new field to a field group.	No	Yes
Adding a new object type.	No	Yes
Adding a new association between object types.	No	Yes
Removing object types or attributes. For information, see "Deleting a custom object type" on page 189.	Yes	Yes
Encrypting a long string (CLOB) field.	No	Yes
Enabling facts or dimensions.	No	Yes
Defining, modifying, or deleting business entity recursive object levels.	No	Yes
Removing a field from a field group.	No	Yes
Disabling an association between object types.	No	Yes
Disabling facts or dimensions.	No	Yes
Switching the security model. **Note:** Switching the security model after data is loaded or migrated into the system is not recommended and requires assistance from the OpenPages Professional Services team.	Yes	Yes
Changing the value of the **Populate past periods** setting. For information, see "Populating past reporting periods" on page 91.	Yes	No
Changing any setting used to compose URL links in the reporting schema, for example, the Host, Port, and Protocol settings. For information about updating the reporting schema, see "Updating URL host pointers for reports" on page 478 if you want to run the `RPS_Update` SQL script or "Creating or recreating the reporting schema" on page 91 if you are update manually.	Yes	No
Adding an index to an RT_column by using the **Settings** > **Platform** > **Reporting Schema** > **Create Index on Fields** setting.	Yes	No
Configuring the triangles setting. For information, see "Triangle object relationships" on page 663.	Yes	No
Changing an enumerated field from single-valued to multivalued and there is data in the field (DB2 only).	Yes	No

Other situations that require the reporting schema to be created, recreated, enabled, and disabled are described in the *IBM OpenPages GRC Installation and Deployment Guide*.

Two ways are provided to update the reporting schema: incrementally through scripts and with the user interface.

- 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 GRC Platform Support and do not ship as part of the product.
- Application user interface - this method updates the entire reporting schema (see "Creating or recreating the reporting schema" on page 91). 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 Cognos reports may not cause your modifications to appear in the standard 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 recreating the reporting schema

You can create or recreate the reporting schema.

Before you begin
Complete the following steps to create or recreate a reporting schema:

Procedure

1. Access the Reporting Schema. Log on to the IBM OpenPages GRC Platform application user interface as a user with the **Reporting Schema** application permission set.
   a) From the menu bar, select **Administration** and click **Reporting Schema**.
2. Enable System Administration Mode (for details, see "Enabling and disabling System Administration Mode" on page 17).
3. Perform one of the following actions:
   - If a reporting schema already exists, click **Re-Create** to drop the existing schema and create a new schema.
   - If no reporting schema exists, click **Create**.
4. When the creation task (or re-creation task) is complete, update the Reporting Framework so that the Cognos reports can access the new schema. For more information, see "Updating the reporting framework" on page 686.

Populating past reporting periods

You can control whether data from previous reporting periods is included in the reporting schema.

By default, the reporting schema is only populated with the data from the current reporting period. Use the following procedure to populate the reporting schema with past periods:

Procedure

1. From the menu bar, select **Administration** and click **Settings**.
2. Expand the **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:

Table 30: Past period reporting values	
Value	**Description**
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. Click **Save**.
6. Recreate the reporting schema (see, "Changes that require the reporting schema to be regenerated" on page 89).

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 icons that allow you to perform these tasks.

Procedure

1. Enable System Administration Mode (for details, see "Enabling and disabling System Administration Mode" on page 17).
2. From the menu bar, select **Administration** and click **Reporting Schema**.
3. Enable or disable the reporting schema:
   - Click **Enable** to enable the reporting schema. If the schema does not exist, click the **Create** icon to create the reporting schema. Creating the reporting schema will automatically enable the new schema.
   - Click **Disable** to disable the reporting schema. If you want to reclaim the database space taken by the reporting schema tables, you must click the **Drop** icon. This will automatically disable the reporting schema.

Viewing reporting schema operation details

IBM OpenPages GRC Platform keeps a log of each reporting schema operation that has been performed.

Before you begin
Complete the following steps to view the reporting schema details:

Procedure

1. Access the Reporting Schema. Log on to the IBM OpenPages GRC Platform application user interface as a user with the **Reporting Schema** application permission set.
   a) From the menu bar, select **Administration** and click **Reporting Schema**.
2. On the **Reporting Schema Operations** pane, click the name of the operation.
3. On the **Operation Detail** pane, click **View Log**.

Chapter 6. Business process visualizations

As a Risk analyst or Compliance manager, you can graphically render your business process and communicate it to other users of risk analysis. By visualizing the business process, which can include the subprocesses, activities, risks, and controls, you can speed the risk management process and data analysis.

Some of the visualizations that you can add to your processes are Business Entity Organization charts and process diagrams. These built-in templates are available to help users create interactive visualizations. You can use the visualizations to communicate information about the process flows and the business organizational structure and to share the information throughout the enterprise. You can design the flow of a business process and key components from beginning to end.

The business process visualizations provide users with the following benefits:

Navigation
Users can go from the process flow to the details page of the GRC object or to the Activity View in OpenPages GRC Platform.

Representation
Data is displayed graphically for easier interpretation and analysis.

Context
To understand the context in which models are shown, supporting information is provided.

By using visualizations, users can achieve the following goals:

- Proactively assess risks that affect the organization.
- Analyze materialized risks, such as losses or violations.
- Identify and track actions in response to risks.
- Identify problems or trouble areas.
- Conduct a risk and control self-assessment to identify missing risks.
- Determine whether the organization has the necessary controls on the risks, and evaluate those controls.
- Capture changes to laws and regulations, and provide visibility into policies, incidences, and issues, and ultimately provide the status of regulatory compliance.
- Report on the data.

The process flow diagrams are dynamic and directly connected to the underlying data that supports them. The diagrams represent the status of the GRC data. You can directly access data from common databases, such as DB2 and Oracle, including data that is stored in report services definitions. Report authors can also embed visualizations in IBM Cognos reports.

Restriction: Navigational views are not available for the following visualization object types and cannot be defined in any object profile:

- Process Diagram

  A process diagram object can be accessed only through the **Detail** page of the parent Process object.
- Data Input and Data Output

  These object types are connectors that are used in visualization diagrams and can be accessed only through the **Detail** page of the associated Process and Risk objects.

As an administrator, even if you enable a navigational view for the Process Diagram, Data Input, or Data Output object type, the navigation view is not available as a standard menu item in the appropriate menu for users who are associated with that profile. These objects are available only in the context of business process flow and Business Entity visualization diagrams.

If you are upgrading OpenPages GRC Platform from a version earlier than 7.0.0, the visualization object types and related diagrams are not available. To add support for visualizations, contact OpenPages GRC Platform Professional Services for assistance.

The reporting schema is required to successfully render visualizations. Because the reporting schema is populated only with the data for the current report period, active reporting periods are not supported for visualizations.

Types of visualizations

Built-in visualizations are provided as a starting point for designing new process diagrams or viewing the organizational chart for a Business Entity.

By default, the following visualization templates are installed on all IBM OpenPages GRC Platform systems:

- Business Process Flow visualization
- Business Entity Organizational Charts

Business process flow visualization

Risk professionals can use the process flow visualization to make sure that the documented flow accurately reflects the business process and its sub-processes, data inputs and outputs, risks and controls. Users can also update in real time to reflect any changes.

A process flow visualization is a child object of the Process. You can use the following major elements to build your process flow diagram.

Process Object
Process object types represent the major end-to-end business activities within a business entity that are subject to risk. Process objects are typically used in areas such as financial reporting, compliance, and information security. Depending on the diagram, the process object is not explicitly shown; however, it exists to provide context.

Subprocesses (or Activities)
A Subprocess object type is a component of a Process object. It is used to break down processes into smaller granular units for assessment purposes.

Risks
Risk object types represent potential liabilities. Risk objects can be associated with, for example, business processes, business entities, or compliance with a particular mandate. Each Risk object has one or more Control objects that are associated with it that provide safeguards against the risk and help mitigate any consequences that might result from the risk.

You can use the Risk object to categorize risks; capture the frequency, rating, and severity of inherent and residual risk data; and view reports that help identify your top risk items.

The process flow is visually optimal when risks for each process are fewer than five.

Controls
Control object types typically represent policies and procedures to help ensure that risk mitigation responses are carried out. After you identify the risks in your practices, you can then establish controls (such as approvals, authorizations, and verifications) that remove, limit, or transfer these potential risks.

A process flow is visually optimal when you have one to two Controls per Risk.

Data Input and Data Output objects
Data Input objects and Data Output objects are child objects of the Process and can have associations only to existing Risks. They represent elements of a flow to depict an Input into the Business Flow or an Output from various activities within a process, such as running a report or updating a CRM system or getting an external data source feed.

The flow of the process is represented by connectors that link the activities, inputs and outputs, and decision-branching points. You can specify labels for the decision connections.

All elements and relationships of the Business Process visualizations are stored as data in the OpenPages GRC Platform repository on the OpenPages GRC Platform server. The element types are shown or hidden in the Application Object Views that are based on Profiles. You can have multiple diagrams per process. For example, some diagrams can be at different stages of the process, such as those diagrams that are published or are being revised or approved.

Business Entity organization charts

The Hierarchy diagram provides contextual and aggregate views of the Business Entity data model. The organizational structure of a company is captured as Business Entity objects in the OpenPages GRC Platform GRC repository, which can be visualized as an organizational chart.

This type of structure is useful for infrequent users who must understand the complex model quickly and who have business entities with risk assessments. Color codes indicate the status that is based on aggregation.

The visualization includes the recursive object levels for the Business Entity object type. Users can select to show a specified number of levels of the structure. The following table outlines what the different business levels of the organizational structure might include.

Table 31: Levels of a Business Entity

Level	Description
1	Company name
2	Divisions and subsidiaries
3	Regions

Because the chart is a rendering of the Business Entity objects and the parent-child associations, users cannot modify or author a Hierarchy diagram.

Visualizing a Business Entity organization chart

You can view a graphical representation of the Business Entity as an organization chart.

Procedure

1. Complete one of the following actions:
   - To use a hierarchical view of the Business Entity, click **Organization** > **Business Entity Overview** and select a Business Entity.
   - To use the Filtered List View of Business Entities, click **Organization** > **Business Entities** and select a Business Entity.
2. In the details pane, in the **Business Entity Chart** field, click the **Hierarchy Diagram** link.

   A new browser window shows the organization chart as a visualization of the Business Entity. To view the legend, click the down arrow.
3. To view a different level of the organizational chart, from the Level list, click the level that you want.

   In general, level 1 is the company name, level 2 is the divisions and subsidiaries, and level 3 is the regions and branches. If an element includes a child level that you can expand further, the element includes an ellipsis in a small circle.
4. To make a branch within the root level, right-click the element in the chart, and select **Make Root**.

Tip: To return to the last level viewed, click **Back**  .

5. To view more information about an element in the chart, choose one of the following actions:
   - To view detailed information about an element, right-click the element and click **Properties**.
   - To open the corresponding **Detail** page or **Activity View** for any element, right-click the element, and click **Open Detail Page**.
   - To show the chart that is zoomed to fit entirely into your browser window, click **Fit to Window**  .
6. To refresh the chart and retrieve the most recent data from the database, click **Refresh**  .

Visualizing a business process flow

You can view a graphical representation of the flow for a business process and key components from the beginning of the process to the end.

About this task

The associated IBM Cognos reports control which elements are shown in the diagram. IBM OpenPages GRC Platform objects are obtained from the report that is associated with the process. If you want to view only the controls or risks, the report authors must specify or filter the control or risk data when they design the report specification.

If you have permission to view the process, you have permission to view all of its subprocesses. Although you can view the object associations, you cannot create or change associations between subprocesses, risks, or controls.

A process diagram can have a status of Draft, Published, or Obsolete.

Procedure

1. Click **Organization** > **Processes** and enter a filter.
2. In the **Filtered List View**, select a Process.
3. On the **Process Detail** page, under **Associations**, click **Process Diagrams**.
4. On the **Process Diagram List** page, under **Name**, click the diagram that you want to view.
5. In the form page, click the **Process Diagram** link.
   The Process Diagram editor is opened in Read-only mode or Edit mode, depending on your access permissions to the process.
6. To view more information about the diagram, choose one of the following actions:
   - To view detailed information about an element, click the element to display its details.
   - To open the corresponding **Detail** page or **Activity View** for any subprocess, risk, control, input, or output node, right-click the element, and click **Open Detail Page**.

     The **Detail** page is opened in a new browser window, and you can view the data for the selected object, including fields and any associations it has to other objects.
   - If the connections and nodes in the diagram represent a complex flow and you want to optimize the visualization, click **Auto Layout**.

     When **Auto Layout** is turned off, the objects and nodes are pinned to the canvas as you interact with the diagram. Existing nodes do not move as you add connecting links to the diagram. As a result, you might have complex routing that is difficult to understand. Click **Relayout Diagram**.  to automatically move objects and connecting links to show a less complex diagram.

If Relayout Diagram is the default setting, the diagram is recast to provide optimal visualization when you change the diagram.

- To show the diagram so that it is zoomed to fit entirely into your browser window, click **Fit to Window**  .

7. To remove an element from the diagram, right-click the element and click **Remove**.
8. To update the diagram with any objects that were added since the diagram was last saved, click **Refresh**  .

   Restriction: If you modified the diagram, and you do not complete the refresh step, and if there is a discrepancy between the current diagram and the diagram when it was last saved, you cannot save the changes until you resolve the conflict between the two versions.
9. Click **Save**.

   If the editor is in Read-only mode, you do not have permission to save the changes to your diagram.

Creating a process diagram

As a Risk Analyst, you can create the flow of a business process and key components by using a diagram to visualize the data.

Before you begin
You must have read, write, and associate access to the process diagram object and read and associate access to the parent process object to add a diagram.

About this task
You can show the directional flow of a process through a diagram by connecting the following elements:

- Subprocesses
- Input and output
- Decision node

The following figure shows how these elements are represented in the diagram legend.

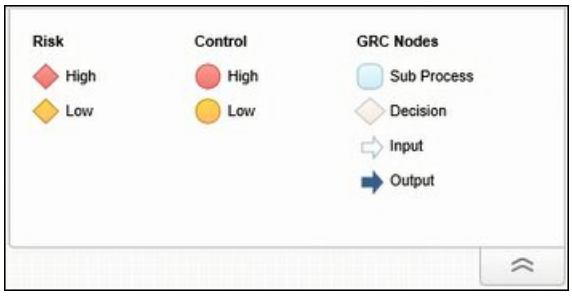


Figure 11: Process flow legend

You can create a process diagram as a child association of the selected Process. Because the process diagram is a child object of the Process, the diagram is displayed under **Associations** in the **Process Details** page.

You can apply labels to flows or directional links. However, flow data, such as reporting or logic, must be available to use in the diagram.

If you have permission to view the process, you have permission to view all of its subprocesses. Although you can view the object associations, you cannot create or change associations between subprocesses, risks, or controls.

Procedure

1. Click **Organization** > **Processes**.
2. Select the process for which you want to graphically show the flow.
3. On the **Detail** page, under **Associations**, click **Process Diagram**.

   The **Process Diagram** list page is displayed.
4. From the **Actions** menu, click **Add a new Process Diagram**.
5. In the **Name** and **Description** fields, enter information about the process diagram.
6. In the **Status** field, click **Draft**, and then click **Save**.

   The new process diagram is now available for selection for modifying. In the Process Diagram detail pane, the **Process Diagram link** field contains the URL to the process diagram.
7. In the Process Diagram detail pane, in the **Process Diagram link** field, click the link.

   When the Process Diagram canvas is opened, the IBM OpenPages GRC Platform objects that are available for your diagram, and to which you were granted access permission, are listed. Objects that were removed from the repository or data model are marked with an X. You cannot save diagrams that include objects that are marked for deletion.

   Tip: To view the legend, click the down arrow  .
8. To view more information about an object, complete one or more of the following actions:
   - To view the full label and description of an OpenPages GRC Platform object, right-click the object and click **Properties**.
   - To open the corresponding **Detail** page or **Activity View** for any subprocess, risk, control, input, or output node, right-click the element, and click **Open Detail Page**

     Note: The security privileges that are defined for your profile determine whether you are able to drill to the **Detail** page or Activity View.
9. To create the process flow, complete the following actions:
   - To connect objects, select the first object that you want, and press Ctrl and click the next object in the flow. When all the objects that you want are selected, right-click the selection, select **Add Link**, and select whether the flow of objects is to the left, right, top, or bottom of the first object.

     When the objects are selected, they are removed from the available list of objects.
   - To add a label for the connecting link between two objects, right-click the link, and select **Properties**. In the **Label** field, type the description for the connector, and click **OK**.
   - To add a decision node, right-click the object, select **Add Decision**, and select the direction in which you want to place it.

     Remember: To change the label for the Decision node, right-click the node and click **Properties**. In the **Label** field, and enter the condition that must be met at this stage of the flow.
   - To remove a connector or an object, right-click the element, and select **Delete**.

     Note: You cannot remove controls or risks that are associated with a subprocess element.
10. To manage the process flow for better viewing, choose how you want to optimize it:
    - If the connections and nodes in the diagram represent a complex flow, turn on Auto Layout by clicking **Auto Layout**.

      Tip: By default, **Auto Layout** is turned off. When **Auto Layout** is turned off, the objects and nodes are pinned to the canvas as you interact with the diagram. Existing nodes do not move as you add connecting links to the process flow. As a result, you might have complex routing that is difficult to

understand. You can click **Relayout Diagram**  to automatically move objects and connecting links to show a less complex diagram.

If Relayout Diagram is the default setting and you change the diagram, the diagram is changed to provide optimal visualization.

- To show the diagram so that it is zoomed to fit entirely into your browser window, click **Fit to Window**  .

11. To save the process diagram that is associated with the process, click **Save**.

Related concept

"Business process visualizations" on page 95

As a Risk analyst or Compliance manager, you can graphically render your business process and communicate it to other users of risk analysis. By visualizing the business process, which can include the subprocesses, activities, risks, and controls, you can speed the risk management process and data analysis.

Refreshing process diagrams

If the source data or objects that a process diagram is using change, you can refresh the diagram to ensure that you are working with the latest version of the objects or data.

When you refresh a process diagram, you are retrieving the latest changes and updates from the IBM OpenPages GRC Platform repository.

Procedure

1. Open a process diagram.
   a) Click **Organization** > **Processes**.
   b) Under the **Folder View**, expand the folders and select the parent process that contains the associated process diagram that you want to refresh.
   c) Under **Associations**, click **Process Diagrams**.

      The **Process Detail** page shows the process diagrams that are associated to the process object.
   d) Click the diagram that contains the process flow you that you want to update.
   e) In the field pane, in the **Process Diagram Link** property, click the **Process Diagram** link.

      The Process Diagram canvas is opened in a separate window.
2. To refresh the data, click **Refresh**  .

   If you did not save the diagram or chart, a warning asks if want to update the diagram or chart without saving the current flow.

Results

The refresh process manages the GRC objects in one or more of the following ways:

- If the GRC object is not in the current diagram, the object and the child objects are added.
- If the GRC object is in the current diagram but was deleted from the system, it is marked as deleted with a red symbol.
- If the GRC object in the current diagram was modified (for example, a change in name, description, or status), the GRC object data is updated.

A GRC object might not be available for use in the diagram because the object was deleted from the OpenPages GRC Platform system or you do not have Read access to the object.

Modifying a process diagram

As a Risk Analyst, you want to revise an existing process diagram because you want the diagram to reflect changes in the current process flow, subprocesses, risks, or controls.

Before you begin

To change an object, such as a Risk or Process or a Process Diagram object, you must have Write access. To view and add objects or nodes to the process diagram, you must have Read access to those objects.

In addition, administrators can use security rules to define a more granular control over access to individual objects in a folder.

About this task

You can create or delete the decision elements of the process diagram, but you cannot delete the subprocesses, input and output objects, and risks and controls. When you delete the subprocesses, input, and output elements from the diagram, they are returned to the selectable list of diagram objects for future use. Deleting these objects means that they are removed from the diagram and not from IBM OpenPages GRC Platform.

Procedure

1. Click **Organization** > **Processes**.
2. Under **Folder View**, expand the folder that contains the parent process that is associated with the process diagram that you want to revise.
3. Under **Associations**, click **Process Diagrams**.

   The **Process Detail** page shows the process diagrams that are associated to the process object.
4. Click the diagram that contains the process flow you that you want to change.

   The field pane is displayed after the list of diagrams.
5. In the field pane, in the **Process Diagram Link** property, click the **Process Diagram** link.

   When the Process Diagram canvas is opened, the OpenPages GRC Platform objects that are available for your diagram, and to which you were granted access permission, are listed. Objects that were removed from the repository or data model are marked with an X. You cannot save diagrams that include objects that are marked for deletion.

   Tip: To view the legend, click the down arrow  .

   If the editor is in Read-only mode, you do not have permission to save the changes to your diagram.
6. To refresh the data, click **Refresh**  .

   If you did not save the diagram or chart, a warning message asks if want to update the diagram or chart without saving the current flow.
7. Complete one or more of the following steps to change the process flow:
   - To view detailed information about an element, right-click the element and click **Properties**.
   - To open the corresponding **Detail** page or **Activity View** for any subprocess, risk, control, input, or output node, right-click the element, and click **Open Detail Page**.

     The **Detail** page is opened in a new browser window, and you can view the data for the selected object, including fields and any associations it has to other objects.
   - If the connections and nodes in the diagram represent a complex flow, and you want to optimize the visualization, turn on Auto Layout by clicking **Auto Layout**.

     Tip: When **Auto Layout** is turned off, the objects and nodes are pinned to the canvas as you interact with the diagram. Existing nodes do not move as you add connecting links to the diagram. As a

result, you might have complex routing that is difficult to understand. You can click **Relayout Diagram**  To automatically move objects and connecting links to show a less complex diagram.

If Relayout Diagram is the default setting and you change the diagram, the diagram is recast to provide optimal visualization.

- To show the diagram so that it is zoomed to fit entirely into your browser window, click **Fit to Window** 

8. To modify the process flow, complete the following actions:
   - To connect objects, select the first object that you want, press Ctrl, and click the next object in the flow. When all the objects that you want are selected, right-click the selection, select **Add Link**, and select whether the flow of objects is to the left, right, top, or bottom of the first object.

     When the objects are selected, they are removed from the available list of objects in the pane.
   - To add a label for the connecting line between two objects, right-click the link, and select **Properties**. In the **Label** field, type the description for the connector.
   - To add a decision node, right-click the object, click **Add Decision**, and then click the direction in which you want to place it.

     Remember: To change the label for the Decision node, right-click the node and click **Properties**. In the **Label** field, enter the condition that must be met at this stage of the flow.
   - To remove a connector or an object, right-click the element, and select **Delete**.

     Note: You cannot remove controls or risks that are associated with a subprocess element.
9. To save the process diagram that is associated with the process, click **Save**.

Copying a process diagram to use as a template

You can create a process diagram that is based on the process flow of an existing diagram. Instead of creating the structure of a process diagram from scratch, you can copy a diagram with a predefined process flow.

About this task

You cannot copy a process diagram to a different parent process. However, you can copy a diagram within the same process. When a parent process is copied from one business entity to another, the process diagram is included in the objects that are copied.

Procedure

1. Click **Organization** > **Processes**.
2. Select the process that contains the associated process diagram that you want to copy.
3. On the **Process Detail** page, under **Associations**, click **Process Diagrams**.

   The **Process Diagrams** list page is displayed.
4. From the **Actions** menu, click **Copy an existing Process Diagram**.

   The **Copy Process Diagrams - Select Process Diagrams** page is displayed.
5. On the **Folder View** tab, select the diagram whose process flow you want to copy, and click **Next**.
6. Under **Copy Options**, select whether you want to copy associated files or associated issues.
7. Under Resolving naming conflicts, choose how you want to copy and later identify the new process diagram.

- To create a new version of the diagram with the same name, select **Create a new version of the existing object in the destination directory**
- To create a new diagram by using the selected diagram as the template, select **Create new object whose name is prefixed with 'Copy of'**.
- To prevent the addition of process diagrams with similar names, select **Do not copy resources with naming conflicts**.

8. Click **Copy**.

Results
A copy of the process diagram is included in the list of diagrams on the **Process Detail** page.

Changing the status of a process diagram

The status of a process diagram indicates whether the design of the business flow is in progress or is in the approved state. By changing the status, the diagram author can explicitly show whether the diagram is available for use in the decision-making process.

Procedure

1. Click **Organization** > **Processes**.
2. Under **Folder View**, expand the folders to locate the process for which you want to change the status.
3. On the **Process Detail** page, under **Associations**, click **Process Diagrams**.
4. From the **Process Diagrams** detail page, under **Name**, click the process diagram whose status you want to change.
5. In the field pane, from the **Actions** menu, click **Edit this Process Diagram**.
6. In the **Status** field, select one of the following states for your diagram:
   - If work on the diagram is in progress, click **Draft**.
   - If the diagram is ready for approval, click **Published**.
   - If the diagram is out-of-date and no longer reflects your current process flow, click **Obsolete**.

   If the diagram has a status of **Obsolete**, it is not removed from the IBM OpenPages GRC Platform system. However, users cannot refer to it for decision making because it does not contain updated process flows for the Business Entity.
7. Click **Save**.

Deleting a process diagram

You can delete process diagrams that are obsolete or do not accurately reflect a process flow of the business entity.

About this task

When you delete a process diagram, all associated items are also deleted.

Only users with Delete permission can delete a process diagram.

Procedure

1. Click **Organization** > **Processes**.
2. Under the Folder View, expand the folders to locate the process diagram that you want to delete.
3. On the **Process Detail** page, under **Associations**, select **Process Diagrams**.
4. Under **Name**, select the check boxes next to the process diagrams that you want to delete.
5. From the **Actions** menu, click **Delete selected Process Diagrams**.

Modifying field properties of a process diagram

You can modify the properties of a process diagram when you want to change the name, description, or status of the diagram.

Procedure

1. Click **Organization** > **Processes**.
2. Under **Folder View**, expand the folders to go to the process for which you want to modify the details.
3. On the **Process Detail** page, under **Associations**, click **Process Diagrams**.
4. Under **Name**, click the process diagram whose details you want to change.
5. In the **Fields** pane, from the **Actions** menu, click **Edit this Process Diagram**.
6. Make the necessary modifications and click **Save**.

Exporting a process diagram from an OpenPages GRC Platform environment

Use the ObjectManager tool to export process diagram data from an IBM OpenPages GRC Platform environment. The export includes both child and parent hierarchies of a process.

Before you begin

You must know the full path of the process object, which is the parent of the process diagram that you want to export.

For example:

`/_op_sox/`*`Project`*`/Default/ICDocumentation/Processes/TopEntity/`*`Process_filename`*`.txt`

Before you modify the `ObjectManager.properties` file, make a backup copy of the file. When you are using the ObjectManager tool, ensure that the OpenPages GRC Platform services are running.

About this task

You can use ObjectManager settings to specify which process diagrams you want to export by defining the folder path of the parent process for the process diagram.

To control or limit the scope of exported data from the ObjectManager tool, you must first modify the `ObjectManager.properties` file, which contains configuration and migration settings.

Procedure

1. Verify that the OpenPages GRC Platform application is running.
2. On the source OpenPages GRC Platform system, in a text editor, open the `ObjectManager.properties` file and set the following properties where *full_path* is the full path of the process object that you want to use as the scope for the export:

   configuration.manager.dump.associated.resources.root.node.1=*full_path*

   Change the values of the parameters whose names begin with the pattern configuration.manager.dump.from `true` to `false`

   configuration.manager.dump.associated.resources=true

   Tip: The `ObjectManager.properties` file is in the *`root_installation_folder`*`/bin` directory where *root_installation_folder* is the folder of your OpenPages GRC Platform installation.
3. At the command line, go to the `bin` installation directory.
   For example, `cd C:\OpenPages\bin`
4. At the command line, type one of the following commands on a single line:

- On a computer that is running a Microsoft Windows operating system:

  `ObjectManager d c` *`Super_Administrator_Account Super_Administrator_Password OP_Home`*`\export` *`dump_file_name`*
- On a computer that is running an AIX or Linux operating system:

  `ObjectManager.sh d c` *`Super_Administrator_Account Super_Administrator_Password OP_Home`*`\export` *`dump_file_name`*

Two loader files are created in the *`OP_Home`*`\export` folder: *`loader_file_prefix`*`-op-config.xml` and *`loader_file_prefix`*`_op-file-content.zip` where *loader_file_prefix* is the *dump_file_name*.

These files contain the process hierarchy instance data, including the process diagram data.

What to do next

On the target OpenPages GRC Platform server, extract the files from the output file.

"Running ObjectManager commands" on page 590

"Modifying the ObjectManager properties file" on page 601

Importing a process diagram to an OpenPages GRC Platform environment

Use the ObjectManager tool to import process diagram data to an IBM OpenPages GRC Platform environment. You can use a loader file to import the instance data to the OpenPages GRC Platform repository on the target server.

Before you begin

When you are using the ObjectManager tool, ensure that the OpenPages GRC Platform services are running.

Procedure

1. On the target server, copy the two dump files that contain the process diagram and related data to an *extract_folder*.
2. In a text editor, open the `ObjectManager.properties` file and set the following property:

   configuration.manager.load.resource.ignore.undefined.property.value=`true`

   Tip: The `ObjectManager.properties` file is in the *`root_installation_folder`*`/bin` directory where *root_installation_folder* is the folder of your OpenPages GRC Platform installation.
3. At the command line, go to the `bin` installation directory.
   For example, `cd C:\OpenPages\bin`
4. At the command line, type one of the following ObjectManager commands on a single line:
   - On a computer that is running a Microsoft Windows operating system:

     `ObjectManager l c` *`Super_Administrator_Account Super_Administrator_Password extract_folder_name dump_file_name`*
   - On a computer that is running an AIX or Linux operating system:

     `ObjectManager.sh l c` *`Super_Administrator_Account Super_Administrator_Password extract_folder_name dump_file_name`*

Results

The following rules are observed when you import the process diagram objects:

- If the objects with matching data exist on the target environment, the objects are not overwritten.
- If the objects with different field values exist on the target environment, new versions of the objects are created with data from the import file.

- If the objects do not exist on the target environment, new objects are created and associations are defined.

Chapter 7. Managing reports

The IBM OpenPages GRC Platform 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.

Supplied reports

The OpenPages GRC Platform application comes with a selection of predefined and supplied reports that allow you to quickly view important information about your project.

Note: The list of reports in this documentation is for a fresh installation of the OpenPages GRC Platform application. If you have additional reports tailored to your particular business needs or have upgraded from an earlier version of the application, the classification of the supplied reports may differ from the classification documented here.

OpenPages GRC Platform V6 folder reports

The V6 folder in IBM OpenPages GRC Platform contains subfolders for the report types that are available. The All Documentation report resides at the top level of the reporting hierarchy.

Important: In reference to Reporting Framework V6, V6 refers to the latest framework version, not to any specific OpenPages GRC Platform release number.

Table 32: OpenPages GRC Platform V6 folder reports and folders

Report or folder name	Description
All Documentation report	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 subreports for each count.
Administrative Reports folder	Folder that contains predefined administrative reports such as a list of files that are checked out.
Audit Reports folder	Folder that contains predefined audit reports such as an audit summary.
Issue Reports folder	Folder that contains predefined reports on issues such as the issues and associated action items for a chosen reporting period and business entity.

Administrative Reports folder

OpenPages GRC Platform includes the following, predefined administrative reports:

Table 33: 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 checked out the File. • 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 subfolders:

- Configuration (see Table 36 on page 112)
- Security (see Table 37 on page 112)

Table 34: Audit Reports folder	
Report Name	**Description**
Audit Change	Lists all object changes that fulfill the user's runtime 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" on page 110.
Audit Summary	Administrative summary of changes to documentation data, which is filtered by date and time range. You can also filter by Business Entity and object type and drill into a detailed Audit subreport.

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 identifies change events for any field value change.

Notice: This information also applies to the detail subreport from the Audit Summary report.

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

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

Any one parent object (such as a Risk) might have multiple child objects (such as Controls). However, the system allows only one of the object parent-child relationships to be marked as "Primary". Primary associations are used to determine the path that the system should follow when you are executing a number of operations that require object hierarchy traversal.

In the OpenPages GRC Platform 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

Audit Trail Reports are "parent object centric" when the report captures events that pertain to an object associations. For an object, all association-related events are defined as 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 35 on page 111 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 35: 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.
Added	Object	A new object was created in the repository.
Added	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.
Removed	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 is set to Primary. This first association is always set to Primary

Table 36: Audit Reports Configuration subfolder	
Report Name	**Description**
Configuration Audit	Lists all configuration changes made to the OpenPages GRC Platform application during the chosen date range.

Table 37: Audit Reports Security subfolder	
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 accessed the OpenPages GRC Platform system during the 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 or log out), login status (Failed or Succeeded), and number of login attempts.
Roles by Security Domain	Lists each role that is 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

The following table identifies the Issue reports available in the Issue Reports folder:

Table 38: Issue Reports	
Report Name	**Description**
Issue List	Detailed listing of Issues and associated parent objects, which are 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 that are associated with Controls that are indirectly associated with a Risk Assessment will not appear. Issues associated with Risks that are directly associated in a chain, from Business Entity to Process or Subprocess to Control Objective, appear.

Table 38: Issue Reports (continued)	
Report Name	**Description**
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.

Accessing reports from the application user interface

You can access reports from the IBM OpenPages GRC Platform application user interface.

They are typically found in the `/openpages` folder.

Procedure

1. From a browser window, log on to OpenPages GRC Platform.
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.

Adding reports

To run a report from the IBM OpenPages GRC Platform user interface, the report must have a corresponding report page published to the OpenPages GRC Platform server.

A report page does the following:

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

All Studio report pages are based on the `Cognos Report Redirect` page template, and all Cognos Workspace report pages are based on the `Cognos Dashboard Redirect` page template. Additionally, all Cognos Analytics dashboard and story pages are based on the Cognos Analytics Dashboard Redirect page template. These templates are located at the root of the Reporting publishing channel on the OpenPages GRC Platform server.

You can use one of the following methods to add new reports to the OpenPages GRC Platform 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.
- OpenPages GRC Platform server administrator interface - this method involves using the publishing channels facility on the OpenPages GRC Platform server to manually create the required report page and publish the report. This method is typically used for editing report pages and troubleshooting publishing issues.

Regardless of the method you use to add the report, be sure to save it in a folder, for example, `0penPages V6`. Do not save the report in the OPENPAGES_REPORTS_V6 reporting package. OPENPAGES_REPORTS_V6 is the reporting framework that is used for authoring reports.

Using the application user interface to add reports

You can add a report from the IBM OpenPages GRC Platform user interface.

When you add a report, the following process occurs:

- A corresponding report page is automatically generated on the OpenPages GRC Platform server that is 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 281.

Before you begin

Before you can add a Cognos report from the OpenPages GRC Platform application user interface, you must have details about the report available.

- The name of the report. Do not enter special characters, including the underscore, in the report name.
- A description of the report
- The path and name of the folder to be deployed (the folder selection is filtered to list report folders only). By default, the path is `/_cw_channels/Reporting/S0X`.

Example

A new unpublished report was created called "My Control Summary" in the `OPENPAGES_SHARED` folder on the Cognos server. Publish the report to make it available for users in the US English and Japanese locales.

From the **Reports** page in the OpenPages GRC Platform application, you click **Add** and select the report from the listing. For the US English locale (this locale is automatically selected by default), 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`.

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

Attention: To view the new report on the Reports menu, users must log out and log back in to the application.

Report publishing limitations
Publishing report pages from the application user interface has some 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 IBM OpenPages GRC Platform server (for details, see "Modifying a report template" on page 120).
- 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 GRC Platform server to add that report (for details, see "Manually creating an instance of a report" on page 117).

Accessing the publish report page
To access the **Add** icon on the Reports page, you must have the **Add Pages** application permission set on your account.

For details, see "Types of application permissions" on page 32.

Procedure

1. From a browser window, log on to the OpenPages GRC Platform 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 report from the application user interface
The Report selection list contains all available reports that are not already published.

Procedure

1. Access the **Publish Report** page (see "Accessing the publish report page" on page 115).
2. Select a report from the Report 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 My Work 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.

Modifying the displayed report name or description
You can localize and modify the name and description that is displayed to users on the IBM OpenPages GRC Platform 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 "Modifying display text in the application user interface" on page 282.

Installing the Java applet to work with reports

Before working with reports, you must have access to the IBM OpenPages GRC Platform server administrator interface.

Before you begin

The applet in OpenPages GRC Platform server (typically `/opx`) requires that the Java Runtime Environment 7 is installed on the client where you launch Internet Explorer.

Procedure

1. Ensure 32-bit Java 8 is installed and launch Internet Explorer.
2. When you navigate to pages in OpenPages GRC Platform server that require the Java applet, a message is displayed requesting that the applet be run. Complete the following steps to run the applet:
   a) Click **Run**.
   b) If Java is not installed on the client, when you navigate to pages in OpenPages GRC Platform that require the Java applet, you are prompted to install Java Runtime Environment 7 Update 60. Click **Install**.

      Note: Internet Explorer Enhanced Security Configuration must be disabled 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 Cognos 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 GRC Platform application to create multiple reports based on the same layout and internal logic. Each report page represents a report as viewed in OpenPages GRC Platform.

Report pages and page templates reside on the OpenPages GRC Platform server.

Note:

- Cognos 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 “Adding reports” on page 113.
- 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 Cognos report pages are based on the `Cognos 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 JavaServer Pages (JSP) reports, are located in the IBM OpenPages GRC Platform repository on the OpenPages GRC Platform server.

The OpenPages repository handles the data storage and access capabilities for the OpenPages GRC Platform application. To create, modify, or delete OpenPages reports, you must have an OpenPages GRC Platform account with permission to modify publishing channels. If you are not sure whether you have access to this functionality, contact your OpenPages administrator for additional information.

Accessing report pages and page templates

You can access report pages and page templates for JSP reports.

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

Before you begin

The administrator should be a member of the **OPAdministrators** group to access report pages and page templates. If you are not a member of this group, you will receive the following message:

```
You do not have permission to view this file.
```

Procedure

1. From a browser window, log on to the IBM OpenPages GRC Platform server (typically `/opx`) as a user with the correct Reporting permissions).
2. Click the **Browse channels** link under the **Publishing** heading in the 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 OpenPages GRC Platform 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 OpenPages GRC Platform report.

Manually creating an instance of a report

To manually create an instance of a report, you must log on to the IBM OpenPages GRC Platform server, and create a report page based on a copy of an existing page template.

The new report page will display clickable links in the OpenPages GRC Platform user interface for running the new report.

Note:

- Cognos 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 “Adding reports” on page 113.
- 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 Cognos report pages are based on the `Cognos Report Redirect` page template, which is located at the root of the Reporting publishing channel on the IBM OpenPages server.

Identifying the page template

You can determine which existing report page you want to copy from or use as the basis of a new report page.

Procedure

1. From a browser window, log on to the IBM OpenPages GRC Platform 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 OpenPages GRC Platform 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.

Creating a report page

To create a new report, you must log on to the IBM OpenPages GRC Platform server, and create a new report page based on a copy of an existing page template.

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 Cognos report in the U.S. English locale would be placed in the `Reporting/S0X/OpenPages V6` folder.

   Optionally, create a category folder for grouping the reports under the appropriate `/S0X` folder. For example, to create a new report grouping titled "My Custom Reports" on the Reporting menu and Reports page in the OpenPages GRC Platform application for the U.S. English locale, you could create a folder with the path `Reporting/S0X/My Custom Reports`. Any report pages placed in the folder will appear under that grouping in the reporting sections of the OpenPages GRC Platform application.
3. Click the **Add Page** icon.
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.

   For reports from IBM Cognos Analysis Studio, IBM Cognos Query Studio, or Cognos Analytics - Reporting, or IBM Cognos Workspace, use the `CommandCenter Report Redirect` page template.

   c) Click **Next**.
5. If this is a JSP report, skip to Step 7. Otherwise, for a Cognos 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 39: Cognos Report Redirect Selection Fields	
Field Name	**Description**
Report Type	The IBM Cognos Studio application used to develop the report. Valid values are: • `report` (for Cognos Analytics - Reporting, this is the default value) • `query` (for Cognos Query Studio) • `analysis` (for Cognos Analysis Studio) • `pagelet` (for Cognos Workspace, 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. • `ReportStudio` - opens the report in Cognos Analytics - Reporting so it can be modified. • `QueryStudio` - opens the report in Cognos Query Studio so it can be modified. • `AnalysisStudio` - opens the report in Cognos Analysis Studio so it can be modified. • `CognosWorkspace` - enables the report to be opened in Cognos Workspace.
Report Format	The display format for the report. Valid values are: • `HTML` (This is the default value. This value is required for Cognos Workspace reports.) • `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.
Report Folder	The report folders must be syntactically correct and separated by forward slashes. The `Team content` folder is assumed, and does not need to be included in the **Report Folder** field. For example, the report folder could be `Vision 2013/Workspaces`.
Report Name	The report name must be the name that you want to appear in Cognos Analytics.

b) Skip to Step 8.

6. For a report 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 Cognos Workspace 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 40: 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 "The Custom folder" on page 286.

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 OpenPages GRC Platform application user interface, the new report should be visible in the selections on the Reporting menu and on the Reports page.

Modifying a report template

You can modify 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 S0X 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 GRC Platform application.

Procedure

1. From a browser window, log on to the OpenPages GRC Platform server (typically /opx) as a user with the correct Reporting permissions.
2. Click the **Browse Channels** link under the **Publishing** heading in the 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...** icon before 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 misnamed 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 "The Custom folder" on page 286.

6. When finished, click **Save**. The modified information is saved and immediately applied to the dashboard or story.

Deleting a report

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

Procedure

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

   Attention: Do not delete a page template. If a page template is deleted, all report pages based on that template are deleted as well.
4. Click **Delete** at the top of the table.
5. Click **OK** to delete the report page (or JSP report instance).

Manually creating an instance of a Cognos dashboard or story

To manually create an instance of a Cognos dashboard or story, you must log on to the IBM OpenPages GRC Platform server, and create a dashboard or story page based on a copy of an existing page template.

The new dashboard or story page will display clickable links in the OpenPages GRC Platform user interface for running the new dashboard or story.

Note:

- Dashboards and stories 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 Cognos dashboard and story pages are based on the `Cognos Analytics Dashboard Redirect` page template, which is located at the root of the Reporting publishing channel on the IBM OpenPages server.

Identifying the dashboard or story page template

You can determine which existing dashboard or story page you want to copy from or use as the basis of a new dashboard or story page.

Procedure

1. From a browser window, log on to the IBM OpenPages GRC Platform 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 dashboard or story page you want to copy from or use as the basis of the new dashboard or story 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 OpenPages GRC Platform Cognos dashboard or story you want to copy or use and modify as the basis of a new dashboard or story.

c) Click the name of the dashboard or story page to open its detail page.

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

Creating a dashboard or story page

To create a new dashboard or story, you must log on to the IBM OpenPages GRC Platform server, and create a new dashboard or story page based on a copy of an existing page template.

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 dashboard or story page to be created.

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

   Optionally, create a category folder for grouping the dashboards or stories under the appropriate `/SOX` folder. For example, to create a new dashboard grouping titled "My Custom Cognos Dashboards" on the Reporting menu in the OpenPages GRC Platform application for the U.S. English locale, you could create a folder with the path `Reporting/SOX/My Custom Cognos Dashboards`. Any dashboard pages placed in the folder will appear under that grouping in the reporting sections of the OpenPages GRC Platform application.
3. Click the **Add Page** icon.
4. In the **Describe page** step of the **Add a Page** wizard, do the following:
   a) Type an informative name and description for the dashboard or story.

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

   b) Choose the page template you will use to create the dashboard or story.

      Cognos dashboards and stories use the `Cognos Analytics Dashboard Redirect` page template.

   c) Click **Next**.
5. In the **Specify page contents** step in the **Add a Page** wizard, select a value for each of the following fields:

Table 41: `Cognos Analytics Dashboard Redirect` Selection Fields

Field Name	Description
Action	Select the method for opening the dashboard or story. Valid values are: • view (opens the dashboard or story in view-only mode, this is the default value) • edit (opens the dashboard or story in Cognos Workspace so it can be modified)
Mode	Select the page mode. Valid values are: • `dashboard` • `story`

Table 41: Cognos Analytics Dashboard Redirect Selection Fields (continued)	
Field Name	**Description**
Dashboard (or) Story Folder	The dashboard or story folders must be syntactically correct and separated by forward slashes. The `Team content` folder is assumed, and does not need to be included in the **Dashboard (or) Story Folder** field.
Dashboard (or) Story Name	The dashboard or story name must be the name that you want to appear in Cognos Analytics.

6. Enter values in the following key fields:

Table 42: Cognos Analytics Dashboard Redirect Key Fields		
Key Field	**Format**	**Description**
Dashboard (or) Story Name Key	dashboard.name.<user-defined> story.name.<user-defined> Examples: dashboard.name.control.analysis story.name.control.analysis	A key that references an application text string for localizing the title of the dashboard or story.
Dashboard (or) Story Description Key	dashboard.description.<user-defined> story.description.<user-defined> Examples: dashboard.description.control.analysis story.description.control.analysis	A key that references an application text string for localizing a description of the dashboard or story.

Note: You can use the values in the **Dashboard (or) Story Name Key** and **Dashboard (or) Story Description Key** fields on the dashboard or story page to manually create custom application text keys to localize the name and description of a dashboard or story after it is created. For details, see "The Custom folder" on page 286.

7. Click **Apply** to save the modifications.
8. Click **Finish** to create the new dashboard or story page and exit the wizard.

Results

When you log on to the OpenPages GRC Platform application user interface, the new dashboard or story should be visible in the selections on the Reporting menu.

Modifying a dashboard or story template

You can modify an existing dashboard or story template.

Important: If you want to modify the supplied dashboard and story template for your own purposes, you must copy it to a new location outside the S0X 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 GRC Platform application.

Procedure

1. From a browser window, log on to the OpenPages GRC Platform server (typically /opx) as a user with the correct Reporting permissions.

2. Click the **Browse Channels** link under the **Publishing** heading in the navigation Action menu.
3. Navigate to the dashboard or story that you want to modify and click the dashboard or story name to display the detail page.
4. Find the section containing the information you want to change, and click the **Edit...** icon before the section. An editable version of the information is displayed.
5. Change the desired settings.

   Note: You cannot modify the name of a dashboard or story. In order to change the name of a dashboard or story, you must delete the misnamed dashboard or story and create an identical dashboard or story with the new name.

   As an alternative, you can use the values in the **Dashboard (or) Story Name Key** and **Dashboard (or) Story Description Key** fields on the dashboard or story page to manually create custom application text keys to localize the name and description of a dashboard or story after it is created. For details, see "The Custom folder" on page 286.
6. When finished, click **Save**. The modified information is saved and immediately applied to the report.

Deleting a dashboard or story

You can delete an instance of a dashboard or story page for a Cognos dashboard or story.

Procedure

1. From a browser window, log on to the IBM OpenPages GRC Platform server (typically /opx) as a user with the correct Reporting permissions.
2. Click the **Browse Channels** link under the **Publishing** heading in the navigation Action menu.
3. Navigate to the dashboard or story page to delete and select the dashboard or story name.

   Attention: Do not delete a page template. If a page template is deleted, all dashboard or story pages based on that template are deleted as well.
4. Click **Delete** at the top of the table.
5. Click **OK** to delete the dashboard or story page.

Creating an interactive JSP report

The IBM OpenPages GRC Platform application allows administrative-level users with the option to create interactive reports to prompt a user at run-time for parameter values. You can either modify an existing JSP report to be interactive, or specify an interactive parameter during report creation.

Procedure

1. From a browser window, log on to the OpenPages GRC Platform server (typically /opx) as a user with the correct Reporting permissions.
2. Click the **Browse channels** link in the 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...** icon before 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.
6. Select the check box marked "Interactive Value" and click the **Apply** icon.
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 defined as an interactive parameter that requires a user to provide information at run time, IBM OpenPages 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. However, the value for these fields must be entered manually, using 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

The IBM OpenPages GRC Platform application allows administrative-level users with the option to create interactive reports to prompt a user at run-time for parameter values.

Note: Although any parameter type can be defined as an interactive parameter that requires a user to provide information at run time, IBM OpenPages 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. However, the value for these fields must be entered manually, using 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 OpenPages GRC Platform (such as `/openpages`).
2. Select **Reporting** on the menu bar, and select the name of the report you want to run. If the report contains interactive parameters, a prompt page is displayed.
3. Type information into the required fields.
4. Click **Next** 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 GRC Platform server interface and in the Cognos Analytics portal.

Note: If you restrict access to reports only through the Cognos Analytics portal, but not in the OpenPages GRC Platform server interface, the reports may be displayed in a selection list to users in the OpenPages

GRC Platform 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 JSP and reports

You can restrict users and or groups from accessing and running JSP reports from the OpenPages GRC Platform 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 >> Cognos folder). After you grant access to administrative reports for the System Administrators group, you can 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 OpenPages GRC Platform server (typically /opx) as a user with administrative privileges.
2. Click the **Browse channels** link under the **Publishing** heading in the 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 /S0X folder you want.

   Note:

   - Each folder represents a report grouping in the OpenPages GRC Platform user interface.
   - Reports that are under the Reporting/S0X folder structure are published to the U.S. English locale. To select a different locale, choose the /S0X folder under the locale you want (for example, ja_JP/S0X for the Japanese locale).
5. Under the selected /S0X 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 OpenPages GRC Platform application user interface.
   b) Click **Properties** to open the **Folder Details** page.
6. In the **Access Controls** pane, select **Add** from the **Actions** menu.
   a) Select a group or user to whom you want to grant permission.
   b) Select the permissions you want to allow or deny the group or user (Read, Write, Delete, Manage).
   c) Click **Add**. The selected group or user appears in the list.
   d) To select another group or user, repeat Steps a-c.
   e) To remove a group or user, select the group or user then select **Remove** from the **Actions** menu.
7. Break inheritance on the folder so other groups or users cannot access these reports from the OpenPages GRC Platform 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.

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

Securing access to the report portal

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

Note: This task is optional.

Use the following tasks 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 Cognos Analytics portal:

Note: IBM OpenPages GRC Platform standard reports could be overwritten during an upgrade. If you want to modify the standard reports, it is best that you copy the reports to your own folder structure where you can then modify and control access to these reports.

Assigning CommandCenter administrative rights to a group

Before you can specify access rights and restrictions to reports and reporting functions, you must assign CommandCenter administrative rights to a new or existing group.

Procedure

1. From a browser window, log on to the IBM OpenPages GRC Platform application as a user with administrative privileges.
2. Create a group in 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 GRC Administrator's Guide*.

Specifying user access to administrative functions in the Cognos Analytics portal

You can specify which users have access to administrative functions within the Cognos Analytics portal.

Procedure

1. From a browser, log on to the Cognos Analytics portal as a user with administrative privileges, for example, OpenPagesAdministrator.

   By default, the URL is:

   `http://<hostname>/ibmcognos/bi` (if you are using port 80 for Cognos)

   Where `<hostname>` is the name of the Cognos server.
2. Click **Manage** > **Administration Console** to launch the **IBM Cognos Administration** page.
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 IBM OpenPages GRC Platform group or role to access CommandCenter administrative functions.
   b) Select a group. For example, OPAdministrators.
   c) Click the green arrow to add the role.
8. On the **Members** tab of the **Set Properties** page,restrict access to the administrative functions.
   a) Select the Everyone group.
   b) Click the **Remove** link.

Restricting access to reports in Team content folder

You can restrict users to only being able to access reports that are in the **Team content** folder.

Procedure

1. On the Cognos Analytics page, click the **Team content** folder.
2. On the **Team content** page, click the **More** link in the same row as the IBM OpenPages GRC Platform folder for which you want to restrict access (for example, OPENPAGES_REPORTS_V6 or FCM_REPORTS).
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 end 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.
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.

   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 or FCM_REPORTS package, an error message is displayed to the user.

Restricting users to only running reports

You can restrict users to only run reports, with no access to Cognos Analytics - Reporting to modify reports.

Procedure

1. From a browser, log on to the Cognos Analytics portal as a user with administrative privileges, for example, OpenPagesAdministrator.

   By default, the URL is:

   `http://<hostname>/ibmcognos/bi` (if you are using port 80 for Cognos)

   Where `<hostname>` is the name of the Cognos server.
2. Click **Manage** > **Administration Console** to launch the **IBM Cognos Administration** page.
3. Select the **Security** tab, and click the **Cognos** link in the **Directory** list.
4. On the **Directory > Cognos** page, click the **More** link in the same row as the "Authors" role.
5. On the **Perform an action** page, under **Available Actions**, 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.
   b) Select the group you want (for example, OPAdministrators).
   c) Click the green arrow to add the group and then click **OK**.
8. On the **Members** tab of the **Set Properties** page:
   a) Select the **Everyone** group
   b) Click **Remove**.
9. Repeat Steps 2 - 6 for the "Query User" role.
10. When finished, return to the **IBM Cognos Administration** page and select the **Security** tab.

11. 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**.
12. 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".
13. In the list on the **Permissions** tab, select the "Everyone" group and grant the group Execute and Traverse permissions.

    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. Select the "Everyone" group and grant the group Execute and Traverse permissions.
14. 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**.
15. 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.

Results

After completing this procedure, the user cannot modify reports but can still run out-of-the-box reports.

Chapter 8. System file management

The ability to manage system folders and files is essential for information management in IBM OpenPages GRC Platform.

Overview of folders and files

The system folders and files can be found in the following location: **Administration** > **Manage System Files**.

The **Manage System Files** area of OpenPages contains seven types of system files. Six types are unique system file types, but the seventh type, SOXDocument, can be either system files or non-system files. Administrators go to **Administration** > **Manage System Files** > **Files** to access SOXDocument system files. Users go to **My OpenPages** > **Files** to access SOXDocument non-system files.

Using the **Manage System Files** area of OpenPages you can complete the following tasks:

- View folders and files
- Manage folders and files
- Search for files

Access to the Administration > Manage System Files menu item

Add the ready-to-use OpenPages Platform 3 profile to the list of available profiles for your administrators who manage system files. Using this profile, you have access to the **Administration** > **Manage System Files** menu item and the Detail, Folder, and Filter list views for the object types for system files. If you do not use the OpenPages Platform 3 profile, you can add the system file object types to any other profiles that administrators use. Users must be members of the OPAdministrators user group for the **Administration** > **Manage System Files** menu item to display.

System file types

When you click **Administration** > **Manage System Files**, you can access the following content file types:

Table 43: System file types

Content file type	**Description and examples**
Files (SOXDocument)	System files • `DefaultTemplate.xls`
SysXMLDocument	End user application configuration JSON and trigger configuration files • `deck_config.json` • `_trigger_config.xml` • `openpages-solutions.xml` • `OPLC-QuestionnaireAssessment.xml` • `lossevent_config.json`
ExporterXML	Notification reports

Table 43: System file types (continued)	
Content file type	**Description and examples**
MigrationJAR	JAR files that are imported by using **Administration** > **Import Configuration** and exported by using **Administration** > **Export Configuration** • `Migration Documents` folder • `imported-migration-121117082838.jar`
ModelConnectionConfig	Visual diagram files
Report	JSP files, for example, solution helpers, Command Center redirects, FastMap reports, and more • `ORM_Custom_Scope_Wizard.jsp`
VizConfig	Visualization configuration files • `EntityDetail.json` • `EntityHierarchy.json` • `ProcessFlow.json`

Comparison of OPX administrative interface to Manage System Files

Reports permissions are still managed in the OPX administrative interface. They are not available in **Administration** > **Manage System Files**.

In the OPX administrative interface, the SOXDocument system and non-system files are in the same location. But in OpenPages, SOXDocument system files are accessed in **Administration** > **Manage System Files** > **Files**. SOXDocument non-system files are accessed in **My OpenPages** > **Files**.

If you are familiar with how files and folders were organized in the OPX administrative interface, the following table explains where you can find the most commonly used system files in **Administration** > **Manage System Files**:

Table 44: Comparison of OPX to Manage System Files	
These files in OPX...	**Are located in ...**
Trigger configuration files	**Administration** > **Manage System Files** > **SysXMLDocument**
End user application configuration files	**Administration** > **Manage System Files** > **SysXMLDocument**
FLV export spreadsheet template files	**Administration** > **Manage System Files** > **Files**

Access permissions

Not all folders and files are accessible to all users. Each folder and file can have its own set of access permissions that determine which users are allowed to view or edit it. Sensitive or private information remains visible only to selected users, most often to prevent accidental editing or deletion.

Each user can view only the folders and files to which they have access permissions. Each user's view of the file system can appear differently, although all users are typically working from the same set of data. For example, one user can have access to all folders and files and be able to see all files in the system. Another user can have access to only a limited set of folders and files, which makes the folders and files to which they do not have access uneditable.

Note: The creator of a file is automatically granted all access permissions to that file, regardless of the limitations set by a group or the folder where the file is located.

The OpenPages Platform 3 profile includes access to all of the system file types. An administrator assigned this profile has access to all the system files and folders.

Object types and Folder Views

The content file types are defined as the following seven object types in OpenPages:

- Files (SOXDocument)
- SysXMLDocument
- ExporterXML
- MigrationJAR
- ModelConnectionConfig
- Report
- VizConfig

You manage these object types like other object types in the system. Do not disable the Folder View for these object types.

Known issues

The following behaviors are known issues in **Administration** > **Manage System Files**:

- If you set up filters for SysXMLdocument files for the Analytics bar, the filter correctly displays the results but incorrectly calculates as zero the number of results available.
- In Folder View only system files under the current reporting period are displayed. If you click a system file folder and select a finalized reporting period, no files in the folder are displayed and an error is shown.
- In Detail View for a system file, you can choose only **Current** in **Reporting Period**. You cannot choose a finalized reporting period.
- If you apply a filter in **Administration** > **Manage System Files**, the filter is not automatically applied in **My OpenPages** > **Files**, and vice versa.
- You must disable System Administration Mode to add new system files.

System file management tasks

To enable you to manage your content effectively, changes often have to be made to your folder and file structure, including changing file locations, changing file and folder names, and removing unwanted content from IBM OpenPages GRC Platform.

CAUTION: System files must have specific names and be in specific folders so use caution when moving, deleting, or renaming these types of files or their folders.

Creating folders

In IBM OpenPages GRC Platform, you can create a new folder within any folder for which you have access permissions.

Procedure

1. Go to **Administration** > **Manage System Files**.
2. Select the system file type.
3. Select the check box next to the folder that you want to add the new folder to.
4. Click **Add Folder**.

5. Type a name and description for the folder.
6. Click **OK**.

Uploading files

You can add files to folders in IBM OpenPages GRC Platform.

Procedure

1. Go to **Administration** > **Manage System Files**.
2. Select the system file type.
3. Select the check box next to the folder that you want to upload the file to.
4. Click **Add New**.
5. Click **Choose File** and select the file that you want to upload.
6. Type a description for the file.
7. Click **Create**.

Moving files or folders

IBM OpenPages GRC Platform enables you to move files or folders from one location in the folder hierarchy to another.

About this task

If you attempt to move a file into a folder that already contains a file with the same name, the file will not be moved. If you paste the file into a folder that does not already contain a file with the same name, then the original file name will be used.

CAUTION: Because some files are referenced by other system processes, and because other users may be working with common files, please ensure that you are not going to inadvertently disrupt the work or files of others before moving a file.

Procedure

1. Go to **Administration** > **Manage System Files**.
2. Select the system file type.
3. Select the check box next to the file or folder that you want to move.
4. Click **Move To**.
5. Navigate to the folder that you want to move the file to.
6. Click **OK**.

Copying files and folders

You can copy files and folders to a different folder in IBM OpenPages GRC Platform.

Procedure

1. Go to **Administration** > **Manage System Files**.
2. Select the system file type.
3. Select the check box next to the file or folder that you want to copy.
4. Click **Copy To**.
5. Navigate to the folder that you want to move the file to.
6. Click **OK**.

Renaming files or folders

IBM OpenPages GRC Platform enables you to rename folders and files in the system. You can only rename a folder or file if you have the correct permissions to do so.

Procedure

1. Go to **Administration** > **Manage System Files**.
2. Select the system file type.
3. Select the check box next to the file or folder that you want to rename.
4. Click **Rename**.
5. Type a new name and click **OK**.

Deleting files or folders

When you delete a folder, the folder and all of its contents are removed from IBM OpenPages GRC Platform. When you delete a file, it is removed from OpenPages. You can only delete a folder or file if you have the appropriate access permissions.

About this task

CAUTION: Because some folders and files are referenced by other system processes, and because other users may be working with shared files, please ensure that you are not going to inadvertently disrupt the work of others before deleting content.

Procedure

1. Go to **Administration** > **Manage System Files**.
2. Select the system file type.
3. Select the check box next to the file or folder that you want to rename.
4. Click **Delete**.

System file modification

You can download a copy of a file to view if you have view permissions for the file or you can edit a file by checking it out of IBM OpenPages GRC Platform.

When you check in an updated file, the original file is updated in OpenPages with the newer edited version. If file versioning is enabled, then older versions of files are maintained as you make edits. The most recently checked in version of a file is considered as the current version.

Downloading files

You can view a file stored in IBM OpenPages GRC Platform by downloading it to your computer.

Procedure

1. Go to **Administration** > **Manage System Files**.
2. Select the system file type.
3. Navigate to the file that you want to download.
4. Click the file.
5. In the **Name** field, click **View file**.

   The file is downloaded to your computer.

Checking out files

You can edit a file by checking it out of IBM OpenPages GRC Platform.

About this task

While a file is checked out, it is locked in OpenPages, thereby preventing any other user from making changes while you have the file checked out.

Procedure

1. Go to **Administration** > **Manage System Files**.
2. Select the system file type.
3. Navigate to the file that you want to check out.
4. Click the file.
5. From the **Actions** drop-down menu, select **Check out this <type of system file>**.

   The file is now locked.
6. In the **Name** field, click **View file**.

   The file is downloaded to your computer and available for edit.

Uploading modified files

After you have made changes to a checked out file, you must upload the revised file to IBM OpenPages GRC Platform.

Procedure

1. Go to **Administration** > **Manage System Files**.
2. Select the system file type.
3. Navigate to the file that you want to upload the newest version of.
4. Click the file.
5. From the **Actions** drop-down menu, select **Edit/Upload this <type of system file>**.
6. Click **Choose File** and select the new version of the file.
7. Click **Save**.

Checking in files

After you have edited and uploaded a file you can check it back in to IBM OpenPages GRC Platform.

About this task

When you check a file back in, it becomes unlocked, and may then be edited by other users.

Procedure

1. Go to **Administration** > **Manage System Files**.
2. Select the system file type.
3. Navigate to the file that you want to check back in.
4. Click the file.
5. From the **Actions** drop-down menu, select **Check in this <type of system file>**.

   The file is now unlocked.

Chapter 9. Fields and field groups

A field group is a container for fields. Each field must belong to a field group.

You can add new fields to object types and custom forms, and manage existing fields.

If a field is defined as a simple string or long string data type, you can also encrypt the field values in the IBM OpenPages GRC Platform repository.

To manage new fields, either add new fields to an existing field group or create a new field group and add the fields to it.

A field group is identified by the **Field Group** icon . An object field is identified by the **Object Field** icon .

Definition of fields

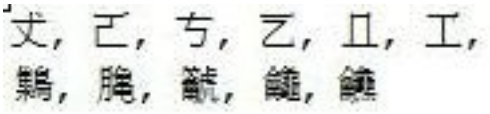
An object field represents information that is specific to an object type.

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

By default, each object type has a predefined field group that contains fields that are specific for that object type. For example, the "Effectiveness Rating" and "Operating Effectiveness" fields belong to the Control object field group called `OPSS-Control`.

Fields are added to a new or existing field group. It is then associated with a profile for display in 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 are new or existing field groups. For more information, see “Adding an object type for a custom form” on page 188.

Important: Do not use the four-byte characters 

that are defined in the CJK Unified Ideographs EXTENSION-B Unicode Block Name in field values. These characters will not be saved.

Definition of a field group that is in use

When a field group is associated with an object type, an instance of the object type is created. The field group is identified as in use.

When a field group is in use, you cannot delete the field group or any fields from that field group.

For example, you create a new field group that is 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 new fields on any Risk object view page, the Extra Fields field group is in use and cannot be deleted.

Note: If a management operation is being modified by two administrators at the same time, an error message is displayed, notifying you to try again later.

Field and field group process overview

You can add new fields to an object type and then display the new fields.

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

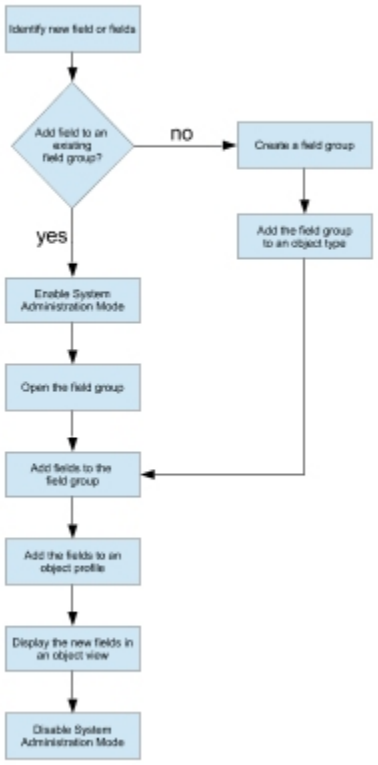


Figure 12: Tasks for configuring new fields

Table 45 on page 138 provides information about the configuration tasks.

Table 45: Tasks for configuring new fields

Task Description	**Related Topic**
1. Identify the new field.	See "Requirements for new fields" on page 139 for the information to identify before you create a new field.
2. Add a new field group or identify the existing group where the field is associated.	See "Adding field groups" on page 142 for instructions on how to create a new field group.
3. Add field definitions to the field group.	See "Adding fields to a field group" on page 142 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 177 for information about how to add the new field group to an object type or custom form object type.
5. Display the new fields in an object view.	See "Configure views for objects" on page 236 for information on displaying the new fields in a selected view and configuring a display type.

Requirements for new fields

Before you create a new field, determine the characteristics of the field and the object types that will use the new field.

The following list identifies information that is needed before you create a new field:

- Object - Will the new field be added to a custom form or object? For objects, identify the object types where the new field will be added.
- Name - How will the new field be identified? The name is important because it is also the label that appears next to the field. Special characters cannot be used. For additional information, see “File naming guidelines” on page 140.
- Label - What text is displayed when this field appears on an object View page? The initial label 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 is also displayed on the Add and Edit pages. If required, modify the label text. For more information, see Chapter 13, “Localizing text,” on page 277).
- Data type - What is the type of data, such as Boolean or Date that is captured by the field? For more information, see “Data types” on page 143.
- Entry type - Is the user required to enter data in the field or is data entry optional? For more information, see “Making fields required or optional” on page 151.
- Default value - Is a default value defined or is it blank?
- Encrypted - If the field is defined as a simple string or long string data type, decide if the field values should be further secured by using encryption. For more information, see “Encrypting field values” on page 151.
- How many fields are 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, consider categorizing collections of object field definitions in the same field group for ease of maintenance.
- Object view - Which view pages will display the new field? Views include Detail, Folder, or List. A custom form or survey can only have a detail view page. For more information, see “Configure views for objects” on page 236.
- Display order - Where does the new field appear on a view page? What 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 display order of object types” on page 220.

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 create a generic **Owner** field and field group for all object types and reuse it later if you want to add it to an object.

To simplify the work, 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. Name the field group **Custom Fields** and the name of the field **Owner**. The field name is important because it is the initial label that appears 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 13, “Localizing text,” on page 277.

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, 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, there are no other fields to be added to the **Custom Fields** field group (**Owner** is the only field). 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).

You must now 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, place the **Owner** field for both object types after the **Modified By** field on the detail page. Because you 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 you have identified all the necessary information, you can begin "Adding field groups" on page 142 in the Task list. For details, see Table 45 on page 138.

File naming guidelines

To create an object field that you can use in reports, there are several factors to consider when choosing a field name.

Avoid using the object name in the field definition

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

For example, in the supplied field definitions, the OPSS-TestResult field group contains a field named Test Result.

Table 46: Prefix conventions

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

When the Cognos framework model is generated, the Test Result field is converted to the query item "TR_TEST_RESULT".

When the Cognos report is run, the "TR_TEST_RESULT" field column header displays as "Test Result Test Result" by default.

Limit the field name to 20 characters or fewer

Note:

- Limit the name definition to 20 character or less because characters that exceed 20 are truncated.
- The framework generator reserves character positions 21 and 22 for a unique ID in the query item name. Field names that exceed 20 characters are truncated after the 20th character.
- The object prefix is not counted in these 20 characters.

If are multiple field names are more than 20 character and have no unique characters in the first 20 characters, recreate the Reporting Schema only when necessary. The Cognos Reporting Schema generator may not generate the same two-digit unique ID for the field definitions for each reporting cycle. Reports that use these field definitions may not clearly identify each field definition.

Table 47: Example of framework generator naming results

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

Table 47: Example of framework generator naming results (continued)		
This Reporting Schema generation	**For a field definition with this name**	**May result in this**
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 is required, create the name with unique characters at the beginning of the name, such as "2008 Total Actual Financial Loss" instead of "Total Actual Financial Loss 2008".

Running the Schema Analysis report

Before adding fields to an object type, run the Schema Analysis report to determine the number of object fields that can be added to an object type.

The report shows how many object fields:

- Are currently configured for an object type
- Can "safely" be added to extend that object type

In general, 350 is the threshold limit for the number of fields that can be added to an object type when the average of all field names is 22 characters in length. By keeping the average field name short, it might be possible to include more than the 350 threshold limit for the number of fields.

Important:

Calculations on the Schema Analysis report use and display 175 as the threshold limit rather than 350. You can add more fields than the report shows.

Additionally, each currency field within an object type equates to six fields. This is because each currency field has six distinct columns within the database RT_ table. These six columns equate to the core currency field and its five subfields: Local Amount, Local Currency Code, Exchange Rate, Base Amount, and Base Currency Code.

The Schema Analysis report is accessed through the Cognos Analytics portal. The Report lists all object types, in alphabetical order, that are in the schema. The following example shows the name of each column in the Report and sample data for the Control object type.

Table 48: Information in the Schema Analysis report	
Report Column Name	**Example**
Object type	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

For example, you want to add three currency fields to the Control object type. Because each currency field equates to six fields, you would be adding 18 fields to the Control object type (3 X 6).

Using the numbers from the Example column in Table 48 on page 141, 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 can add 136 fields with names that do not exceed 22 characters in length, or up to 187 fields if the field names are 14 characters (or less). Adding the three currency fields (for a total of 18 fields) would be well within the threshold for this object type.

The values 136 and 187 are calculated based on 175 as a threshold limit. Since the threshold is 350, you can actually add approximately 311 or 413 fields, respectively.

Procedure

1. Click **Reporting** > **Cognos Analytics**.
2. Click **Team content**.
3. On the **Team content** page, navigate through the links as follows:

   OpenPages_Platform_V6 > Administrative Reports
4. On the **Administrative Reports** page, click the **Schema Analysis Report** link to run the report.

Adding field groups

A field group is a container for fields. Each field you create must belong to a field group.

Procedure

1. Enable System Administration Mode.
2. Click **Administration** > **Field Groups**.
3. On the **Field Groups** table, click **Add**.
4. On the **Field Groups** page, type a name for the field group.
5. Click **Create**.

What to do next
Add field definitions to the new field group. For details, go to “Adding fields to a field group” on page 142.

Adding fields to a field group

A field group can contain one or more fields.

A field definition stores the data type and other properties of a field. For each new field 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.

Before you begin
If the field group is already associated to an object type and you use DB2 and the reporting schema is enabled, perform this task when there is limited or no activity on the system. It can cause significant system delays in OpenPages due to locking conflicts on the DB2 platform. For more information, see “System delay when modifying object types and fields (DB2)” on page 796.

Procedure

1. Enable System Administration Mode.
2. Click **Administration** > **Field Groups**.
3. In the **Field Definitions** table of the field group, click **Add**.

4. On the **Field Definition** page, type a name and select a data type.

   The following table lists the properties that you can specify:

Table 49: Field definition properties	
In this box...	**Do this...**
Name	Type a name for the field. **Important:** The name must start with a letter, and can contain only letters, numbers, spaces, and the underscore (_) character. Examples: `Owner, owner1, Owner1_Risk`
Description	Type a description of the field.
Data Type	Select a data type for this field: a. Click the down arrow and select a data type from the list. b. Click the double arrows (>>) to display more options for the selected data type. For details see, "Data types" on page 143.
Computed **Note:** This additional option appears for most data types.	Select this box if you want this field to be a computed field. More boxes are displayed. For details, see, "Creating computed fields" on page 153.
Required **Note:** This additional option appears for all data types.	Select this property if you want the field to require data entry. For details, see, "Making fields required or optional" on page 151.

5. Click **Create**. The new field definition is listed on the Field Definitions table of the selected field group.
6. To add another field definition to this field group, repeat Steps 2, 3, and 4.
7. 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 177.

Data types

The IBM OpenPages GRC Platform application provides various data types from which you can choose.

After you select a data type for a field and save it, only the parameters or settings for the data type can be modified; you cannot change the data type itself.

To display more parameters for a selected data type, click the double arrow icon next to the data type selector.

Boolean data type

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.

Classifier data type

The classifier data type accepts simple string text that can be interpreted and classified by a Natural Language Classifier that uses Watson technology. It has the following settings:

Classifier Configuration Name
The name of a classifier configuration defined in **Administration** > **Cognitive Services** > **Natural Language Classifiers**.

Classifier Input Field
The field that provides text that is interpreted and classified by a Natural Language Classifier. Format is `<Field Group>.<Field Name>`.

For more information, see "Defining a Classifier Configuration" on page 728.

Currency data type

- **Include Conversion** - this setting controls whether the exchange rate and base amount conversion are visible.

  If this value is set to:

  – **True** - the following 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 might 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 specific date.

  – **False** - the following items are displayed in the currency field:

    Local Currency Code (drop down)

    Local Amount (text input)

    For example, you might 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 is accepted for this field.

  Maximum Value
  The greatest allowable currency value that is accepted for this field.

  If a user enters a value that is either below or above the specified value range, an error message is shown.

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 you enter 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 "Adding a currency field to a field group" on page 147.

Date data type

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.)

Decimal data type

The decimal data type accepts numeric values with decimal places for the following settings:

Minimum Value
The lowest allowable decimal value that is accepted for this field.

Maximum Value
The greatest allowable decimal value that is 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 is shown.

Enumerated String data type

The enumerated string data type accepts a list of string values and has these settings:

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 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.

If you are using Oracle, you can convert a single value selection setting to a multi-value selection setting.

If you are using IBM DB2 and you want to convert a single value selection setting to a multi-value selection setting, you must:

- Perform the conversion when there is limited or no activity on the system if the reporting schema is enabled. The conversion can cause significant system delays in OpenPages due to locking conflicts on the DB2 platform. For more information, see "System delay when modifying object types and fields (DB2)" on page 796.
- Complete remediation steps after the conversion is finished. For more information, see "Remediating after an Enumerated String field is changed to a multi-select field (DB2)" on page 795. Or, drop the reporting schema, change the setting, and then recreate the reporting schema.

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 reorder the list of values, see “Changing the order of enumerated string values” on page 160.

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 a display type for enumerated strings” on page 274.

Integer data type

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 is accepted for this field.

Maximum Value
The greatest allowable integer value that is 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 is shown.

Long String data type

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.

You can encrypt long string field values up to a maximum of 2 MB in the IBM OpenPages GRC Platform repository.

The long string has two sub types, medium and large.

The size of the medium sub type is fixed to 32 KB. The medium sub type is the only sub type that is supported for FastMap uploads.

The size of the large sub type set by default to 256 KB. It can be increased by changing the **Platform** > **Repository** > **Resource** > **Large Text** > **Maximum Size** setting.

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Enter a value in bytes. The maximum size applies to all large subtype long strings.

Important: After it is set, this value cannot be reduced.

Note: The maximum size is a hidden setting. To show hidden settings set **Applications** > **Common** > **Configuration** > **Show Hidden Settings** to **true**.

See “Long string fields” on page 174

Reporting Fragment data type

The Reporting Fragment data type displays a component (such as a bar or line chart) from a Cognos report or dashboard in a field. For details, see “Reporting fragment fields” on page 162.

Simple String data type

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.

You can encrypt simple string field values in the IBM OpenPages GRC Platform repository.

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 , you must do it through the profile. For details, see “Configuring display types for simple string fields” on page 262.

Single File data type

For legacy internal use. Do not use because this data type cannot be used in profiles.

Adding a currency field to a field group

You can add a currency field to a field group.

Procedure

1. Click **Administration** > **Field Groups**.
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 the field definition appears.
4. On the add page:
   a) In the **Name** box, type a name for the new currency field.
   b) Select **Currency** from the **Data Type** drop-down list.

      Important: Do not change or translate currency codes.
   c) 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 155 for information on computed fields.
   d) Check **Include Conversion** if the field is to include currency conversion.
   e) Click the >> icon and type the minimum and maximum allowable currency values to be allowed in the field in the **Minimum Value** and **Maximum Value** boxes.
   f) 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

You can edit currency field information.

Procedure

1. Click **Administration** > **Field Groups**.
2. In the **Field Groups** pane, click the name of the field group that contains the currency field to edit.
3. In the **Field Definitions** pane, click the name of the currency field to edit.
   a) Click **Edit**.
4. Edit the information.
5. Click **Save**.

Viewing and editing a currency display type

You can view and edit currency display type information for object types that contain a currency field.

Procedure

1. Click **Administration** > **Profiles**.
2. Click the name of the profile that contains both the object type and currency field you want to view or edit.
3. Click the object type.
   For example, to view or edit the currency display type for the **Inherent Severity** object field, select the **SOXRisk** object type.
4. 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.
5. To edit the currency display type, complete the following actions:
   a) Click **Edit**.
   b) Set the read only value to True or False.
   c) To set the field as required, select **Required**.
   d) Click **Save**.

Editing currency field values in individual accounts

If you have IBM OpenPages 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 **Accounts**.
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

You can add, edit, and enable or disable currency exchange rates.

Use one of the following methods to update currency exchange rates.

- Upload a CSV file with currency exchange rates from:
  - The application user interface. For more information, see "Formatting and uploading a CSV file" on page 149.
  - An ObjectManager loader file. For more information, see "Importing exchange rates" on page 610.

- Edit the rates in the application user interface manually. For more information, see "Editing exchange rates for an existing currency code" on page 149.
- Upload currency exchange rates in an ObjectManager loader file. For more information, see "Importing exchange rates" on page 610.

Note: You cannot use these functions with a new currency. The currency must exist.

Editing exchange rates for an existing currency code

One of the ways to modify an exchange rate for an existing currency code is by using the IBM OpenPages GRC Platform user interface.

Procedure

1. Click **Administration** > **Currencies**.
2. On the **Currencies** page, click **Edit**.
3. On the **Edit Exchange Rate** page, edit the currency exchange rates as wanted.
4. Click **Save**. The edited currency exchange rates appear on the Currencies page.

Formatting and uploading a CSV file

The file containing the exchange rate currency data must be in a comma separated value (.csv) file that is formatted in a specific way.

The file must have the following format:

```
<currency code>,<exchange rate>
<currency code>,<exchange rate>
```

Where:

Table 50: CSV file format placeholders for exchange rates

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. You can use either of the following formats: • `mm/dd/yyyy` • `mm/dd/yyyy HH:mm:sss` If no historic date is supplied, the current date is used.

The following data sample from a CSV file shows the ISO currency codes for Euros, Canadian dollars, and Japanese yen with the corresponding exchange rate for each currency, and the historical date that the rate was applied for two of the three currencies.

```
EUR,0.1589,12/26/2007
CAD,0.8636
JPY,0.0083,5/8/2008
```

Procedure

1. Click **Administration** > **Currencies**.
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. Click **Upload**. The new currency exchange rate appears in the Currencies table on the Currencies page.

Enabling currency exchange rates

You can enable disabled currency rates, making them available to the appropriate processes.

Procedure

1. Click **Administration** > **Currencies**.
2. On the **Currencies** page, click **Enable**.
3. On the **Enable Currencies** page, check all the currencies you want to enable.
4. Optional: Change the exchange rate for any listed currencies.
5. Click **Save**. The enabled currencies appear on the Currencies table.

Disabling currency exchange rates

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. Click **Administration** > **Currencies**.
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 group properties

You can modify the description property of any field group; however, the name of a field group cannot be changed.

Procedure

1. Click **Administration** > **Field Groups**.
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. Click **Save**.

Modifying object field definitions

After you create an object field, you can modify field definition properties.

For any type of object field - modify the description, whether 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, 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 more information, see “Adding enumerated string values” on page 160

Note: You cannot modify the name of any object field or its data type.

Procedure

1. Click **Administration** > **Field Groups**.
2. Click the name of the field group containing the object field to modify.
3. On the **Field Definitions** table, click the name of the field to modify.
4. On the **Field Definition Information** table, click **Edit**.
5. To define object fields as required or optional, see “Making fields required or optional” on page 151.
6. To set a default value for an object field, see “Setting a default value for an object field” on page 152.
7. Click **Save**.

Making fields required or optional

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 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 221).

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.

You can omit a required field for a particular view if the field is filled in by a trigger or if the field will have been filled in prior to this view being used to edit the object.

Procedure

1. Click **Administration** > **Field Groups**.
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. Click **Save**.

   Note: Changing a field to Required also causes all profile references to the field to be required as well.

Encrypting field values

You can encrypt a simple string or long string field value in the IBM OpenPages GRC Platform repository to prevent system administrators from viewing confidential data directly from the database. Encrypted field values are shown as a string of random characters.

Note: Before encrypting long strings in OpenPages running on Oracle 12.1, refer to the following Technote: http://www.ibm.com/support/docview.wss?uid=swg22010106. The Technote describes a potential issue and how to resolve it by obtaining the appropriate patch from Oracle support and applying it to your environment.

Procedure

1. Click **Administration** > **Field Groups**.
2. Click the name of the field group that contains 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. To encrypt all values for the field, select the **Encrypted** box.
6. Click **Save**.

   The field is now marked for encryption. The timing of the encryption depends on the status of the field level encryption keystore:

   - If keystore is enabled, all field values are encrypted when you save the field definition.
   - If the keystore is disabled, no field values are encrypted until you enable the keystore.

   For more information, see "Field level encryption" on page 81.

Decrypting field values

You can decrypt a simple string or long string field value in the IBM OpenPages GRC Platform repository if the data is no longer considered to be confidential. System administrators can view decrypted data directly from the database.

Procedure

1. Click **Administration** > **Field Groups**.
2. Click the name of the field group that contains 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 to decrypt this field, clear the **Encrypted** box.
6. Click **Save**.

   The field is now marked for decryption. The timing of the decryption depends on the status of the field level encryption keystore:

   - If the keystore is enabled, no field values are decrypted until you disable the keystore.
   - If keystore is disabled, all field values are decrypted when you save the field definition.

   For more information, see "Field level encryption" on page 81.

Setting a default value for an object field

When you create a new object field, by default, the **Default Value** property is empty (not populated).

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.

Restriction: The new default value will only be populated for new instances of an object type. In other words, if a user attempts to edit an existing object where the value was blank, it will remain blank. The new default value will be used when a user or administrator creates a new instance of that object type. For example, if an administrator modifies an enumerated string (dropdown field) on a test object. The new default value will be populated if new test objects are created. If an end user attempts to edit an existing test object, the new default value won't be set or modified for it.

Procedure

1. Click **Administration** > **Field Groups**.
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. 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 the Context, Detail, Activity, List, Home Page Filtered List, Filtered List, Grid and Folder views in the IBM OpenPages GRC Platform user interface.
- Must have unique field names. Adding more than one computed field with the same field name in the same view will result in an error.

If you want to import (load) and export (dump) computed field definitions, you must use the ObjectManager tool. For details, see "Importing computed field definitions" on page 614.

Computed fields require an installed and active Cognos server as they use the Cognos Computation Handler. If a computed field is executed in the application and the Cognos server is not available, the following message is displayed to users: *Cognos is unavailable. Please contact your System Administrator*.

Procedure

1. In Cognos Analytics - Reporting, model the computed field in a calculation object. For details, see "Modeling a new computed field in Cognos " on page 153.
2. In the OpenPages GRC Platform application user interface:
   a) Define the computed field. For details, see "Defining a computed field" on page 155.
   b) Regenerate the reporting framework. For details, see "Updating the reporting framework" on page 686.

Modeling a new computed field in Cognos

You can model an equation in Cognos to define a computed field in the application.

Note: If you do not know how to use Cognos Analytics - Reporting, seek the help of an experienced Cognos report author or call your IBM representative.

Procedure

1. Log on to the Cognos Analytics portal as an IBM OpenPages GRC Platform user with the locale set to **Report Design Language**.
2. Create a 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 **Toolbox** on the Insertable Objects pane and complete the following actions:
   a) Drag a **Calculation** object onto the report page.
   b) At the prompt, type a name.
   For example, type `Calc-Risk`.
5. In the **Expression Definition** pane of the model, complete the following actions:
   a) Enter an expression using model query items from the same namespace, function, or parameters.

   The Cognos SQL used to define this computed value can be an existing query item in the published Cognos 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). For details, see "Using Predefined Database Functions" in the IBM OpenPages Report Author's Guide.

   For example, the following equation returns a value with 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 and make any needed changes.
6. Run the report. Check the results.
7. Click **XML Show Specification** on the toolbar to view the Cognos SQL in an XML representation. The following XML sample shows which sections of the report will be used to define the computed field in IBM OpenPages GRC Platform and the corresponding field name in the application.

```
<querySet xml:lang="en-ca">
    <BIQuery name="Query1">
        <cube>
            <factList>
                <item refItem="RI_RISK_ID" aggregate="none"/>
                <item refItem="REPORTING_PERIOD_ID" aggregate="none"/>
                <item refItem="Calc-Risk" aggregate="none"/>
                <tabularModel>
                    <dataItem name="RI_RISK_ID">
                        <expression>[DEFAULT].[SOXRISK].[RI_RISK_ID]</expression>
                    </dataItem>
                    <dataItem name="REPORTING_PERIOD_ID">
                        <expression>[DEFAULT].[SOXRISK].[REPORTING_PERIOD_ID]</expression>
                    </dataItem>
                    <dataItem name="Calc-Risk">
                        <expression>total ([DEFAULT].[SOXCONTROL].[CN_INHERENT_SEVERITY_REDU]
                            for [DEFAULT].[SOXCONTROL].[RISK_ID]) / 100</expression>
                    </dataItem>
        </tabularModel>
    </querySet>
```

Note: Because the values in the Report Specification XML window cannot be selected, you can copy the report specification to the Clipboard (**Tools** | **Copy Report to Clipboard**) and then paste the information into a text document. Then, you can copy the attribute values into the application user

interface. The value to be used in the **Equation** definition box can also be obtained from the **Expression Definition** pane of the calculation object.

What to do next
In OpenPages GRC Platform, define the computed field. For more information, see "Defining a computed field" on page 155.

Defining a computed field

You can define a computed field.

Note: The following data types do not support computed fields: Currency, Enumerated String, and Single File.

Procedure

1. Click **Administration** > **Field Groups**.
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 51 on page 155 to select a data type for the new computed field.

Table 51: 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 icon  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 Cognos Computation Handler attribute fields appear.

If you modeled the computed field in Cognos Analytics - Reporting, the values displayed in the Report Specification XML window are not selectable (see "Modeling a new computed field in Cognos " on page 153). 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 Cognos SQL used to define the computed value for the object field. It can be a reference to an existing query item in the published Cognos framework or an equation involving multiple query items.

   For 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 Cognos 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.

    For example, DEFAULT.

11. Enter a value in the **Alternate Namespaces** box if necessary.

    The Alternate Namespace is the Cognos framework namespaces to which the computation will be added during reporting framework generation.

    Note: See “Using computed fields with multiple namespaces” on page 156 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 Cognos 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 Cognos 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.

    For example, [DEFAULT].[SOXRISK].[REPORTING_PERIOD_ID]

14. Enter the package label of the reporting package that the field is run against in **Package Name**. The value is case sensitive. The package label for a framework model is defined in the **Administration** > **Settings** > **Platform** > **Reporting Framework V6** > **Models** > **[model name]** > **Package Label** setting. If **Package Name** is empty, the package for the OPENPAGES_FRAMEWORK_V6 framework model is used.
15. Click **Create**. IBM OpenPages GRC Platform will then validate the equation against the primary and alternate namespaces.
16. Regenerate the reporting framework to make the computed field available to report authors. For details, see “Updating the reporting framework” on page 686.

Using computed fields with multiple namespaces

The IBM OpenPages GRC Platform application allows multiple parent object types for a given child object type.

The Cognos 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 × 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 × (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 OpenPages GRC Platform 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 OpenPages GRC Platform application will not allow you to save the computed field until corrected. The 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.

Troubleshooting: Computed field 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 IBM OpenPages GRC Platform supports multibyte characters and so this may not be the equivalent of 20,000 characters if you are using a multibyte language.

Troubleshooting: 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.

If 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.

Troubleshooting: Optimizing report request performance

With the addition of computed fields there is a large increase in the number of report requests and so it is important to make sure Cognos 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, log on to the Cognos Analytics portal as a user with administrative privileges, for example, OpenPagesAdministrator.

   By default, the URL is:

   `http://<hostname>/ibmcognos/bi` (if you are using port 80 for Cognos)

   Where `<hostname>` is the name of the Cognos server.

2. Click **Manage** > **Administration Console** to launch the **IBM Cognos Administration** page.
3. On the **Status** tab, click the **System** link.
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`

      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:
   a) Expand **Process**.
   b) View and optionally 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 optionally 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 optionally 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 metrics and additional settings that are not listed here, see the Cognos Analytics 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 Cognos server. For example, if your environment is always at peak and Cognos 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.

Troubleshooting: Computed field query direction performance

While in Cognos it is possible to query up the relationship tree (that is, compute values based on ancestors), but it is strongly discouraged.

When exploring all the computation possibilities there is one large distinction in what can and should be done. 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.

Adding enumerated string values

You can add new values to an existing list of enumerated string values at any time. The modifications you make to values in a list are globally applied to all instances wherever that field group is in use.

For example, 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. Click **Administration** > **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) 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” on page 160.

Defining a default value for an enumerated string value

You can define a default value for an enumerated string value. When you define a default value, it is automatically applied to new objects that you create, but it is not applied to existing objects.

If you define a multi-select enumerated field value as the default value, and the field is hidden, users can see the hidden field value in the Add New wizard because the default attribute overrides the hidden attribute.

Procedure

1. Click **Administration** > **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, click **Edit**.
5. Update the **Default Value**.
6. Click **Save**

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, 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 reorder 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. Click **Administration** > **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".

If you define a multi-select enumerated field value as the default value, and the field is hidden, users can see the hidden field value in the Add New wizard because the default attribute overrides the hidden attribute.

Procedure

1. Click **Administration** > **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) 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** icon 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. Click **Administration** > **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) 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** icon 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 161.

Procedure

1. Click **Administration** > **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) 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**.

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 Cognos report.

Reporting fragment fields are configured in a number of ways:

- Associate with an object type
- Add to various object view pages
- Configure as dependent fields
- Modify their display type

By default, reporting 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 overridden when the reporting 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 Cognos 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 GRC Platform Report Author's Guide* on your documentation media for designing reports that can be used in reporting fragment fields.

Tasks for configuring reporting fragment fields

Use the following configuration tasks to set up new reporting fragment fields.

Table 52: Tasks for configuring reporting fragment fields

Task Description	Related Topic
Identify the Cognos report and report component and the field group you want to use.	“Planning considerations for reporting fragment fields” on page 163
From Cognos, obtain the parameter information for the reporting fragment field.	“Fields requiring parameter information” on page 164
In the IBM OpenPages GRC Platform application, define the reporting fragment field.	“Defining a reporting fragment field” on page 164
Add the field group to an object type if it is not already included.	“Including field groups for an object type” on page 177
Select a profile and add the reporting fragment field to an object type in that profile.	“Including fields in an object type” on page 219
Select an object view in that profile and add the reporting fragment field to that view page.	“Configure views for objects” on page 236
Optionally, change the display type and display characteristics.	“Configuring the display type for reporting fragment fields” on page 261

Planning considerations for reporting fragment fields

Before you add a reporting 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 reporting 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 reporting fragment field:

- Report component — What report component data does the user need to see to accomplish their task? Which Cognos report contains the component?
- Field group — Will new reporting fragment fields reside in new or existing field groups?
- Object type — Which object type will use the reporting fragment field or fields?
- Views — Which view pages in a profile will use the reporting fragment fields (such as Filtered List View, Detail View, Activity View, My Work tab)?
- Display — How many reporting fragment fields will be included in a Detail or Activity View page? Will a reporting fragment field be embedded (Automatic) on the page or displayed as a pop-up window (On Demand)?

Fields requiring parameter information

The process of creating a new reporting fragment field for use in the IBM OpenPages GRC Platform application involves copying parameter information from Cognos and either pasting or entering it into fields on the Reporting Fragment data type field definition page in the IBM OpenPages GRC Platform application.

Note: You must have administrative privileges set on your account so you can access:

- The Cognos Analytics portal and Cognos Analytics - Reporting for obtaining parameter information
- The IBM OpenPages GRC Platform application for defining the new reporting fragment field

Table 53 on page 164 lists the various fields on the Reporting Fragment data type field definition page that require specific parameter information.

Table 53: Required parameter information

Fields	Field description	Where to find the parameter information
Report Path	Required. The file path of the selected Cognos report that contains the component you want to use. “Defining the report path” on page 165	Cognos Analytics, **Team content** folder
Fragment Name	Required. The unique name of the particular report component (such as a ’Pie Chart’, ‘List’, ‘Combination Chart’, and so forth). “Defining the reporting fragment name” on page 166	Cognos Analytics - Reporting, 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. “Defining the object ID prompt” on page 167	Cognos Analytics - Reporting, 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. “Defining the reporting period ID prompt” on page 167	Cognos Analytics - Reporting, Prompt Page

Defining a reporting fragment field

When defining a reporting fragment field, some tasks are required and some tasks are optional.

For purposes of illustration, the following tasks use examples from a sample Assessment Status report to configure a reporting fragment field that will display the chart component of this report as an embedded report on a Risk Assessment Detail View page.

Table 54: Tasks to define a reporting fragment field

Task	Required or optional
"Setting up a field group for a new reporting fragment field" on page 165	Required.
"Defining the report path" on page 165	Required.
"Defining the reporting fragment name" on page 166	Required.
"Defining the object ID prompt" on page 167	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.
"Defining the reporting period ID prompt" on page 167	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.
"Defining the reporting fragment size" on page 168	Optional. Use if you want to manually control the height and width of the pop-up window for a fragment field.

Setting up a field group for a new reporting fragment field

You can use either an existing field group or create a new field group for the new reporting fragment field.

Before you begin

Complete the following steps to set up a field group for a new reporting fragment field:

Procedure

1. Access the **Field Groups** page. See "Adding field groups" on page 142.
2. To include the reporting fragment field in an existing field group, click the name of the field group.
3. To include the reporting fragment field in a new field group, see "Adding field groups" on page 142.
4. On the detail page of the field group, navigate to the **Field Definitions** pane and click **Add**.
5. On the field definitions detail page, type the name of the object field.
6. Click **Reporting Fragment** from the **Data Type** field.
7. Click the double arrow  next to the data type selector to display additional parameters.

   Note: Keep the browser window open because you will return to it.

Defining the report path

To define the report path, gather information from both the Cognos Analytics portal and IBM OpenPages GRC Platform to obtain path information for the report.

Before you begin

Complete the following steps to define the report path:

Procedure

1. From a browser, log on to the Cognos Analytics portal as a user with administrative privileges, for example, OpenPagesAdministrator.

   By default, the URL is:

   `http://<hostname>/ibmcognos/bi` (if you are using port 80 for Cognos)

   Where `<hostname>` is the name of the Cognos server.
2. Click the **Team content** folder and navigate through the folder hierarchy to the report location.

   For example,

   ```
   Team content > OPENPAGES_REPORTS_V6 > Risk Assessment Reports >
   Risk Assessment Status
   ```
3. In the Actions column for the report, click the **Set Properties** icon  .
4. On the **Set Properties** page of the report, select **General**.
5. Click the **View the search path, ID and URL** link.
6. In the **View the search path, ID and URL** window, copy the text in the **Search path** field.

   The following example is a sample search path text for the Risk Assessment Status report.

   ```
   /content/folder[@name='OPENPAGES_PLATFORM']/folder[@name='Risk
   Assessment Reports']/report[@name='Risk Assessment Status']
   ```
7. In OpenPages GRC Platform, go to the **Reporting Fragment field definitions detail** page and paste the search path text into the **Report Path** field.
8. In the Cognos Analytics portal, close the **View the search path, ID and URL** window. Exit the "Set properties" page (do not exit Cognos).

Defining the reporting fragment name

To define the reporting fragment name, the steps in this task require going back and forth between the Cognos Analytics portal and the IBM OpenPages GRC Platform application user interface to obtain the name of the report component within the selected report.

Before you begin

Complete the following procedure to define the reporting fragment name:

Procedure

1. In Cognos Analytics - Reporting, open the report containing the component you want:
   a) On the Team Content tab, navigate through the folder hierarchy to where the report you want is saved.

      For example, `Team Content > OpenPages Solutions V6 > Risk Assessment Reports > Risk Assessment Status`
   b) Under the Actions column for the report you want, click **Edit report**.
2. In edit 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) Click **Show Properties** in the application bar.
   b) In the **Properties** pane, look at the title bar. It should display the name of the selected component, such as Pie Chart, List, Combination Chart, and so forth.

c) 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. In the Properties pane, under the **Miscellaneous** heading, copy the value in the **Name** property.

   For example, the Name property value for the Combination Chart component of the sample Risk Assessment Status report is `Combination Chart1`.

5. In OpenPages GRC Platform, on the Reporting Fragment field definitions detail page, paste or type the value into the **Fragment Name** box.

   For 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 Cognos Analytics - Reporting.

Defining the object ID prompt

To define the Object ID Prompt, the steps in this task require going back and forth between the Cognos Analytics portal and the IBM OpenPages GRC Platform application user interface.

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.

Procedure

1. In Cognos Analytics - Reporting, open the report:
   a) On the Team Content tab, navigate through the folder hierarchy to where the report you want is saved.

      For example, `Team Content > OpenPages Solutions V6 > Risk Assessment Reports > Risk Assessment Status`

   b) Under the Actions column for the report you want, click **Edit report**.

2. For the selected report:
   a) Click **Pages**.
   b) Navigate to the prompt page of your report.

3. On the prompt page:
   a) Click the prompt for the object identifier (such as Entity, Process, and so forth).
   b) Click **Show Properties** in the application bar.
   c) Under the **General** heading, click the **Parameter** property icon and copy the value in the box (for example, `Entity`).

      For 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`.

4. In OpenPages GRC Platform, on the Reporting Fragment field definitions detail page, paste or type the value into the **Object ID Prompt** box.

   For example, for the sample Risk Assessment Status report, you would paste or type `Entity` in the Object ID Prompt box.

Defining the reporting period ID prompt

To define the Reporting Period ID Prompt, the steps in this task require going back and forth between the Cognos Analytics portal and the IBM OpenPages GRC Platform application user interface.

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.

Procedure

1. In Cognos Analytics - Reporting, open the report:
   a) On the Team Content tab, navigate through the folder hierarchy to where the report you want is saved.

      For example, `Team Content > OpenPages Solutions V6 > Risk Assessment Reports > Risk Assessment Status`

   b) Under the Actions column for the report you want, click **Edit report**.
2. For the selected report:
   a) Click **Pages**.
   b) Navigate to the prompt page of your report.
3. On the prompt page:
   a) Click the prompt for the reporting period identifier.
   b) In the **Properties** pane, scroll to the **General** heading.
   c) Under the **General** heading, click the **Parameter** property icon and copy the value in the box.
4. In OpenPages GRC Platform, on the Reporting Fragment field definitions detail page, paste or type the value into the **Reporting Period ID Prompt** box.

Defining the reporting fragment size

When defining the reporting fragment size, if you leave the pixel values for height and width blank (this is the default), the pop-up window is sized automatically.

This task is optional. Use if you want to manually control the height and width of the pop-up window for a reporting fragment field.

Procedure

1. In IBM OpenPages GRC Platform, on the **Reporting Fragment field definitions detail** page:
   a) In the **Height** box, type a numeric value for the pixel height of the reporting fragment.
   b) In the **Width** box, type a numeric value for the pixel width of the reporting fragment.
2. Click **Save**.

Using object fields to launch JavaServer Pages and external URLs

You can customize the OpenPages application to launch JavaServer Pages (JSPs) or external URLs from object fields. You can pass arguments to the JSP or external URL in a URL configuration string that is defined on the object field.

The launchers use simple string fields with a URL display type to show a labeled hyperlink in the application. The URL parameters for the hyperlink can contain system-generated elements, such as the ID of the target object and the current reporting period. The availability of the hyperlink can be controlled by a set of conditions. For example, the link is active when the current user is the Process Owner and they select the current Reporting Period.

The attributes for the launchers are specified by using a URL configuration string that is defined as the default value for the object field, called a URL launcher field in this context. The application processes the configuration string when an object view that contains the URL launcher field is rendered. You can add

launchers to Detail, Activity, Filtered List Views, and Grid Views. You define the hyperlink's label using application text. You can make the label meaningful for your users. For external URLs, you can make the label a short name that users know rather than a long URL.

To set up a URL launcher field:

1. Define the URL configuration string. Learn about the attributes in the string and study the examples. For information, see “Attributes in the URL configuration string” on page 169 and “URL configuration string examples” on page 171.
2. Define the URL launcher field and add the URL configuration string to it. For information, see “Adding a URL launcher field ” on page 173 .
3. Define the label for the URL launcher field in application text. For information, see “Configuring application text” on page 172.
4. Add the URL launcher field to views. For information, see “Adding a URL launcher field to views” on page 173.

Attributes in the URL configuration string

The URL configuration string is in JSON format.

It uses the following attributes:

- labelKey
- path
- parameters
- conditions
- popUp

labelKey attribute

Identifies the application text key for the localized URL text. If it is omitted, the label defaults to **Go**.

path attribute

Specifies the relative path to the target JSP, report, or application object view. If the target is a JSP, then it must be in a folder that is under the `sosa` application deployment folder. The path attribute is required.

The application root is automatically prepended to the specified path by the application. The application root is determined from the application.url.path property in the `sosa.properties` configuration file.

The path value must contain the leading slash. For example, `"path" : "/custom/mycustom.jsp",`

modes attribute

Controls whether the URL launcher field is available in edit or view mode.

In order for a URL launcher field to appear in an Activity View Child Hierarchy pane, the "Edit" mode must be included.

parameters attribute

Contains the list of request parameters that are assembled to create the query string of the URL. The parameters are specified as a list of key-value pairs. In most instances, the key names can be anything that you define.

System-populated keys and values are indicated by a $ in the name. They consist of:

- the ID of the current object, indicated by a parameter value setting of "$objectId"
- the ID of the current reporting period selection, indicated by a parameter value setting of "$reportingPeriodId"

Any subset of these parameters can be specified.

Hardcoded parameter values can also be included. For example, where the target JSP or report is reused in different contexts and requires additional information to identify the context for this specific URL launcher field.

The URL parameter values are URL encoded, while the keys are not.

conditions attribute

Defines conditions that must be met in order for the URL to be active.

The conditions can include the following:

- Whether the Reporting Period selected is the current period.
- Whether the target object is locked.
- Whether the value of a specific field matches a value.
- Whether the value of a specific field matches the name of the current user.
- Whether the current user is a member of the group name set in a specific field.

Any subset of the available conditions can be included in the URL configuration string. These conditions are evaluated in the order in which they appear in the string. Each condition can optionally include a labelKey that contains an application text string that is displayed when a condition is not met, for example, "Available only for the Process Owner." If the labelKey is omitted, the key for the field is applied.

Multiple conditions of the same type can be used, except for the objectState and reportingPeriod conditions. You can use only one objectState and one reportingPeriod.

Most errors in the configuration of a condition cause a positive failure in the condition and evaluate to true. The errors are logged. Thorough testing of both positive and negative cases is encouraged to ensure the expected behavior.

reportingPeriod condition

The reportingPeriod condition is met when:

- The value of "isCurrent" is true and the user is in the current Reporting Period.
- The value of "isCurrent" is false and the user is in any previous Reporting Period.

objectState condition

The objectState condition is met when:

- The value of "isUnlocked" is true and the current object is not locked.
- The value of "isUnlocked" is false and the current object is locked.

fieldValue condition

The fieldValue condition evaluates the value of the field against the value that is specified by the value attribute by using the specified operator. The target field is identified by using the

`FieldGroup.FieldName` convention. The supported operators are "equal" and "notEqual". If the operator is invalid or omitted, the evaluation defaults to "equal".

The `Simple String`, `Boolean`, and `Enumeration` field types are supported. Ensure that you specify the system name and not the localized label for the enumeration values.

The fieldValue condition supports checking the current user—by specifying "$currentUser"—against the value of the target field.

The fieldValue condition does not support system fields ("Created by" and "Modified by") or multi actor fields.

popUp attribute

Controls the behavior of the new window. The "windowAttributes" string determines the characteristics, such as size and scroll bars, of the new window that is created when the user clicks the hyperlink. The popUp attribute is optional.

URL configuration string examples

The following examples illustrate how to define URL configuration strings.

Launching a custom JSP

The following example launches a custom JSP.

```
$ {
      "labelKey" : "custom.url.labelForMyCustomUrl",
      "path" : "/custom/mycustom.jsp",
      "modes" : ["edit", "view"],
      "parameters" :
       {
             "objId" : "$objectId",
             "repId" : "$reportingPeriodId",
             "isRisk" : "true" ,
             "includeVersions" : "false"
       },
       "conditions" :
       {
             "reportingPeriod" :
             {
                   "isCurrent" : true/false,    // no quotes for boolean values
                   "labelKey" : "custom.url.label.invalid.ReportingPeriod"
             },
             "objectState" :
             {
                   "isUnlocked" : true/false,   // note the UN-locked designation
                   "labelKey" : "custom.url.label.object.locked"
             },
             "fieldValue" :
             {
                   "field" : <"FieldGroup.FieldName">,
                   "value" : "$currentUser",
                   "operator" : "equal",     // supported operators include "equal" and
"notEqual"
                   "labelKey" : "custom.url.label.invalid.user"
             }
             "fieldValue" :
             {
                   "field" : <"FieldGroup.FieldName">,
                   "value" : true,
                   "labelKey" : "custom.url.label.invalid.value"
             }
             "fieldValue" :
             {
                   "field" : <"FieldGroup.FieldName">,
                   "value" : "Undifferentiated",
                   "operator" : "notEqual",
                   "labelKey" : "custom.url.label.invalid.value"
             }
       },
       "popUp" :
```

```
        {
              "windowAttributes" : "height=600,width=800,menubar=no,status=yes,toolbar=no,
   scrollbars=yes,resizable=yes"
        }
   }
```

Launching a Cognos report

The following example launches a Cognos report from a Command Center redirect with a security condition:

```
${
  "labelKey": "report.name.security.domain.role.assignments",
  "path": "/report.tree.post.do",
  "modes": ["view"],
  "parameters": {
    "reportPath": "/_cw_channels/Reporting/SOX/OpenPages V6/Audit Reports/Security/Security
Domain Role Assignments.pagespec",
    "label": "Current Reporting Period",
    "submitAction": "preview",
    "actionContext": "preview",
    "entity_id": "$objectId"
  },
  "conditions": {
    "fieldValue": {
      "field": "OPSS-BusEnt.Executive Owner",
      "value": "$currentUser",
      "operator": "equal",
      "labelKey": "custom.url.invalid.user"
    }
  }
}
```

Launching a custom JSP

The following example launches a custom JSP.

```
$ {
      "labelKey" : "url.custom.jsp",
      "path" : "/custom/custom.jsp",
      "modes" : [ "view", "edit" ],
      "parameters" :
      {
          "Risk Category" : "Damage to Physical Assets",
          "Risk Sub-category" : "Willful Damage"
      }
}
```

Configuring application text

You can add translated labels for the keys that you specify in the URL configuration string.

Procedure

1. Under **Administration**, click **Application Text**.
2. In the Custom line, click **Add New**.
3. Enter the key value in **Name**.
4. Enter useful information, for example, the URL field that uses the key, in **Description**.
5. Enter the label text in **Default Label**.
6. Click **Create**.
7. Expand the new key, and add the translated text.
8. Repeat theses steps for each key in the URL configuration string.

Adding a URL launcher field

The URL launcher field is defined with the URL configuration string as the default value.

Before you begin

Define the URL configuration string before you create the URL launcher field.

Procedure

1. Under **Administration**, click **Field Groups**.
2. Click **Add**.
3. Enter a **Name** and **Description** for the field, and click **Create**.
4. In the list of field groups, click the field group that you added.
5. In the Field Definitions table, click **Add**.
6. Enter the information for the field:
   a) Enter a system name for the field.
   b) In the **Data Type** box, select **Simple String**, and click the arrow to add it.
   c) Set the **Default Value** to the URL configuration string.
   d) Clear the **Required** and **Computed** boxes.
   e) Click **Create**.

Adding a URL launcher field to views

Add the URL launcher field to the object type and then to the views.

Procedure

1. Under **Administration**, click **Object Types**.
2. Select the object type that you want to add the URL launcher field to.
3. In the **Included Field Groups** section, click **Include**, select the field you created in “Adding a URL launcher field ” on page 173, and click **Add**.
4. Under **Administration**, click **Profiles**.
5. Select a profile you want to update.
6. Click the object type that contains the new field.
7. Click **Include**, select the new field, and click **Include**.
8. Click the newly added field, and in the **Object Field Information** pane, click **Edit**.
9. Change the **Display Type** to URL, and click **Save**.
10. Go back to the profile detail page and click the name of a view that you want to add the field to.
11. In the **Included Field Groups** section, click **Include**, select the new field, and click **Include**.
12. Select **Read-Only** for the field, and click **Save**.

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. Enable System Administration Mode.

2. Click **Administration** > **Field Groups**.
3. Select the box next to the name of the field group to delete.
4. Click **Delete** on the **Field Groups** pane.

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. After a field definition is deleted, it cannot be restored.

Procedure

1. Access the **Field Groups** page (see "Adding field groups" on page 142).
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. Click **Delete**.

Long string fields

A long string field is assigned to the long string data type. Long string fields allow users to enter more than 4000 bytes in a single field.

You can encrypt long string fields up to a maximum of 2 MB in the IBM OpenPages GRC Platform repository.

There are two sub types of the long string field: medium and large. The size of medium long string fields is fixed to 32 KB. The size of the large long string fields is set by default to 256000 bytes, but that can be increased by changing the **Platform** > **Repository** > **Resource** > **Large Text** > **Maximum Size** setting.

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Note:

- For more information about long string data types, see "Data types" on page 143.
- For more information about setting display types for long string fields, see "Configuring display types for long string fields" on page 271.
- For more information about filtering on long string fields, see "Utilities for filtering on long string field content in an Oracle database" on page 451 and "Utilities for filtering on long string field content in a DB2 database" on page 404.
- For more information about concatenating simple string fields into a long string field, see "String concatenation utility" on page 457
- For more information about encrypting fields, see "Field level encryption" on page 81.

Chapter 10. Object types

An object type contains metadata about a category of object, such as a Risk or Process object, or a custom form.

From an Object Type page, you can view and access the following information:

- 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 that are used to narrow the scope of data for this object type
- Dependent fields and pick lists 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 that are 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 includes 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 information, see "Tasks required to set up custom forms" on page 187.

Related information

- Configuring groups and fields for an object type, see Chapter 9, "Fields and field groups," on page 137.
- Customizing text labels for object types, see Chapter 13, "Localizing text," on page 277.
- Configuring facts and dimensions in the reporting framework, see "Facts and dimensions" on page 661.

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

Platform object types

The IBM OpenPages GRC Platform object model is configurable and can contain object types.

Because the object types and schema vary widely from customer to customer, Table 55 on page 175 lists only the Platform object types that are installed, by default, on all systems.

Table 55: Platform object types

Icon	Object Name	Singular Label
	SOXBusEntity	Business Entity
	SOXIssue	Issue
	SOXTask	Issue Action Item
	SOXDocument	File
	SOXExternalDocument	Link

Table 55: Platform object types (continued)		
Icon	**Object Name**	**Singular Label**
	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 Milestones.

Property rendering JSP files

Every object type requires a property rendering JSP file. The JSP file controls the format of the elements that comprise the layout of a form on a Web page.

Note: This information applies only to Windows environments. For AIX environments, see an IBM representative for assistance.

IBM OpenPages GRC Platform includes a generic property rendering JSP file, called `properties.jsp`, that is used by object types and cannot be changed. It is located in the *<OP_Home>*|`applications`|`op-apps`|`sosa`|`activityview` folder.

Where *<OP_Home>* is the installation location. By default, this location is `c:\OpenPages`.

Note: For backward compatibility with upgraded OpenPages systems prior to the 5.5 release, the existing JSP file, called `renderProperties.jsp`, is still used by the standard object 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 best to 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

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.

Note: To access the **Object Types** menu item, you must have the Object Types application permission set on your account (for details, see "Types of application permissions" on page 32).

Procedure

1. Log on to the IBM OpenPages GRC Platform as a user with the Object Types application permission set.

2. With the Object Types application permission set, select the **Administration** menu and click **Object Types**.

Editing object type properties

You can edit the description of an object type and set whether to keep older versions of the object type. The JSP Path can be edited only for custom forms.

Restriction: Do not use characters defined in CJK Unified Ideographs EXTENSION-B on Unicode in the description field.

Procedure

1. With the Object Types application permission set, click **Administration** from the menu and click **Object Types**.
2. Click the name of the object type to modify.
3. Click **Edit**.
4. Make the necessary changes.
5. To save an older version of this object type, select the **Save older versions of this object type?** check box. If this box is not checked, the old version is overwritten.
6. Click **Save**.

   Note: To change label text for an object type, see Chapter 13, "Localizing text," on page 277.

Including field groups for an object type

A new or existing field group must be added to an object type before any of the fields can be displayed on an object view page.

To create a new field group, see "Adding field groups" on page 142.

The object type can be predefined (see the topic, "Platform object types" on page 175, for a list of object types) or a custom form.

Restriction: Before you can add a field group to a custom form or survey, create an object type for the custom form or survey. For information, see "Adding an object type for a custom form" on page 188.

When you include a field group with an object type, the field group is displayed on the **Included Field Groups** tab of the object.

Before you begin

If you use DB2 and the reporting schema is enabled, perform this task when there is limited or no activity on the system. It can cause significant system delays in OpenPages due to locking conflicts on the DB2 platform. For more information, see "System delay when modifying object types and fields (DB2)" on page 796.

Procedure

1. Enable System Administration Mode.
2. With the Object Types application permission set, click **Administration** from the menu and click **Object Types**.
3. From the list, click the name of the object type.
4. On the **Included Field Groups** panel, click **Include**.
5. Select the field groups to include.
6. Click **Add**.

What to do next
To make fields visible to users in an object view, see “Configure views for objects” on page 236

Disabling associations between object types

If an association between a parent or child object type is no longer needed, disable the relationship between these object types.

For example, if a survey becomes obsolete and you no longer want it associated with a specific Risk object, disable the association between the survey object and the parent object type (SOXRisk).

For example, if you do not want users to associate certain object types together, such as Accounts with Business Entities, 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 child object type is removed from the Detail View page of the parent object. The parent object type removed from the Detail View of the child object type.
- For a custom form or survey, the custom form or survey is removed from the available form types that can be added from the **Associated Files and Forms** tab of a parent object.
- The **Disable** icon 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. Enable System Administration Mode.
2. With the Object Types application permission set, select **Administration** from the menu bar. Click **Object Types**.
3. From the list, click the name of the object type to modify.
4. Navigate to either the **Child Associations** tab or **Parent Associations** tab on the Object Type Information detail page.
5. From the list of associated object types, click the name of the object type to disable.
6. On the **Association Detail Info** page, click **Disable**. The icon changes to **Enable**.
7. To add the object relationship changes to reports, complete the following tasks:
   a) Update the Reporting Schema. For details, see “Creating or recreating the reporting schema” on page 91.
   b) Regenerate the reporting framework. For details, see “Updating the reporting framework” on page 686.

Enabling associations between object types

To allow an association between a parent or child object type that was disabled, enable the association between these object types.

When you enable an association between object types, the following events occur:

- The enabled child object type displays on the Detail page of the parent object type.
- The **Enable** icon 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. Enable System Administration Mode.
2. With the Object Types application permission set, select **Administration** from the menu and click **Object Types**.
3. From the list, click the name of the object type to modify.
4. Navigate to either the **Child Associations** tab or **Parent Associations** tab on the detail page of the selected object type.
5. From the list of associated object types, click the name of the object type to enable.
6. On the **Association Detail Info** page, click **Enable**.
7. To add the object relationship changes to reports, complete the following tasks:
   a) Update the Reporting Schema. For details, see "Creating or recreating the reporting schema" on page 91.
   b) Regenerate the reporting framework. For details, see "Updating the reporting framework" on page 686.

Configuring IBM OpenPages GRC Platform to associate a large number of child objects

If the number of associations that you add exceeds the maximum, the result is a long running process. The default is 250. This information applies only to child associations, not parent associations.

About this task

You can use IBM OpenPages GRC Platform to associate a large number of child objects by using the Add New Wizard as well as using the **Associate an existing issue** command from the **Actions** menu in the Detail view or Activity view. When the number of child associations exceeds the limit set in the **Max Child Associations Interactive** setting in the registry, the process runs in the background and you receive an email when it completes.

You might see something similar to the following message:

```
Due to the large number of associations, the objects will be associated in the background. You will receive an email when the process is complete.
```

These settings are set by default. You can change the following settings to specify the maximum number of associations, the timeout length, and the email response to a long running process.

Procedure

1. From the menu bar, click **Administration** > **Settings**.
2. To specify the number of child objects to associate before background processing begins: **Applications** > **Common** > **Max Child Associations Interactive** . The default is 250.
3. To specify the transaction timeout for the background process, click **Platform** > **Processes** > **Associate Resources** > **Transaction Timeout**. The default is 21600 seconds.

   To show the **Transaction Timeout** setting, change the value of **Applications** > **Common** > **Configuration** > **Show Hidden Settings** from false to true. The default value is false.
4. To specify the email settings for the email server configuration, click:
   - **Applications** > **Common** > **Email** > **Mail Server**
   - **Applications** > **Common** > **Email** > **SMTP Password**

- **Applications** > **Common** > **Email** > **SMTP Port**
- **Applications** > **Common** > **Email** > **SMTP Security Type**
- **Applications** > **Common** > **Email** > **SMTP User Name**

5. Optional: You can customize the email subject and content. From the menu bar, click **Administration** > **Applications** > **Application Text** > **Miscellaneous**.
   - com.resource.association.email.subject.success
   - com.resource.association.email.subject.warning
   - com.resource.association.email.subject.error
   - com.resource.association.email.content.success
   - com.resource.association.email.content.warning
   - com.resource.association.email.content.error

Object relationship types

In IBM OpenPages GRC Platform, a relationship type is either Association or Reference between objects in the object model.

An object model must not contain relationship definitions that result in a loop (a cyclic relationship) when the object hierarchy is traversed.

The Association type relationship is the most common 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 new installations of the product, loops cannot be created in the new model.

However, for upgrades from a version prior to 5.5, the object model may contain relationship definitions that create a loop between objects. If OpenPages GRC Platform encounters a loop between objects in the hierarchy, some pages may return incomplete results.

The following diagram demonstrates how a path from SubAccount to Process in an object model can create a loop or cyclic relationship. 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.

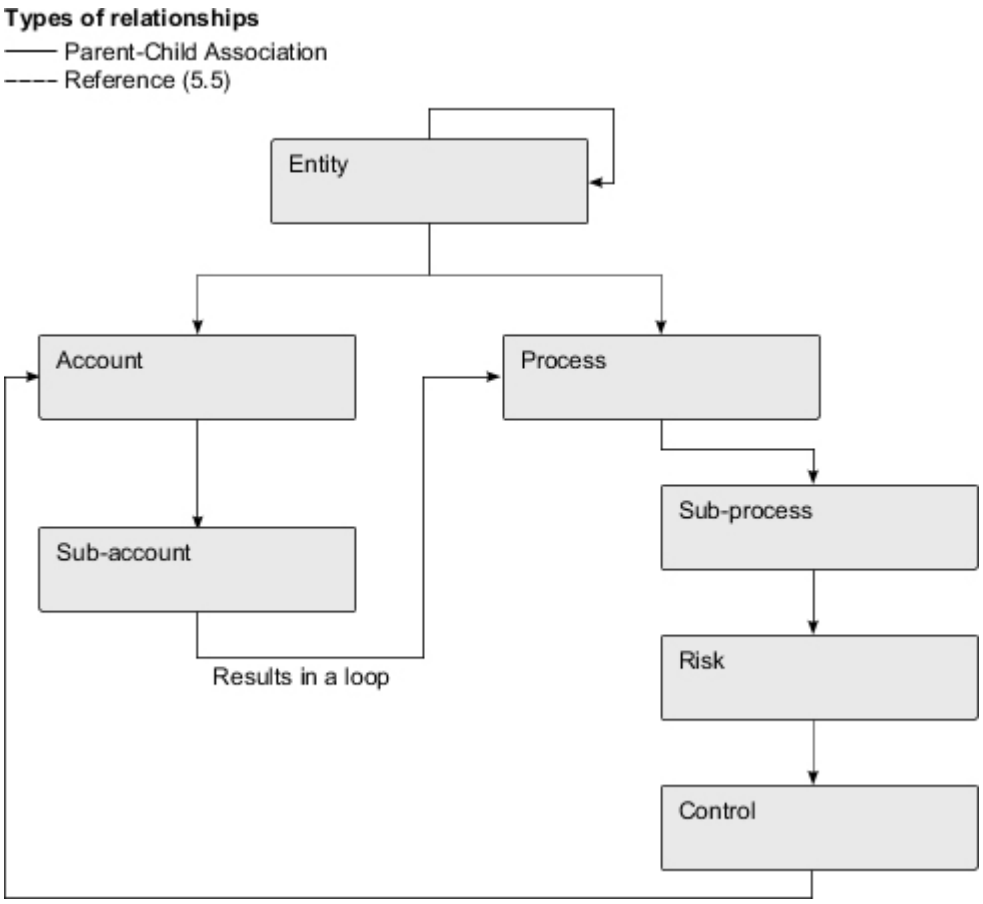


Figure 13: Sample invalid cyclic relationship

To resolve a loop 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 not being used (that is, there exists no instance data in your database that has these relationships), disable the relationship. For details, see "Disabling associations between object types" on page 178.
- Leave the relationship that creates the loop, but change its type. For example, to retain the relationship that creates a loop because the object model accurately describes your business, change its type from Association to Reference (see Figure 14 on page 182). For details on changing the reference type, see "Setting the relationship type" on page 182.

Figure 14 on page 182 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.

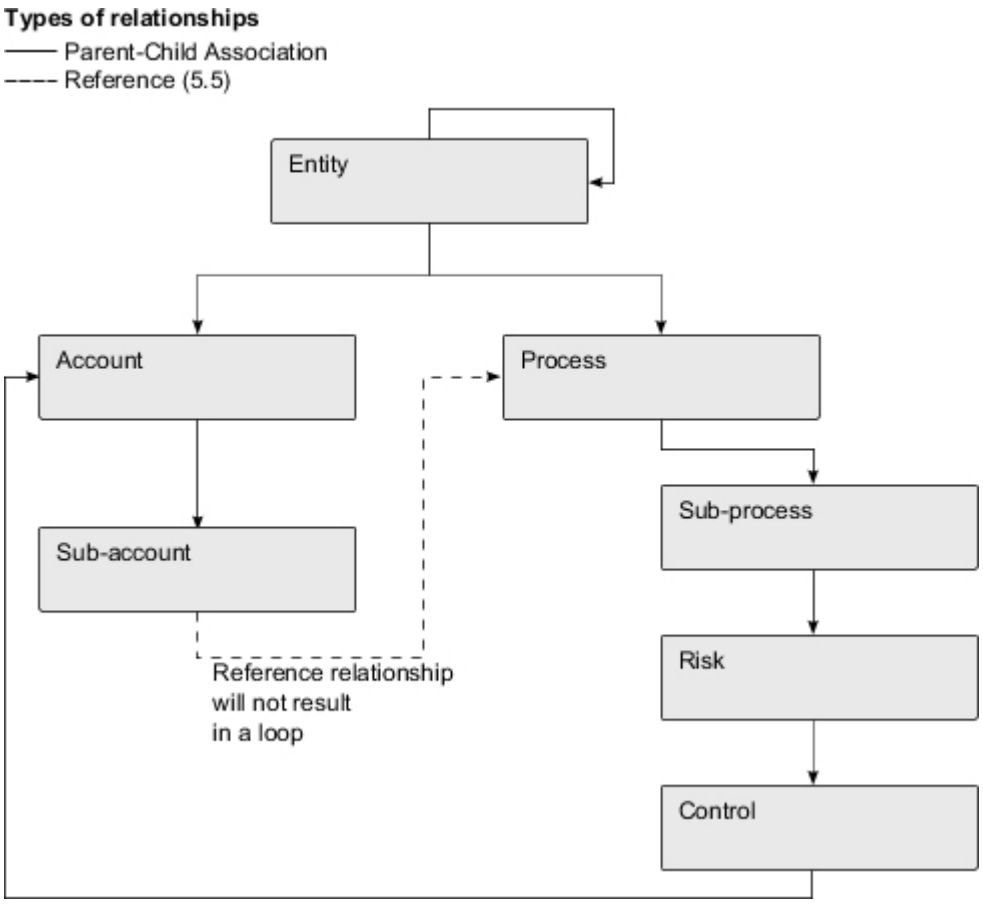


Figure 14: Sample reference relationship

Setting the relationship type

You can set the relationship between parent and child objects.

Procedure

1. Enable System Administration Mode.
2. With the Object Types application permission set, select **Administration** from the menu and click **Object Types**.
3. Click the name of the parent object type with the child relationship to modify.
4. On the **Child Associations** panel, select the child object to modify.
5. Click **Edit**.
6. Select a value in the **Relationship Type** field.
7. Click **Save**.

Configure the ability to create a draft copy of an Object

Configure the Save As Draft feature to display a **Save As Draft** icon when the user edits or creates objects. Users can save object data without completing all required fields.

The **Save As Draft** icon is displayed next to the **Save** icon on the **Detail View** page of an object type when the object is in edit mode.

To configure the Save As Draft option, create a field group and an enumerated string field. After the group and field are created, use these values to enable the **Save As Draft** icon. The group and field can then be

associated with object types in a profile. The field does not have to be associated with a view in a profile to display the **Save As Draft** icon.

See the following topics for details on the Save As Draft configuration process:

- “Creating a field group and field for a Save As Draft configuration” on page 183
- “Configure the Save As Draft feature for new objects” on page 183
- “Adding the field to the object type and profile to configure the Save As Draft function ” on page 184

In the illustration, the field group in the “Creating a field group and field for a Save As Draft configuration” on page 183 procedure is called "DraftGroup" and the enumerated field is called "Draft Status" with values of "Draft" and "Published".

When the user clicks **Save As Draft**, the value of the **Draft Status** field is automatically set to "Draft". When the user clicks **Save**, the required fields are automatically validated and the value of the **Draft Status** field is set to "Published". It is best to hide the "Draft Status" field from object views in a profile. However, if you make the "Draft Status" field visible in a profile object view, configure it as Read only.

Use the Save As Draft feature with Activity View pages

To use the Save As Draft feature with **Activity View** pages, the **Save As Draft** icon must be configured on the root or parent object type. The root or parent object is the first object type that is listed in the Activity View.

If a child object type has **Save As Draft** configured but the parent object type does not, **Save As Draft** is not visible on the **Activity View** page.

The required field validation is skipped on child objects if they have the draft field in the profile. Required field validation on the child object is completed if no draft field is defined in the profile, even when a user click **Save as Draft**.

Creating a field group and field for a Save As Draft configuration

To add a Save As Draft icon to an object view, you first create a field group and field.

Before you begin

Complete the following steps to create a field group and add field definitions to the group:

Procedure

1. Create a field group and name it. See “Adding field groups” on page 142.
2. Add a field definition to the new field group and name it.
   a) Select the **Enumerated String** data type.
   b) Add a value for `Draft` and a value for `Published` . See “Adding fields to a field group” on page 142.

Related tasks

“Configure the Save As Draft feature for new objects” on page 183
“Adding the field to the object type and profile to configure the Save As Draft function ” on page 184

Configure the Save As Draft feature for new objects

To configure the Save As Draft feature, the second task is to configure settings.

Before you begin

Complete the following steps to configure settings:

Procedure

1. Click **Administration > Settings**.

2. From the configuration folder, click **Show Hidden Settings**. Set the value to true. For more information, see "Show hidden settings" on page 311.
3. Expand the **Common | Configuration | Required Field Validation** folder hierarchy.
4. Select **Draft Status Field**. In the **Value** field, type the name of the field group and the field. click **Save**.
   The format is `<field group>.<field name>`.
   For example, type`DraftGroup.Draft Status`.
5. Click **Draft Status Value**. In the **Value** field, type the system name of the draft value and click **Save**.
   For example, type`Draft`
6. Click **Publish Status Value**. In the **Value** field, type the system name of the draft value.
   For example, type `Publish`.

Related tasks

"Creating a field group and field for a Save As Draft configuration" on page 183
"Adding the field to the object type and profile to configure the Save As Draft function " on page 184

Adding the field to the object type and profile to configure the Save As Draft function

The third task in the Save As Draft configuration is to add the new field to the object type and profile.

Procedure

1. Enable System Admin Mode. See "Enabling and disabling System Administration Mode" on page 17.
2. For each object type to enable the **Save As Draft** icon, include the new field group.
   For example, include the field group called `DraftGroup`. See "Including field groups for an object type" on page 177.
3. Disable System Admin Mode.
4. Include the new field.
   For example, include the field that is called `Draft Status`, in a profile. See "Including fields in an object type" on page 219.

   Note: Unless you want the field to be visible to users, the field does not have to be included on a **View** page for **Save As Draft** to be displayed.

Related tasks

"Creating a field group and field for a Save As Draft configuration" on page 183
"Configure the Save As Draft feature for new objects" on page 183

Stand-alone object settings

Cardinality settings determine if an object can be created as a standalone object and whether it can be associated with more than one parent object.

Important: The setting values control the options on the user interface that allow users to create objects as stand-alone. The setting values are NOT currently used to enforce the number of associations between object instances.

In new installations, the default values for the minimum (Min Children = 0) and maximum (Max Children = 2147483647) number of children should not be modified.

Enabling the creation of stand-alone objects

When a user adds a child object type from the **Detail** page of a parent object type, the child object type is created and associated with the parent object type. A stand-alone object is a child object that is not associated with a parent object.

For example, if you select **Risks** on the **Assessments** menu, and then click **Add New** on the Risk **Folder View** page, a child object is created in the top-level Risk object type folder but is not be associated with a parent object.

You control the ability of users to create standalone object types 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 - **Add New** is displayed on the object **Folder View** page. Users can create stand-alone 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 stand-alone objects from a Detail View or Activity View page.
- 1 - **Add New** is removed from the object **Folder View** page. Users cannot create stand-alone instances of a child object type. This value is the default setting in new installations.

Note: For data consistency, set the minimum parent setting to either 0 or 1. A minimum parent setting that is greater than 1 is the same as setting it to 1.

Procedure

1. With the Object Types application permission set, select **Administration** from the menu and click **Object Types**.
2. Click the name of the object type to modify.
3. On the **Parent Associations** panel, click the name of a parent object type.
4. On the **Association Detail Info** panel, click **Edit**.
5. In the **Min Parents** box, type 0 (for standalone) or 1 (to prevent a stand-alone object type).
6. Click **Save**.
7. For multiple parent objects, repeat Steps 3 - 6 for each parent object.

Enabling the ability to associate objects

For object type relationships that contain a child object type, you can control the ability of users to associate child object types. Control them by configuring the value of the maximum parents cardinality setting.

Use the following information to determine the value to set in the maximum parents cardinality setting (`Max Parents`):

- 2147483647 (infinity) in the **Max Parents** field enables the display of the **Associate** and **Disassociate** menu items on the **Detail** view of the object type. Users can associate that object to more than one parent object. The default value is 2147483647.
- 1 in the **Max Parents** field removes **Associate** and **Disassociate** menu items from **Detail** view of the object type. Users cannot create shared instances of a child object type.

Notice: The maximum parents associations on a child object is not enforced. For instance, if the maximum parents setting is 2, the application allows a child object to be shared among 3 or more parent objects of the same type. A maximum parent setting of greater than 2 is the same as setting it to infinity.

Procedure

1. With the Object Types application permission set, select the **Administration** menu and click **Object Types**.
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. Click **Save**.
7. If you more than one child objects for which you want to restrict the parent object relationship, repeat Steps 3 - 6 for each child object.

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).

In IBM OpenPages GRC Platform file type extensions are case sensitive.

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 GRC Platform application supplies a number of predefined MIME types.

Adding a file type

When you add a file type to the application, it is automatically added to the File Type Information selection list.

Before you add a file type, verify that it does not already exist. To view a list of file types, click **Include** on the **File Types Information** panel of the SOXDocument object type. If the file type is displayed in the list, go to "Associating a file type with an object type" on page 186. If the file type is not displayed, click **Cancel** and complete this procedure.

In IBM OpenPages GRC Platform file type extensions are case sensitive.

Procedure

1. With the Object Types application permission set, select **Administration** from the menu and click **Object Types**.
2. Click **SOXDocument**.
3. On the **File Types Information** panel, click **Add New**.
4. In the **MIME Type** field, type a MIME content type and subtype. For example, image/cgm.
5. In the File Extension field, type a file extension that corresponds to the MIME Type. For example, cgm.
6. Click **Create**.

What to do next

To associate the new file type with the SOXDocument object type, see "Associating a file type with an object type" on page 186.

Associating a file type with an object type

You can associate various file types with the SODocument 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. With the Object Types application permission set, select the **Administration** menu and click **Object Types**.
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. You can select multiple boxes.

b) When finished, scroll down 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. With the Object Types application permission set, select the **Administration** menu and click **Object Types**.
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**.

Results

The associated file type is removed from the list on the **File Types Information** tab of the SOXDocument object type.

Note: Files might still be discovered after the extension of these files is excluded from search. If a file extension is associated with more than one MIME type, then files with this extension are still discovered until all associated MIME types are excluded or are disabled from search. Follow the procedure "Removing a file type from other object types" on page 187 with each associated MIME type to remove the types from searches. For more information, see "Enabling attachment file types for global search" on page 362.

Removing a file type from other object types

You can remove a file type if a file extension is associated with more than one MIME type..

Procedure

1. Move the MIME type from the exclusion list to the inclusion list.
2. Disable the MIME type.
3. Move the MIME type back to the exclusion list.
4. Run the **Update** command.
   For more information, see "Enabling or disabling object types or fields for global search" on page 363.

Tasks required to set up custom forms

To set up custom forms, such as surveys, you must complete many tasks.

Note: If you imported a custom form through the ObjectManager, perform Task 6.

Table 56: Tasks for adding custom forms	
Task Description	**Related Topic**
1. Create an object type for the custom form.	See "Adding an object type for a custom form" on page 188 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 field groups" on page 142 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 fields to a field group" on page 142 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 177 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 from a parent object" on page 189 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 219 for information about how to include the custom form object type on an object's view page.
7. To run reports against a custom object type, specify a custom prefix for the real-time reporting schema tables.	See "Enabling the reporting framework for custom forms" on page 667 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. After the object type is created, you can include field groups and associate parent objects to it.

Procedure

1. Enable System Administration Mode.
2. With the Object Types application permission set, select **Administration** from the menu and click **Object Types**.
3. On the **Object Types** pane, click **Add**.
4. On the add page, complete the following steps:
   a) Type a name for the new object type.

      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 include:

      ```
      RiskSurvey, survey1, Survey1_Risk
      ```

b) In the **JSP Path** field, 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 *<OP_Home>*\profiles\(servername)-OPNode1\installedApps\OpenPagesCell\op-apps.ear\sosa.war\ folder.
If you are using, for example, a custom JSP file, the folder and file name might look similar to this: /Survey/MySurvey.jsp.

c) Click **Create**.
The object type is created, and the Object Type detail page displays where you can configure properties. For details see, "Editing object type properties" on page 177.

5. To run reports against this custom object type, you must configure a custom prefix for the real-time reporting schema tables. For details, see "Enabling the reporting framework for custom forms" on page 667.

Deleting a custom object type

You can only delete custom object types that are not in use in the application.

Procedure

1. Enable System Administration Mode.
2. With the Object Types application permission set, select **Administration** from the menu and click **Object Types**.
3. Select the object type to delete..
4. On the **Object Types** tab, click **Delete**.

Associating a custom form from a parent object

You can only add child object associations to object types; you cannot add child associations to a custom form or survey object types from the Detail page of a parent object.

Procedure

1. Enable System Administration Mode.
2. With the Object Types application permission set, select **Administration** from the menu and click **Object Types**.
3. Click the name of the object type to modify.
4. On the **Child Associations** tab, click **Add**.
5. On the **Available Custom Forms** page, select each custom form to associate with the selected parent object type.
6. Click **Add**.

Associating a custom form to a parent object

You can only add parent object associations to a custom form or survey object types; you cannot add new parent object associations to an object type from the Details page of a custom form object.

Procedure

1. Enable System Administration Mode.
2. With the Object Types application permission set, select **Administration** from the menu and click **Object Types**.
3. Click the name of the custom form object you want to modify.
4. On the **Parent Associations** tab, click **Add**.
5. On the **Available Object Types** page, select each parent object where the object type will be attached.
6. Click **Add**.

Tasks to define filters for an object type

Filters are specific to an object type and are used to narrow the scope of data that is returned in a view for that object type.

About this task

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 are returned for that object type.

Filters are used with Filtered List Views, Grid Views, Activity Views, and the Home page. An object type can have multiple filters.

The following table provides an overview of the flow of tasks for adding filters to object types and views.

Table 57: Tasks for configuring filters and views

Task	Task Description	Related Topic
1	Determine the purpose and characteristics of the filter.	“Filter considerations” on page 190
2	Add the filter to an object type.	“Adding filters to object types” on page 191

Filter considerations

Before you create a filter, determine the characteristics of the filter and identify the object type on which the new filter is used.

For instructions on creating a filter, see “Adding filters to object types” on page 191.

The following list identifies information that you need 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 profiles will be associated with the filter?
- Filtering criteria - Which fields are 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 (Grid View, Filtered List View, Home page, Activity View)?

Example

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:

Table 58: Sample risk assessments fields

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 and from any Risk Assessment Grid View for that profile.

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 196) 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.

Filters that contain unavailable fields

When a filter contains a field that is no longer available (for example, the field was excluded from a profile), when that filter is selected, the row with the unavailable field is replaced by the default filter condition.

To resolve this issue, edit the filter to remove the unavailable field.

Adding filters to object types

Filters are specific to an object type and narrow the scope of data that is returned in a view for the object type. When you create a filter for an object type, 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 in an Oracle database” on page 451.

Attention: If you create a new filter that uses the character % as the value, for example `Name Contains %2`, the Name Contains value field appears empty after you load the filter: the % character does not appear. However, the filter runs properly.

Procedure

1. Access the **Object Types** page (see “Accessing object types” on page 176).
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 the plus sign icon.
4. On the **Add Filter** page:
   a) Click the **Field** field and select a key field from the list.
      Common fields are listed first, 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 is not case sensitive.

Table 59: Search conditions

If a field has a	You can do this
user icon	Click to select a user from a phonebook. You can also select multiple users.
group icon	Click to select a group from a hierarchical tree structure. You can also select multiple groups.
search icon	Click to search for a user or group.

Table 59: Search conditions (continued)	
If a field has a	**You can do this**
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 196
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.
 calendar icon 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 special characters in filters for long string fields" on page 192.

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 195.

d) Click **Save**.

5. To associated the filter with a view, see "Tasks to associate filters with views" on page 196.
6. To create a duplicate filter using the new filter as a template, see "Copying filters" on page 196
7. To localize the display name of a filter, see "Modifying display text for public filters" on page 280.

Limitations on special characters in filters for long string fields

When you create filters for long string fields, some special characters have limitations on how they are used.

Do not use special characters as first or last character

When you use a filter to search for text in long string fields, the following special characters and symbols might 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 * № € Å ☆ @

Note: When you search for text that contains these special characters, you must use the **Contains** search condition in the filter.

For example, 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.

Important: You can use the forward slash to create filters for folders. If you want to start or end your filter with a forward slash, then you must use a double forward slash. The first forward slash is stripped out. For example, if you enter a folder, enter it as `//foldername`.

Reserved characters

Table 60: Reserved characters that have special meaning in the filters

Reserved character	Description
_	An underscore is used as a single character wildcard.
%	A percent sign is used as a multiple character wildcard.

Do not use these special characters

Table 61: Special characters that are not supported in search filters

Special Character	Description
&	Ampersand
@	At symbol on keyboard
!	Exclamation point or bang
\	Backward slash
^	Caret or circumflex
:	Colon
;	Semicolon
,	Comma
-	Dash
>	Greater than sign
<	Less than sign
(	Opening parenthesis
)	Closing parenthesis
=	Equal sign
|	Pipe or vertical bar
+	Plus sign
#	Pound or number sign, hash symbol
?	Question mark
~	Tilde or equivalency sign
`	Grave accent

Table 61: Special characters that are not supported in search filters (continued)	
Special Character	**Description**
[	Opening bracket
]	Closing bracket
{	Opening brace
}	Closing brace
$	Dollar sign
¥	Yen sign
₩	Won sign
ꑭ	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
- 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 191) 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 62: 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. Click **Save** or select from **Actions** menu.

Examples

- 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)`.
- 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.

Tasks to associate filters with views

After you create a filter for an object type, you can associate it to a profile and an object view.

Table 63: Associating filters procedures	
Filter tasks	**Procedure**
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 and Grid view pages" on page 248
Use the filter to personalize the home page for users who are assigned a particular profile.	"Configuring filtered lists on the My Work tab" on page 229
Use the filter in an **Activity View** page to limit the scope of listed child objects.	"The layout of Activity views" on page 253 or "Modifying an Activity view " on page 256
Use the filter in a **Grid View** page to limit the scope of listed child objects.	"Creating a Grid view " on page 248

Filtering on the currently logged on user

You can 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.

Procedure

Complete one of the following actions:

- 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 End User value 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 "Configuring display types for simple string fields" on page 262.
  - Multi User Selector
  - Multi Group Selector
  - Multi User/Group Selector
- 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.

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. With the Object Types application permission set, select **Administration** from the menu and click **Object Types**.
2. From the list, click the name of the Object type to modify.

3. On the **Filters** panel, click the filter you want to copy.

   The **Edit** window opens for the filter.
4. Select **Save as** from the **Actions** menu.
5. Type a unique name (required) for the new filter. Click **Apply**.

Results

The new filter is now available in the **Filters** tab. For instructions on specifying filters and using complex logic in filters, see "Adding filters to object types" on page 191 and "Using complex logic in a search filter" on page 195.

To display the new filter in the list of Saved Filters on an **Filtered List View** page, add it to a profile. For details, see "Associating filters to Filtered List view and Grid view pages" on page 248.

Modifying filters

After you create a filter, you can modify it. The modifications, once saved, are immediately used in the application.

Procedure

1. With the Object Types application permission set, select **Administration** from the menu and click **Object Types**.
2. Click the name of the Object type to modify.
3. On the **Filters** pane, click the filter to edit.
4. Make the required changes.
5. Click **Save**.

Results

To modify a localized display name of a filter, see "Modifying display text for public filters" on page 280

For instructions on specifying filters and using complex logic in filters, see "Adding filters to object types" on page 191 and "Using complex logic in a search filter" on page 195.

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 and Grid view pages" on page 248.

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 with object views in a profile (such as a Filtered List View, Grid View, or table on the My Work 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. With the Object Types application permission set, select **Administration** from the menu and click **Object Types**.
2. Click the name of the object type to modify.
3. On the **Filters** tab, select the filters you want to delete.
4. Click **Delete**.

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.

Attention: If you configure a field to be required, it is still required even if it is not visible. This ability is for cases where the hidden field is updated by a separate activity, but the field is still required.

Dependent fields can be applied to Filtered List Views, Context Views, Grid Views, and Detail Views. They cannot be applied to Folder Views, List Views or Home Page Filters.

Important: On the Filtered List View page, if a dependent field column is shown, the column values adhere to the field dependency behavior.

Important: When users edit an object in Detail View, fields that are hidden due to how the field dependencies are configured can display as empty space.

Example

You want to know who performs 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 **Does the Control Owner perform 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 this field would remain hidden from the user.

The **Does the Control Owner perform 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 controlling fields. When you add a dependent field, configure the field and a behavior. Then, select the field and value that control the behavior.

About this task

If you want a dependent field to have multiple behaviors, such as Required and Visible, configure the field separately for each behavior.

OpenPages GRC Platform supports standard multi-select functionality on the detail page.

Note that if an administrative user creates field dependencies and dependent picklists that create a loop, an error is displayed in the interface that states that "The operation is not allowed because it would result in the following circular dependencies ...". If you are upgrading and you had a loop in the previous version, if you change your configuration you will get an error in the interface that states that "The operation is not allowed because it would result in the following circular dependencies ...".

If you have multiple controlling fields for a specific behavior, you configure what conditions must be met before the behavior of the dependent field is triggered. The conditions are identified in the following list:

- 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) or Actor fields (User Selector, Group Selector, User/Group Selector, Multi User Selector, Multi Group Selector, or Multi User/Group Selector). If you configure a controller field with multiple values that are combined with an AND, all controller values or criteria must match. If you configure a controller field with multiple values that

are combined with an OR, only one of the controller values or criteria must match. When the values or criteria match, the dependent field behavior is triggered.

- Computed fields and report fragment fields can have only a behavior of Visible.

Procedure

1. With the Object Types application permission set, select **Administration > Object Types**.
2. Click the name of the object type to modify.
3. On the **Field Dependencies** pane, click **Add**.
4. From the **Select Dependent Field**, select a field from the list.
5. In **Dependent Field Behavior**, select one of the following values:

Table 64: Dependent Field Behavior values

Value	Description
Required	Require the user to enter a value in the dependent field only if the controlling field is selected. **Attention:** If you configure a field as required, it is required even if it is not visible. This ability is for cases where the hidden field is updated by a separate activity, but the field is still required.
Editable	Enable the user to modify this dependent field only if the controlling field is selected. Otherwise, the dependent field is read only.
Visible	Display the dependent field to the user only if the controlling field is selected. Otherwise, the dependent field are hidden from view.

6. Click **Next**.
7. On the **Select Controller(s)** page, click the **Controlling Field** and choose a field from the list.
8. In the **Controlling Values** box, select one or more values from the list and click **Add**.
9. If you have multiple controller fields, click **Operator** and choose one of the following logical operator values:

Table 65: 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 of the selected controllers to be used to meet the condition.

10. Click **Finish**.
11. To create additional dependent fields, complete one of the following tasks:

Table 66: Create additional dependent fields		
If you want to	**And the Controllers are**	**Then**
Add another behavior to the same dependent field - OR - Create another dependent field	the same as those selected in Step 4	Complete one of the following steps: • Copy the controller conditions to the new dependent field (see "Copying controller conditions" on page 200) • 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** pane.

Copying controller conditions

If you have multiple 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. With the Object Types application permission set, select **Administration** from the menu and click **Object Types**.
2. Click the name of the object type 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** icon.
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. Click **Create**.

   The newly created dependent fields with the copied controllers are listed on the Field Dependencies pane.

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.

About this task

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.

Note that if an administrative user creates field dependencies and dependent picklists that create a loop, an error is displayed in the interface that states that "The operation is not allowed because it would result in the following circular dependencies ...". If you are upgrading and you had a loop in the previous version, if you change your configuration you will get an error in the interface that states that "The operation is not allowed because it would result in the following circular dependencies ...".

Procedure

1. With the Object Types application permission set, select **Administration** from the menu and click **Object Types**.
2. Click the name of the object type to modify.
3. On the **Field Dependencies** pane:
   a) Select 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) 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) Click **Delete**.
7. To change the operator when there are multiple controllers, click the **Operator** arrow and select a value from the list.
8. 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. With the Object Types application permission set, select the **Administration** menu and click **Object Types**.
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. You can select multiple boxes.

b) 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

You can delete a dependent field.

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 201.

Procedure

1. With the Object Types application permission set, select the **Administration** menu and click **Object Types**.
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. You can select multiple boxes.
   b) Click **Delete**.

Results

The selected dependent field is removed from the list on the **Field Dependencies** tab.

Configuration settings for the Add New wizard

The Add New wizard provides a way for users to easily add new object instances from virtually anywhere in the system. The appearance and function of the wizard is configurable. Some of the configuration settings apply globally and some are profile and object type specific.

With the Add New wizard, users can create and save object instances from wherever they are in the system by entering only the minimum and most important information. There are several launch points for the wizard, depending upon user permissions:

- A global **Add New** icon appears on every page. It can be used to create any object type.
- An **Add New** icon appears in the toolbar for the Filtered List View, Grid View, or Home Page Filtered List View. It can be used to create an object instance that is of the same type as the object type of the list.
- An **Add New** option is available from a context menu when you right-click on a row in Filtered List View, Grid View, or a Home Page Filtered List. It can be used to create an object instance that is of the same type as the object type of the list, or any of the direct children of the object type in the row.
- An **Add New** option is available from the **Actions** menu in Detail and Activity Views. The option allows adding an instance of a specific object type.

In most instances, the Add New wizard provides the most convenient and efficient way to add object instances. However, the original add behavior is available in the following places in the program:

- From the Folder View

- From the **Add New** icon available from the Business Entity Object List View if the Folder View and Filtered List View are both disabled for Business Entity.
- From the **Add New** icon available from **My OpenPages** > **Project** > **Milestones**.
- From the **Add File** link available from **My OpenPages** > **Attachments** > **Browse**.

The Add New wizard consists of a series of tabs that users can move between by clicking the **Previous** and **Next** icons or by clicking the tabs. The tabs that are available to users are determined by the object type, the user's profile, and the configuration.

Create tab

The Create tab allows users to select an existing object from which to prepopulate the field values for the new object they are creating. Type a term in the **Search** field to find an exact match to the object name or description. Configuration determines the following behaviors:

- If this is not possible to create an instance for the specified object type, the tab will not appear
- If it is mandatory to create and object instance from an existing instance, the tab will appear and an object must be selected from the specified location before the user can move to another tab.
- If this creating and object instance from an existing instance is optional, the tab will appear and the user can either select an object from which to prepopulate field values or choose to create the new object from scratch by filling in all the field values manually.

For more information see, "Controlling the ability to use a template object when using the Add New wizard" on page 205

Parents tab

The Parents tab allows users to identify the primary parent; the one in whose context the new object will be created. For most configurations, selecting a primary parent is required. This tab also allows users to select additional secondary parents of the same or different object type as the primary parent. Type a term in the **Search** field to find an exact match to the object name or description.

Object-specific tabs

One or more fields tabs follow the Parents tab. They contain the fields available to users for the specified object type. The tabs and fields displayed are driven by the view definition used for the Add New wizard.

The view definition comes from an Activity View named **Add New** for this object type for the users' profile. The Activity View must have this name but its label can be different. For more information see, "Creating Activity Views" on page 250.

The view definition comes from a Creation View named **Add New** for this object type for the users' profile. The Creation View must have this name but its label can be different. For more information see, "Creation views" on page 241.

The following factors determine the view:

- If the Activity View is not present and enabled, then the Detail View is used.
- If the Detail View is not enabled, then the default Object View is used
- Sections in the view definition become tabs in the Add New wizard. Fields are presented in the same sections and in the same sequence in the Add New wizard as they are in the view definition. If there are fields before the first defined section, or if there are no sections in the view definition, then a tab labeled **Properties** is created to hold those fields. Read-only settings in the view definition are respected by the Add New wizard.
- Certain fields and field types are not supported in the Add New wizard. The following fields are not included in the Add New wizard if you configure them in the view definition:
  - System audit trail fields: Create By, Last Modified By, Created Date, Last Modified Date
  - System location field: Folder
  - System derived fields: Orphan, Business Entity Hierarchy, Primary Association Path
  - Computed fields
  - Reporting fragments

Associated children tabs

If there are child objects that can be linked to the object instance, one or more association tabs may follow the object-specific tabs.

For example, if you are creating a questionnaire assessment, you can choose the processes or assets to associate with the questionnaire assessment.

Type a term in the **Search** field to find an exact match to the object name or description.

Review tab

The Review tab displays all of the information from the preceding tabs in read-only mode. It provides users with an ability to perform a review of their choices and entries before they save their work.

Tab labels are displayed in the wizard with a circle beside each tab label. When a circle is white, it means that all of the required fields for that tab are either not complete or have failed validation. When all required fields in a tab are complete and all field values have passed validation, the circle for that tab is green. An object instance will not be created until the circles for all the tabs are green.

The Add New wizard supports existing configuration parameters, including Save as Draft, Auto-naming, Dependent Fields, and Dependent Picklists.

The Save As Draft feature can be configured to display a **Save As Draft** icon when a user creates a new object instance. This means that users can save object data without completing all the required fields. The **Save As Draft** icon is displayed next to the **Save** icon in the Add New wizard. For information on how to specify the Save as Draft settings, see "Configure the ability to create a draft copy of an Object" on page 182

For most object types, you can auto-generate their names when they are created. This allows users to enforce internal naming policies and ensure unique object names. You can turn auto-naming on or off for each object type individually. For information on how to specify the Auto-naming feature, see "Object auto-naming settings" on page 317.

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. For more information see, "Dependent field behavior" on page 198

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. For more information see, "Configuring dependent picklists" on page 207

Controlling the availability of object types in the Add New wizard

You can configure which object types cannot be created from the Add New wizard with a setting that takes effect for all users and all profiles.

Note: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Procedure

1. From the menu bar, click **Administration** > **Settings**.
2. Click **Applications** > **GRCM** > **Add New Wizard**.
3. Click **Object Types Disabled**.
4. In the **Value** box, type the names of the objects that you want to disable. Separate each object type with a comma (,). Be sure to use the object names and not the object labels.
5. Click **Save**.

Controlling the display of tabs with no fields in the Add New wizard

You configure whether fields tabs without any fields to display appear in the Add New wizard as disabled or do not appear at all. The Add New wizard will dynamically hide or show or enable field tabs as they become empty or not empty as a result of field dependencies.

Procedure

1. From the menu bar, click **Administration** > **Settings**.
2. Click **Applications** > **GRCM** > **Add New Wizard**.
3. Click **Show Empty Sections**.
4. In the **Value** box, type false if you do not want to show empty sections and tabs. Type true if you want empty sections to appear but be disabled.
5. Click **Save**.

   In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Controlling the ability to use a template object when using the Add New wizard

You can specify whether users must create new object instances from an existing object instance, whether they can optionally create new object instances from an existing object instance, or whether the user should create the object from scratch.

About this task

If you want users to be able to create object instances either from scratch or from an existing object instance, ensure that the object type name does not appear in either the **Cannot Create from Existing** setting or in the **Must Create from Existing** setting.

If you do not want users to create object instances from an existing object instance, include the object type names in the **Cannot Create from Existing** setting.

If you want to force users to create object instances from an existing object instance, include the object type names in the **Must Create from Existing** setting.

The **Cannot Create from Existing** and the **Must Create from Existing** settings can be configured globally for all profiles, can be configured individually for each profile, or in combination:

- To configure globally for all profiles, enter the desired information in the **All Profiles** setting under the **Cannot Create from Existing** and the **Must Create from Existing** folders.
- To configure individually for each profile, create a setting for each profile, whose name is the name of the profile, under the **Cannot Create from Existing** and the **Must Create from Existing** folders. Enter the desired information in each profile setting.
- To configure a combination of globally but to override that configuration for specific profiles, create a setting for each profile you wish to override, whose name is the name of the profile, under the **Cannot Create from Existing** and the **Must Create from Existing** folders. Enter the desired information in each of the specific profile settings. Enter the value you desire for all other profiles in the **All Profiles** setting.

Procedure

1. From the menu bar, click **Administration** > **Settings**.
2. Click **Applications** > **GRCM** > **Add New Wizard**.
3. To enter information that applies to all profiles:
   a) Expand the **Cannot Create from Existing** or the **Must Create from Existing** folder.
   b) Select the **All Profiles** setting and enter the desired information.

4. To enter information for a specific profile, you must first create a setting for that profile under the **Cannot Create from Existing** or the **Must Create from Existing** folder, which has the exact name of the profile. For more information, see “Custom settings” on page 340
5. For **Cannot Create from Existing** settings,enter a comma separated list of object type names, not labels, and click **Save**.
6. For **Must Create from Existing** settings, enter a line for each object type where the format is multiple lines separated by carriage return - line feed, each formatted as `<object system name><colon><starting path>`, and click **Save**. The existing object instances to be used as templates must be located under the starting path specified.

Controlling the default object type in the parent picker in the Add New wizard

You can specify the default object type in the parent picker. For each desired object type, you can specify a series of parent object type defaults; the first type available to this user will be set as the default.

About this task

You can configure globally, for individual profiles, or both:

- To configure globally for all profiles, enter the desired information in the **All Profiles** setting under the **Parent Object Type Preferences** folder.
- To configure individually for each profile, create a setting for each profile, whose name is the name of the profile, under the **Cannot Create from Existing** and the **Must Create from Existing** folders. Enter the desired information in each profile setting.
- To configure a combination of globally but to override that configuration for specific profiles, create a setting for each profile you wish to override, whose name is the name of the profile, under the **Parent Object Type Preferences** folder. Enter the desired information in each of the specific profile settings. Enter the value you desire for all other profiles in the **All Profiles** setting.

It is not necessary to specify this information; the system will choose defaults for any object type or profile not specified.

Procedure

1. From the menu bar, click **Administration** > **Settings**.
2. Click **Applications** > **GRCM** > **Add New Wizard** > **Parent Object Type Preferences**.
3. To enter information that applies to all profiles select the **All Profiles** setting and enter the desired information.
4. To enter information for a specific profile, you must first create a setting for that profile under the **Parent Object Type Preferences** folder, which has the exact name of the profile. For more information, see “Custom settings” on page 340
5. For each object type in the setting, specify the default parent object type to be selected in the Select Parents Narrow By panel. Format is multiple lines separated by carriage return - line feed, each formatted as <object type to be created system name><colon><highest priority object type system name to be parent><comma><second highest priority object type system name to be parent>, and so on, as shown in the following example:

   Resource:SOXBusEntity,RiskSubEntity

   ReviewComment:AuditProgram,Finding,Workpaper

   RiskAssessment:SOXBusEntity

Controlling the default folder for new child objects

You can configure the default folder in which to save child objects that you create. This configuration is critical because the folder determines security access for new child objects.

About this task

You can override the default folder setting when you add new child objects from the FastMap tool.

Procedure

1. From the menu bar, click **Administration** > **Settings** > **Applications** > **GRCM**.
2. Click the **Default Folder** setting to open its detail page.
3. In the **Value** field, type one of the following values:
   - `root_folder`

     Use this value to create new child objects in the root folder for the object type. This option is not recommended.
   - `parent_entity`

     Use this value to create new child objects in the same folder as the lowest level Business Entity of the parent object. Children of self-contained object types are not created in the same folders as their parents.
   - `parent_folder`

     Use this value to create new child objects in or under the folder of its primary parent. This option is recommended. Consider this option in the following circumstances:

     – You are working with self-contained object types.
     – You are working with a security model that includes Business Entity and other object types.
     – You are using helpers or triggers that move saved objects into folders other than the default folders.
4. Click **Save**.

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

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.

About this task

Note that dependent picklist behavior is not supported for custom forms.

Note that if an administrative user creates field dependencies and dependent picklists that create a loop, an error is displayed in the interface that states that "The operation is not allowed because it would result in the following circular dependencies ...". If you are upgrading and you had a loop in the previous version, if you change your configuration you will get an error in the interface that states that "The operation is not allowed because it would result in the following circular dependencies ...".

Attention: When using the bulk update feature, the dependent picklists do not change values when the controlling value changes. Instead, all values from both the controller and the dependent picklist are displayed. Validation of selected values will be done before the objects are saved and any conflicts are reported back to the user.

Figure 15 on page 208 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 15 on page 208, 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.

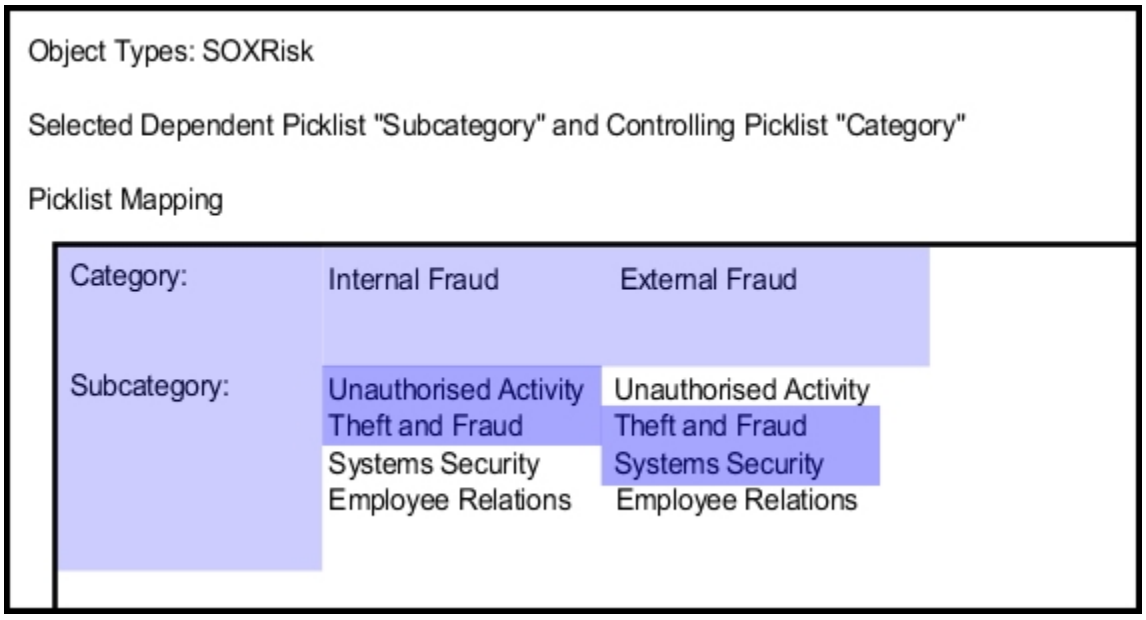


Figure 15: Sample picklist mapping grid

Procedure

1. With the Object Types application permission set, select the **Administration** menu and click **Object Types**.
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. 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.

About this task

Note that if an administrative user creates field dependencies and dependent picklists that create a loop, an error is displayed in the interface that states that "The operation is not allowed because it would result in the following circular dependencies ...". If you are upgrading and you had a loop in the previous version, if you change your configuration you will get an error in the interface that states that "The operation is not allowed because it would result in the following circular dependencies ...".

Procedure

1. With the Object Types application permission set, select the **Administration** menu and click **Object Types**.
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. 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. With the Object Types application permission set, select the **Administration** menu and click **Object Types**.
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) 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

You can delete 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 209.

Procedure

1. With the Object Types application permission set, select the **Administration** menu and click **Object Types**.
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. You can select multiple boxes.
   b) Click **Delete**.

Results

The selected dependent picklist is removed from the list on the **Dependent Picklists** tab.

Excluding fields from a subsystem

IBM OpenPages GRC Platform 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.

For example, 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.

Selecting the fields to exclude

When you exclude a field from a subsystem, the subsystem ignores the excluded field.

The following table identifies that action that occurs when selected fields are excluded:

Table 67: Fields exclusion and results	
Fields excluded from this subsystem	**Results**
Reporting Framework	Any reports (existing or future) that reference these fields fail unless the excluded field is also removed from the report.
Workflow	Existing job type templates that reference these fields 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, refresh the UDA map as follows: • Open the existing job type in edit mode. • Click **Save**. An automatic refresh of the UDA map occurs.

Procedure

1. With the Object Types application permission set, select **Administration** and click **Object Types**.
2. From the list, click the name of the object type to modify.
3. On the **Field Exclusions** pane for object type, click **Exclude**.
4. Complete the following steps on the **Exclude Fields** page:
   a) In the **Select Field** field, select the fields that you want to exclude from the subsystem.
   b) In the **Select Subsystem** field, select the subsystem.
5. 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 - 5.
7. If you excluded fields from the Reporting Framework subsystem, regenerate the reporting framework.
   For more information, see "Updating the reporting framework" on page 686.

Changing the subsystem for an excluded field

You can change the subsystem for individual fields that have been excluded from a subsystem.

Procedure

1. With the Object Types application permission set, select the **Administration** menu and click **Object Types**.
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.
5. Click **Save**.
6. If you modified the list of fields that are excluded from the Reporting Framework subsystem, update the reporting framework.
   For more information, see "Updating the reporting framework" on page 686.

Removing excluded fields

You can remove a field from the list of excluded fields.

When you remove a field from the list of excluded fields, the field is removed from the **Field Exclusions** list for the object type.

Procedure

1. With the Object Types application permission set, select the **Administration** menu and click **Object Types**.
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 remove. You can select multiple boxes.
   b) Click **Remove**.
   c) If prompted, click **OK**.

   The selected excluded field is removed from the **Field Exclusions** list for the object type.
4. If you modified the list of fields that are excluded from the Reporting Framework subsystem, update the reporting framework.

   For more information, see “Updating the reporting framework” on page 686.

Chapter 11. Profiles

Profiles provide end users with a localized view of information that is directly related to their responsibilities.

Use profiles to configure objects, custom forms, fields, and object views. When you change a setting in a profile, the change is dynamic and the change is immediate.

Each user has one or more profiles available to them for their logon session.

You can use profiles to restrict the object types that individual users can view. You can also define 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.

Create profiles by cloning them from existing profiles, then modifying the new profile. A standard profile, called Default, is provided. You can use it as a template to create other profiles. The profiles that you create and assign to users are standalone. No inheritance occurs from one profile to another profile, including the Default profile.

When you associate a profile to a group, all users in the group have that profile added to their Allowed Profiles list. The profile is stored with the user, not the group. If a user is later added to the group, they will not be assigned the profile that was earlier assigned to the users of the group.

You can also designate any profile as the default profile or fallback profile. For more information, see “Setting a default or fallback profile” on page 215.

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. While a user is logged in, you can assign different profiles to the user but you should not change their "Current Profile" or remove it from the list of "Allowed Profiles" because that may result in the user losing unsaved work.
- Users can change from one assigned profile to another themselves. For more information, see "Changing your profile" in the *IBM OpenPages GRC User Guide*.

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 68: Required object types

Object Type	**Label**
SOXBusEntity	Business Entity
SOXSignature	Signature
SOXExternalDocument	Link (this is an external URL link)

Guidelines for working with profiles

Following are some suggested guidelines for working with profiles.

- Create and enable a default profile and a fallback profile before you create any other profiles for users and groups. For more information, see “Setting a default or fallback profile” on page 215.
- Consider designating the most commonly used profile as the default profile.

- Do not disable, delete, or disassociate profiles that users are actively using because it may disrupt their work. In particular, do not do so unless you have created and enabled a fallback profile that users with no other active profile can use to log on.
- Associate one or more new profiles to a user or group before disabling or deleting all of their existing ones.

Accessing profiles

From the detail page of a profile, you can modify profile information, and associate users. You can also 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.

Note: To access the **Profiles** menu item, you must have the Profiles application permission set on your account (for details, see "Types of application permissions" on page 32).

Procedure

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

Creating a profile

You can create a new profile based on an existing profile, including the "Default" profile that is supplied with the product.

Procedure

1. With the Profiles application permission set, select the **Administration** menu and click **Profiles**.
2. On the **Profiles** table, click **Add**.
3. On the **Add Profile** page, type a name for the profile. The name should be easily recognizable by users and identify the purpose for which it is designed. Profile names cannot be translated or changed after they are created.
4. Click **Based on Profile** and select the profile to use as a template for the new profile.
5. If you want the new profile to be the default profile, select **Default**. For more information, see "Setting a default or fallback profile" on page 215).

   Important: Creating a default profile might affect the way IBM OpenPages GRC Platform handles objects and profiles.
6. If you want the new profile to be the fallback profile, select **Fallback**. For more information, see "Setting a default or fallback profile" on page 215).
7. Click **Create**.
8. To configure the profile, do one of the following tasks:

Table 69: Profile configuration tasks

If you want to do this...	**Then see this topic for details...**
associate and disassociate users	"Associating users and groups to a profile" on page 217 "Disassociating users from a profile" on page 218
include and exclude object types	"Including object types in a profile" on page 219 "Excluding object types from a profile" on page 219

Table 69: Profile configuration tasks (continued)	
If you want to do this...	**Then see this topic for details...**
set up a Home page	"Home page" on page 223
configure views for an object type	"Configure views for objects" on page 236

This video demonstrates how to create profiles and add object types and views to a profile:

https://youtu.be/Iylu3p_snfY

Setting a default or fallback profile

You can set default and fallback profiles for users and groups.

Before you create a default or fallback profile, see "Guidelines for working with profiles" on page 213.

You can designate any profile as the default profile for a user or group. Any previously designated profile loses this default designation when you select another profile as the default profile. 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.

When you create users and add profiles, the default profile serves as the profile that is used if no other profile is selected. You do not need to designate a default profile. If no profile is designated as the default profile, the fallback profile will be used.

The fallback profile allows a user who is either not associated with any profile, or whose profile is disabled or deleted, to log on to OpenPages GRC Platform. Only one profile can be designated as the fallback profile. If you choose to designate a profile as the fallback profile, the existing fallback profile (if there is one) loses this designation. The fallback profile is optional, however it's a best practice to designate and enable one so users without any other enabled profiles can log on.

Procedure

1. With the Profiles application permission set, select the **Administration** menu and click **Profiles**.
2. Click the name of a profile. The Detail page opens.
3. On the **Profile Information** table, click **Edit**.
4. On the **Edit Profile** page:
   a) Select one or both of the following options:
      - **Default** - to make this profile the default profile

        Tip: Consider designating the most commonly assigned profile as the default profile for users and groups.
      - **Fallback** - to make this profile the fallback profile
   b) Optionally, enter or change the description of the profile.
   c) Click **Save**.

Associating profiles to users and groups

You can associate one or more profiles to a user or group. Having multiple profiles is beneficial for users that have more than one function and require a different profile for each one. It is also beneficial for administrators because it can reduce the number of profiles that they need to create and maintain.

Tip: It is more efficient to associate profiles to groups rather than individual users. Note that if a user is later added to the group, they will not be assigned the profile that was earlier assigned to the users of the group.

Procedure

1. With the Profiles application permission set, select the **Administration** menu and click **Profiles**.
2. Select the user or group that you want to assign a profile to.
3. Click **Edit**.
4. From the **Allowed Profiles** list, select all the profiles that you want to assign to the user or group.
5. Optionally, you can change the user's current profile by selecting a different profile from the **Current Profile** list.

   Warning: If you change a user's profile while they are logged on you might disrupt their work.

   - If you remove the user's current profile from the **Allowed Profiles** list, the user's current profile is set to the first allowed profile in the alphabetical list.
   - For existing users, the **Current Profile** is set to the user's current profile.
   - For new users, the current profile is set to the default profile, if one exists and is enabled. If an enabled default does not exist, the current profile is set to the fallback profile, if one exists and is enabled. For more information, see "Setting a default or fallback profile" on page 215.
6. Click **Save**. The changes take effect immediately.

Editing a profile

You can modify the description of a profile or designate the profile as the default profile or fallback profile.

Procedure

1. With the Profiles application permission set, select the **Administration** menu and click **Profiles**.
2. Click the name of a profile. The Detail page opens.
3. On the **Profile Information** table, click **Edit**.
4. Make your edits. Note that profile names cannot be translated or changed after they are created.
5. Click **Save**.

Deleting a profile

You can delete a profile.

Important: If you delete a profile, it immediately disappears from the system and you cannot retrieve it. It is immediately unavailable to currently logged in users or to users who subsequently log in. If you are not sure if you might need the profile again, disable it instead.

Before deleting a profile, see "Guidelines for working with profiles" on page 213.

For users with multiple profiles, the current profile becomes the first profile in the alphabetical list of their allowed profiles. If you delete the only profile that is assigned to a user, the user can still log in using the fallback profile if one exists and is enabled. For more information, see "Setting a default or fallback profile" on page 215

Procedure

1. With the Profiles application permission set, select the **Administration** menu and click **Profiles**.
2. Select the box next to each profile you want to delete.
3. On the **Profiles** table, click **Delete**.
4. Click **OK** to delete the profile.

Enabling a profile

When you enable a profile the status of the profile changes from Inactive to Active, and the profile immediately becomes available to users who are assigned that profile (either currently logged on users or to users who subsequently log on).

Procedure

1. With the Profiles application permission set, select the **Administration** menu and click **Profiles**.
2. Click the name of a profile. The Detail page opens.
3. On the **Profile Information** table, click **Enable**.

   The status changes to **Active**.

Disabling a profile

You can disable a profile.

Important: When you disable a profile, it is not deleted. It remains in the system, and the status of the profile changes from Active to Inactive. A disabled profile is immediately unavailable to users to currently logged in users or to users who subsequently log in.

Before disabling a profile, see "Guidelines for working with profiles" on page 213.

For users with multiple profiles, the current profile becomes the first profile in the alphabetical list of their allowed profiles. If you disable the only profile that is assigned to a user, the user can still log in using the fallback profile if one exists and is enabled. For more information, see "Setting a default or fallback profile" on page 215.

Procedure

1. With the Profiles application permission set, select the **Administration** menu and click **Profiles**.
2. Click the name of a profile. The Detail page opens.
3. On the **Profile Information** table, click **Disable**.

   The status changes to **Inactive**.

Associating users and groups to a profile

You can associate users and groups to one or more profiles. Users that have no associated profiles use the fallback profile, if one exists.

For more information, see "Setting a default or fallback profile" on page 215.

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.

When you associate a profile to a group, all users in the group have that profile added to their **Allowed Profiles** list. The profile is stored with the user, not the group. If a user is disassociated from a group, the profile is not disassociated from the user. Note that if a user is later added to the group, they will not be assigned the profile that was earlier assigned to the users of the group.

The profile that you associate with a user is not the current profile unless no current profile is selected.

Table 70: Associating users and groups to a profile	
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 current profile stays the same, and the new profile is added to their list of allowed profiles.
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.

About this task

This task explains how to associate users with a profile on a profile detail page. You can also associate profiles from the **View, Edit, or Disable User** page. For more information, see "Modifying user accounts" on page 28.

Procedure

1. With the Profiles application permission set, select the **Administration** menu and click **Profiles**.
2. Click the name of a profile. The Detail page opens.
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.
   b) Click **Associate**.

   This video demonstrates how to configure multiple profiles for users, and how users can easily switch from one profile to another:

   https://youtu.be/4LTLOf6WUA8

Disassociating users from a profile

When you disassociate a user from a profile, that profile becomes immediately unavailable to that user.

If you disable or disassociate a user from their current profile, one of their available profiles becomes their current profile. If there are no other available profiles, the fallback profile is used. If no fallback profile is assigned, the user is unable to log on to the application. For more information, see "Setting a default or fallback profile" on page 215.

Before disassociating a profile, see "Guidelines for working with profiles" on page 213.

About this task

You can disassociate users from a profile on a profile detail page. Alternatively, you can disassociate users from profiles from the **View, Edit, or Disable User** page. For more information, see "Modifying user accounts" on page 28.

Procedure

1. With the Profiles application permission set, select the **Administration** menu and click **Profiles**.
2. Click the name of a profile. The Detail page opens.
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) Click **OK**.

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. The object types that you select determine which menus appear and the contents of each menu.

Procedure

1. With the Profiles application permission set, select the **Administration** menu and click **Profiles**.
2. Click the name of a profile. The Detail page opens.
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) Click **Include**.
5. To configure views for an object type, see "Configure views for objects" on page 236.

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. It is no longer available to users who are assigned that profile.

Note: Certain object types are required. You get an error message if you try to exclude them.

Procedure

1. With the Profiles application permission set, select the **Administration** menu and click **Profiles**.
2. Click the name of a profile. The Detail page opens.
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) 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. IBM OpenPages GRC Platform stores an excluded object, along with any associated data, in the repository. You can view it through reports.

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.

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 or excluding fields for object types in one profile does not affect object-type fields in other profiles.

Procedure

1. With the Profiles application permission set, select the **Administration** menu and click **Profiles**.

2. Click the name of a profile. The Detail page opens.
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) Click **Include**.

   The included object field now appears in the list of available fields for this object type in this profile.
6. Optional: Configure the object field in a view. Depending on the view, see either "Navigational Views" on page 237 or "Configuring fields in Detail and Activity views" on page 257.

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.

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 or excluding fields for object types in one profile does not affect object-type fields in other profiles.

Procedure

1. With the Profiles application permission set, select the **Administration** menu and click **Profiles**.
2. Click the name of a profile. The Detail page opens.
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) 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 display order of object types

With the exception of the Business Entity object type, you can modify the order in which object types are 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).

Procedure

1. With the Profiles application permission set, select the **Administration** menu and click **Profiles**.
2. Click the name of a profile. The Detail page opens.
3. From the **Object Types** table:
   a) In the box under the **Order** column, change the order value of the object types as wanted.

   The maximum value allowed in the Order field is 999.

b) Click **Update Order**.

The object types in this profile now appear in the new order.

Example

The current display order for the following object types is Business Entity 1, Process 2, Sub-Process 3, and Account 4.

However, if you want to display Account (instead of Process and Sub-Process) after Business Entity, set the order number of Account to 2. When you click "Update Order", the system automatically reorders the Process number to 3 and Sub-Process to 4.

Now, wherever these object types are found together in the application, they appear in the following order: Business Entity 1, Account 2, Process 3, and Sub-Process 4.

Setting a field in a profile to required or optional

You can set a specific field to required or optional for a profile and object type.

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** pane, you must include it before you can modify it (see “Including fields in an object type” on page 219).

Procedure

1. With the Profiles application permission set, select **Administration** from the menu and click **Profiles**.
2. Click the name of a profile. The Detail page opens.
3. In the **Object Types** pane for the profile, click the name of the object type that has the field to modify.
4. In the **Object Fields** pane, click the name of the field to modify (for example, "Description").
5. On the **Object Field Information** pane for the selected field, click **Edit**.
6. In the **Required** field on the edit page, either enable the option to set the field as required or disable it.
7. Click **Save**.

Chapter 12. Managing the Home page, views for objects, and display types

You can manage the display of the Home page, the views for each object type that is included in a profile, and the display types for simple strings, long strings, reporting fragments, and enumerated strings.

Home page

The Home page is the initial page that users see when they log on to the IBM OpenPages GRC Platform 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 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 My Work tab and the Dashboard tab, a tab on a Home page displays the name of the configured report.

The type of tabs that can be configured on the Home page include:

- Cognos reports
- Cognos Workspace reports
- Cognos Analytics dashboards
- Cognos Analytics stories
- JSP Reports
- The My Work tab, which is a Home page tab provided by OpenPages GRC Platform that contains configured panes (sections of a page) for predefined lists, filtered lists, and embedded reports.
- The Dashboard tab, which is a Home page tab provided by OpenPages GRC Platform. Administrators can add tabs that are mandatory and cannot be deleted or altered by users. Users can add panes to the Dashboard tab for quick access to the tasks and information that they use most.

You can control the order in which tabs (including the Dashboard tab and My Work tab) are displayed on the Home page.

For example, a Testers profile might have the following tabs configured: "My Tests - Performer" (report) as tab 1, the My Work tab as tab 2, the Dashboard tab as tab 3, "Test Notifications" (report) as tab 4, and the "FCM Dashboard" (report) as tab 5.

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 My Work tab and the Dashboard tab are both 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 icon on the report tab.
- If the My Work 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 My Work 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 My Work 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.
  ```
- The Dashboard tab on a users Home page displays any panels defined by the administrator plus any panels created by the user. Panels specified as mandatory by the administrator are not editable or removable.

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
- Are any of the selected reports or dashboards already configured for display on the My Work tab. If so, should these be removed?

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 16 on page 224 shows the basic layout of tabs on a Home page.

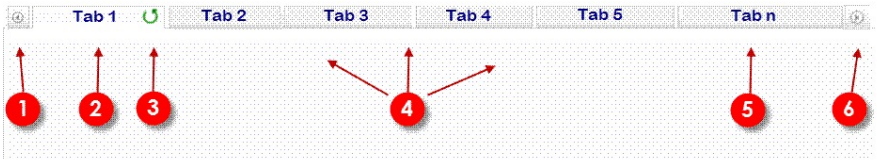


Figure 16: Layout of Tabs on a Home Page

Table 71 on page 224 contains a key to the previous illustration with a brief description of the various Home page elements.

Table 71: 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.

Table 71: Description of Home Page Elements (continued)	
Key	**Description**
2	Active tab. When multiple tabs are configured, only the currently selected tab is highlighted and becomes the active tab.
3	Refresh icon. When clicked, refreshes the data on the selected tab.
4	Inactive tabs. Except for the My Work tab and the Dashboard 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.

Configuring tabs on the home page

To configure tabs on the home page, use the **Home Page Tab Configuration** pane on the detail page of the selected profile.

Table 72 on page 225 describes the information displayed on the Home Page Tab Configuration pane.

Table 72: 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. The My Work tab and Dashboard tab are the default Home page tabs provided by IBM OpenPages GRC Platform and are 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 My Work tab is in position 1 and the Dashboard tab is in position 2. **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 My Work tab and the Dashboard tab cannot be deleted.

For information on localizing display text, see “Localizing application text” on page 281.

Adding tabs for reports or dashboards

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.

Note: For details about configuring the My Work tab, see "Configuring the My Work tab" on page 227.

Procedure

1. Access the **Profiles** page (see "Accessing profiles" on page 214).
2. Click the name of a profile. The Detail page opens.
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) Click **Add**.
5. Optional: Change the order in which tabs are displayed on the Home page (see "Setting the display order of tabs" on page 226).

Setting the display order of tabs

By default, the My Work tab is in position 1 on the Home page, the Dashboard tab is in position 2, and each tabbed report or dashboard that you add is displayed in the order in which it was added. During an upgrade installation, the Dashboard tab is hidden and at the bottom of the tab list.

You can change the order in which tabs (including the My Work tab and Dashboard 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 214).
2. Click the name of a profile. The Detail page opens.
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. Click **Update Order**.

Hiding and unhiding tabs

You can control whether 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 profile.

When you hide or unhide a tab, the following events occur:

- 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 214).
2. Click the name of a profile. The Detail page opens.
3. On the **Home Page Tab Configuration** pane, take one of the following actions in the **Actions** column:

Table 73: Home page tab configuration options

To do this	Click
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 My Work tab or the Dashboard tab from the **Home Page Tab Configuration** table; you can only hide them.

Procedure

1. Access the **Profiles** page (see “Accessing profiles” on page 214).
2. Click the name of a profile. The Detail page opens.
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 My Work tab

The My Work tab is a default tab provided by IBM OpenPages GRC Platform, 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. Predefined lists also includes the My Reports pane, which can be configured with links to reports. For details, see “Configuring predefined lists” on page 228.
- 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 “Filtered lists on the My Work tab” on page 228.
- Embedded Reports - each embedded report is displayed in a separate pane on the My Work tab. For details, see “Configuring reports” on page 230.

You can configure the default settings of the My Work tab for profiles. For more information, see “Home page settings” on page 333.

Note: The My Work tab can be enabled or disabled for a profile but cannot be deleted.

Note: If you disable the Filtered List View for an object type, the **View Details** link (or **Show All** link, in older versions) for that object on the **Home** page might open the wrong view.

Users can personalize the display and order of the panes on their My Work tab. You can control whether this functionality is enabled with the **My Work Home Page Can Be Personalized** setting. The default value is `true`. Upgrading does not change the sort order.

In a first-time installation, the My Work tab is enabled by default, but it is 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

The following table lists the predefined lists that are available for display on the My Work tab.

Table 74: Available Predefined Lists

This predefined list...	Displays this on the Home page...
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.
Report Listing	a **My Reports** pane on the **Home** page for which you can configure links to reports. For embedded reports, see "Configuring embedded reports" on page 231 for details.

Procedure

1. Access the **Profiles** page (see "Accessing profiles" on page 214).
2. Click the name of a profile. The Detail page opens.
3. On the **My Work 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 My Work tab.
   b) Click **Include**. The included items are listed in the **My Work 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 231 for details.

Filtered lists on the My Work 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 My Work tab. For example, if you configured three filtered lists for the My Work 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.

For 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 My Work 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 My Work tab.

  Example

For example, the Risk object type has filtered lists A, B, and C configured for display on the My Work 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 My Work tab.

For each filtered list that you configure on the My Work 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 My Work tab, all filters that are defined for an object type are displayed in a selection list. After you select a filter, it no longer appears in the list of available filters.

The My Work 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 My Work tab.

Configuring filtered lists on the My Work tab

You can configure filtered lists on the My Work tab for object fields or report fragment fields or both.

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.

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 “Tasks to define filters for an object type” on page 190.
- Any report fragment fields and/or object fields that are in addition to the predefined standard IBM OpenPages GRC Platform object fields for that object type. See Chapter 9, “Fields and field groups,” on page 137.

Procedure

1. Access the **Profiles** page (see “Accessing profiles” on page 214).
2. Click the name of a profile. The Detail page opens.
3. On the **My Work Tab Configuration** table, click **Configure Filtered List**.
4. On the **Select a Filter** page, select a filter from the list and click **Next**.
5. On the **Select Fields** page, do any of the following:

Table 75: Summary of Filter Actions

Goal	Action
Include a field as a column in the filtered list	On either the **Included Object Fields** or **Included Reporting Fragment Fields** table, complete the following steps: a. Click **Include**. This opens a field selection page. b. Select the box next to each field you want to display as a column. c. Click **Include**.

Table 75: Summary of Filter Actions (continued)	
Goal	**Action**
Exclude a field as a column	On the **Included Object Fields** or **Included Reporting Fragment Fields** table, complete the following steps: a. Select the box next to each field you want to remove as either a column or report. b. Click **Exclude**.
Change the order in which object fields are displayed as columns	On the **Included Object Fields** table, complete the following steps: a. In the **Order** column, change the order number of the field you want. b. 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, complete the following steps: a. Click **Include**. This opens a field selection page. b. Select the box next to each report fragment field that you want to display. c. Click **Include**.

6. Click **Finish**.

Editing filtered lists on the My Work 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 214).
2. Click the name of a profile. The Detail page opens.
3. On the **My Work 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 My Work tab” on page 229).
5. Click **Finish**.

Configuring reports

You can use the following methods to configure reports on the My Work 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” on page 231.
- **Embedded reports** - this method embeds each specified report in a separate pane on the My Work tab. For details, see “Configuring embedded reports” on page 231.

Note:

- Only published reports are displayed in the list of available reports (under the Cognos folder) for association on a My Work tab (either as a link in a list or as an embedded report). If you want to add a new report, you must first publish that report. For details, see “Adding reports” on page 113.

- Although JSP reports are available for selection as embedded reports on the My Work tab, only Cognos reports can be embedded (JSP reports cannot be embedded) on the My Work tab. A JSP report that is selected as an embedded report will result in a reporting error on the My Work tab.

Configuring a My Reports listing

You can configure links to reports in the My Reports pane on the My Work tab by either clicking the **Add Predefined List** icon or through the wizard by clicking the **Configure Reports** icon.

You can globally control the maximum number of reports that are listed on the My Work tab through the **Maximum Reports Listing** setting (for details, see "Maximum reports allowed on the home page" on page 336).

Procedure

1. Access the **Profiles** page (see "Accessing profiles" on page 214).
2. Click the name of a profile. The Detail page opens.
3. On the **My Work Tab Configuration** pane, take one of the following actions:

Table 76: My work table configuration options

Option	Steps
Add Predefined Lists	On the **Available Predefined Lists** page, click **Add Predefined Lists**: a. Select **My Reports** b. Click **Include**. c. On the **My Work Tab Configuration** pane, click the **My Reports** link. d. Continue to Step 4. **Note:** If you already added a **My Reports** pane on the My Work tab but need to populate the list with reports, do not click the icon and skip directly to Step 4.
Configure Reports	In the Configure Home Page Reports wizard: a. In the **Select Report Type** step, select **My Reports** as the report type. b. Click **Next**. c. Continue to Step 4.

4. Click **Associate** to open the Reports list page.
5. On the **Reports** list page, select each report to include as a link in the **My Reports** pane. Then, click **Associate**.
6. Click **Finish**.

Configuring embedded reports

When you embed a report on the My Work tab, the report is displayed in a pane on the My Work tab of users who have the selected profile.

Use the following steps to embed reports on the My Work tab.

Note: You may need to modify the report to accommodate differences in the My Work tab display area and page targets. Make a copy of the report before you update the display details and targets to suit rendering within the My Work tab display area.

You can globally control the maximum number of embedded reports to show on the My Work tab through the **Maximum Embedded Reports** setting. For more information, see "Maximum number of embedded reports on the home page" on page 335.

About this task

There are performance considerations when working with embedded reports. Although embedded My Work tab reports provide a convenient mechanism to present users with useful Cognos report data upon logon to IBM OpenPages GRC Platform, report execution times can vary depending on the report.

When configuring embedded reports, administrators should be careful not to configure the My Work tab with large or resource-intensive reports, as this will contribute to the overall load on Cognos resources. Some factors that can affect utilization of Cognos 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 My Work 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 My Work tab for the majority of application users.

Procedure

1. Access the **Profiles** page (see "Accessing profiles" on page 214).
2. Click the name of a profile. The Detail page opens.
3. On the **My Work 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 My Work tab.
   b) When finished, click **Associate** (you may need to scroll down to see the icon).

      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) Click **Disassociate**
8. Click **Finish**.

Modifying configured reports

Use the Configure Reports wizard to add or remove reports (both embedded reports and My Report links) from the My Work tab.

Note: You can also remove embedded reports from the **My Work Tab Configuration** pane. For more information, see "Removing items from the My Work tab" on page 233.

Procedure

1. Access the **Profiles** page (see “Accessing profiles” on page 214).
2. Click the name of a profile. The Detail page opens.
3. On the **My Work Tab Configuration** pane, click **Configure Reports**.
4. In the **Select Report Type** field, select the report type that you want to modify.
5. On the **Associated Reports** page, take one of the following actions:

Table 77: Add or remove reports

Task	Procedure
Add more reports	a. Click **Associate**. b. On the **Reports** list page, select each report to include. c. Click **Associate**.
Remove existing reports	a. Select each report to remove. b. Click **Disassociate**.

6. Click **Finish**.

Removing items from the My Work tab

You can remove previously configured tables (including embedded reports) from the My Work tab.

When a user with the modified profile either logs on to the application, refreshes or returns to the My Work 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 232.

Procedure

1. Access the **Profiles** page (see “Accessing profiles” on page 214).
2. Click the name of a profile. The Detail page opens.
3. On the **My Work Configuration** table listing:
   a) Select the box next to each item you want to remove from the My Work tab.
   b) Click **Disassociate**.

Configuring users' Dashboard tabs

The Dashboard tab allows users to create their own dashboard for their Home Page by adding panels and widgets. The configuration of a user’s Dashboard tab is saved in the database and not in the web browser cache. This means that a user can clear the cache, switch to a different browser, or log in from a different computer without changing the configuration of the Dashboard tab.

Users can add new panels to their Dashboard tabs and for each panel add as many of the following types of widgets as needed:

- Filter Count widget, which appears in a user's dashboard panel as the object type name and a number representing the number of filters applied. When a user clicks the number of filters, the Filtered List View page for that object type is opened. If a filtered list for that object type does not exist, then the Filtered List View page will not be opened.
- Object Global Search widget, which appears in the user's dashboard panel as the object type name followed by a search box. When a user enters a search term in the box, for example Accounts Receivable, the Search Results page provides a list of results.

- Static Web Link widget, which appears in a user's dashboard panel as a clickable link with the label that was provided for the widget. When creating this widget, users must begin the URL with the protocol, such as http://.
- Add New widget, which creates an **Add New** button that is preconfigured for a specific object type. Clicking the button, displays the Add New dialog box for that object type.

For each profile, administrators can add panels to a default Dashboard tab that is displayed for users who are logging on to OpenPages for the first time.

Administrators can specify that a panel is locked and cannot be changed by users. Administrators lock a panel by selecting the **Lock panel contents** check box in the **Create New Panel** window. When a locked panel is saved, it is automatically pushed to all users in the profile the next time they log into OpenPages. Administrators can also create panels that are unlocked, and these panels will be included in the default Dashboard tab for users who are logging on to OpenPages for the first time. Users can edit or delete unlocked panels in their own Dashboard tabs.

Both the Dashboard tab and the My Work tab will be present on a user's Home page unless specified as hidden by an administrator in the profile configuration. Clicking the Home button in the global header will return the user to either the Dashboard or My Work tab, depending on which tab was opened most recently.

Administrators can export the configuration of a default Dashboard tab in JSON format. This can be useful when migrating from one environment to another. For more information, see "Exporting the configuration for a dashboard tab" on page 236.

Note: If the Global Search component is not enabled, then the Global Search widget is not available for users to add to their Dashboard tabs. If you disable the Global Search component for a profile, then any existing Global Search widgets are removed from users' Dashboard tabs the next time they log on to OpenPages. If you disable the Global Search component for an object type, then any Global Search widgets for that object type will be removed from users' Dashboard tabs. The Static Web Link widget type is always available, but the other widget types will only be available if users in the profile have access rights to the object type related to that widget type. If access rights are revoked for widget types that users have already placed on their Dashboard tabs, then those widgets will be removed the next time the users log on to OpenPages. Similarly, if the Add New capability is disabled for an object type that users have associated with a widget on their dashboard, then that widgets will be removed the next time the users log on.

Creating content for users' Dashboard tabs

For each profile, administrators can create content on a default Dashboard tab that is displayed for users who are opening the application for the first time. Administrators can also specify that a panel is locked. When a locked panel is saved, it is pushed to the Dashboard tab for all users in the profile and cannot be edited or removed by users.

Note: If the Global Search component is not enabled, then the Global Search widget is not available for users to add to their Dashboard tabs. If you disable the Global Search component for a profile, then any existing Global Search widgets are removed from users' Dashboard tabs the next time they log on to OpenPages. If you disable the Global Search component for an object type, then any Global Search widgets for that object type will be removed from users' Dashboard tabs. The Static Web Link widget type is always available, but the other widget types will only be available if users in the profile have access rights to the object type related to that widget type. If access rights are revoked for widget types that users have already placed on their Dashboard tabs, then those widgets will be removed the next time the users log on to OpenPages. Similarly, if the Add New capability is disabled for an object type that users have associated with a widget on their dashboard, then that widgets will be removed the next time the users log on.

Procedure

1. Log on to IBM OpenPages GRC Platform as a user with the Profiles application permission set.

2. From the menu bar, select **Administration** and click **Profiles**.
3. Click the name of the Profile for which you want to create a default Dashboard tab.
4. From the menu bar of the Profiles detail page, click **Home Page Tab Configuration**.
5. In the Dashboard row, click **Edit**.
6. To add a panel, click **Create New Panel**.
7. In the **Create New Panel** window, type a title for the panel. The name for the panel must be unique. If a user in the profile already has a panel with same name, the name of the user panel is changed. For example, if you create a panel called My Panel and the user already has a panel by that name, the user panel is renamed to My Panel(1).
8. Under **Panel Widgets** select a widget type.

   You can add as many widgets as you want by clicking the **Add New Widget** button and specifying the object type for each widget. The order of widgets in the panel can be changed by dragging them up or down.
9. When you are finished adding and arranging the order of widgets, click the **Create Panel** button.
10. To change the layout of panels in the default Dashboard tab, you can use drag and drop.
11. Click **Done Editing**.

Results

When you save a locked panel, it is pushed to the Dashboard tab of all users in the profile and will appear the next time that they log on to OpenPages. In order for the change to occur for all users in the profile, all users must log on to OpenPages after the profile change.

To edit or delete a panel, administrators and users can hover their mouse pointers over the panel and click the edit or delete icon. Users are not able to edit or remove locked panels. When users hover their mouse pointers over locked panels, the edit and delete icons are not available to them.

When you save a panel that is not locked, it appears only on the default Dashboard tab that users see when they open the application for the first time. Unlocked panels are not pushed to users' Dashboard tab. They can be edited or removed by users.

Editing the content of users' Dashboard tabs

For each profile, administrators can edit content on a default Dashboard tab that is displayed for users who are opening the application for the first time. Edits to the default Dashboard tab will not affect the Dashboard tab for existing users unless a panel is locked. If an administrator specifies that a panel is locked, then that panel is pushed to the Dashboard tab for all users in the profile and cannot be edited or removed by users.

Procedure

1. Log on to IBM OpenPages GRC Platform as a user with the Profiles application permission set.
2. From the menu bar, select **Administration** and click **Profiles**.
3. Click the name of the Profile for which you want to edit a default Dashboard tab.
4. From the menu bar of the Profiles detail page, click **Home Page Tab Configuration**.
5. In the Dashboard row, click **Edit**.

   You can perform the following tasks:

   - To add a new panel to the default Dashboard tab, click **Create New Panel**. For more information, see “Creating content for users' Dashboard tabs” on page 234
   - To edit an existing panel, hover your mouse pointer over the title bar of the panel and click the pencil icon. You can change the title of a panel by clicking the title and typing a new name.
   - To delete a panel, hover your mouse pointer over the title bar of the panel and click the trash can icon.

- To make a panel mandatory for all users in the profile and push it to their Dashboard tab, select the **Lock Panel Contents** check box. When you save the panel, it is pushed to users' Dashboard tabs and will appear the next time that they log on to OpenPages, and users will not be able to edit or remove it. Panels that are not locked can be edited and removed by users.

6. Click **Done Editing**.

Exporting the configuration for a dashboard tab

Administrators can export the configuration of a default Dashboard tab in JSON format. This can be useful when migrating from one environment to another.

Procedure

1. Log on to IBM OpenPages GRC Platform as a user with the Profiles application permission set.
2. From the menu bar, select **Administration** and click **Profiles**.
3. Click the name of the Profile for which you want to export the configuration of the default Dashboard tab.
4. From the menu bar of the Profiles detail page, click **Home Page Tab Configuration**.
5. In the Dashboard row, click **Edit**.
6. Click the **Download JSON** button, and open the JSON file in a text editor.

   If the Dashboard tab uses multibyte characters, you must use a text editor that supports UTF-8, such as Notepad or Microsoft Word. If you open the JSON file in Microsoft Wordpad, the multibyte characters might not display correctly.

Configure views for objects

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 different formats and provides a means for customizing and filtering information on a page for objects and custom form objects.

The following list summarizes the standard views that you can configure. IBM OpenPages GRC Platform categorizes views as follows:

Navigational Views

- Overview Pages
- Folder View
- Filtered List View
- Grid View

Object Views

- Detail View
- Activity View

Association Views

- List View
- Context View

Creation Views

Note: If you enable a navigational view for the Process Diagram, Data Input, or Data Output object type, it is not available as a menu item for users who are associated with that profile. These objects are available only in the context of a Process.

For information about configuring specific object types in a profile, see “Including object types in a profile” on page 219.

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 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 OpenPages GRC Platform application. Changes that you effect for one profile do not result in changes to other profiles.

For example, 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 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.

Navigational Views

Navigational Views assist users in finding instances of specific objects.

Navigational views include the following view types:

- Overview
- Folder
- Filtered List
- Grid

When you add, remove, or modify Navigational Views in a profile for a specific object type, consider the following items:

- Views can be enabled or disabled.

  Note: If you disable the Filtered List View for an object type, the **View Details** link (or **Show All** link, in older versions) for that object on the **Home** page might open the wrong view.
- Some views can be deleted.
- Most views, except Overview pages, can be reordered.
- The **Bulk Update** feature can be used with grid views because grid views contain editable fields.
- Users with the assigned profile who are already logged on to the application must log out and log in to see the changes.
- Users can change the sort order and field order in Filtered List Views and Grid Views.
- Users cannot add the primary parent hierarchy or business entity hierarchy fields to a Navigational View for any object type.

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.

As an administrator, you can:

- Control which object types are included or excluded in the object-tree hierarchy on an Overview page (see “Including object types on an overview page” on page 247 and “Excluding object types from an overview page” on page 247 for details)
- Enable or disable an Overview page for an object type (see “Configure views for objects” on page 236 for details)

An Overview page is not supported for the following object types: SOXProject, SOXDocument, SOXExternalDocument, SOXMilestone, SOXIssue, SOXTask, SOXSignature, and ProjectActionItem.

Folder views and Filtered List views

A **Folder view** displays a page view of folders (including sub-folders) containing the selected object type. The information is displayed in columns on the page.

A **Filtered List view** displays a page with search filter options that you can use to display objects of the same type that match your search criteria. First, select the object type to view. Then, select the **Filtered List view** from the Filter selector. The view is then populated with objects that match the filter criteria. Use this view to display filter objects of the same type that match the search criteria in the filter the user selects. The user can personalize the display of a Filtered List view and limit what fields of information are displayed.

For Filtered List and Folder views:

- The **Name** field is required. Always configure it in the first column.
- If report fragment fields are configured, the Reports column is always the last column in the table. The position of the Reports column can be changed in Grid View.

Example

If you previously disabled the Folder view and Filtered List view pages for Control Objectives in a profile, and you 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 perform the following functions:

- Control which fields are displayed as table column headings in a Folder or Filtered List view (see “Navigational Views” on page 237)
- Set the order in which table column headings appear (see “Setting the display order of fields in a view” on page 243)
- Enable or disable a Folder or Filtered List view page for an object type (see “Configure views for objects” on page 236 for details)
- Control which view page (Folder or Filtered List view) is displayed first to users when both views are configured (see “Setting a default view” on page 242 for details)
- Control whether users can edit fields in the Filtered List view (“Editable fields in a Filtered List View” on page 340 for details)

Grid views

The grid view allows you to select how information about an object is displayed by selecting an option from the View selector.

A grid view allows users to view, compare, and edit fields from up to three different object types in one location. A grid view allows users to perform operations on multiple objects at the same time. Additionally, users can personalize the information by modifying the fields that are displayed, field order, sort criteria, and column widths.

The grid view allows users to move between the display of objects fields in full mode and compact mode. This ability allows the user to show all configured fields for an object or display only the subset that you select. You define the objects that are displayed on a grid view. Users can then select a grid view and edit the fields in the view, including reordering columns of information.

Use the **Grid Actions** menu to create an item, update multiple items (bulk update), export information, delete, lock, and unlock.

The grid view provides access to an Info Card. The card displays the values for all configured fields for an object type.

If users are allowed to edit fields in an object, define a grid view. Because grid views have editable fields, you can use the **Bulk Update** feature.

For information about creating grid views, see “Creating a Grid view ” on page 248

Object views

Object Views provide detail instance data for an object.

Object Views include the following 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. Object views can be enabled or disabled. Some object views can be deleted.

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.

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. You can configure the **Detail View** or any **Activity View** to be the page that users see by default when they click the linked name of an object from an Overview, Folder, Filtered List, or List View page.

Fields can be object fields, computed fields, and 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 a spreadsheet, the data that is directly exported corresponds to the fields that are configured in a Detail view for the selected object type with the exception of Long String fields that have a large sub type. Fields with a large sub type are ignored by Export and FastMap as these fields might be too large to be stored in a cell (the maximum storage for a cell is 32 KB).

As an administrator, you can:

- Control which fields are displayed in the table rows of a Detail view (see “Configuring fields in Detail and Activity views” on page 257)
- Set the display order of the fields (see “Setting the display order of fields in a view” on page 243)
- Set specific fields to be view only or editable (see “Setting object fields as read-only or editable” on page 260)
- Set specific fields to span the 2-column table layout of the Detail page (see “Spanning table columns” on page 260)
- Insert section headings on a page to delineate a set of fields (see “Inserting section headings” on page 258)
- Configure how report fragment fields are displayed to users (see “Configuring the display type for reporting fragment fields” on page 261)
- Configure how string data is displayed to users (see “Configuring display types for simple string fields” on page 262)

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).

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). 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 on the object's detail page. Users who are assigned the selected profile have immediate access to the new Activity View.

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.

For more details on using Activity Views, see "Creating Activity Views" on page 250.

As an administrator, you can:

- Create, modify, or delete Activity Views (see "Creating Activity Views" on page 250)
- Control which fields are displayed in the table rows of an Activity View (see "Configuring fields in Detail and Activity views" on page 257)
- Set the display order of the table rows containing the fields (see "Setting the display order of fields in a view" on page 243)
- Set specific fields to be view only or editable (see "Setting object fields as read-only or editable" on page 260)
- Set specific fields to span the 2-column table layout of the activity page (see "Spanning table columns" on page 260)
- Insert section headings on a page to delineate a set of fields (see "Inserting section headings" on page 258)

Association views

Users with the assigned profile can use Association Views to view a page that displays parts of another pages.

Association Views include the following 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.

List views

A **List view** displays objects of the same type in a list format, with objects listed in ascending order. Depending on the object type, list views can be displayed as either a page or a pane.

By default, list views are displayed as pages for the following object types: Business Entities (SOXBusEntity), Milestones (SOXMilestone), Milestone Action Items (SOXTask), and as panes on a Detail view page for listing associated parent or child objects.

If you have a Folder or Filtered List view for Business Entities, the default list view for this object type is not used.

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.

For list views:

- 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.
- Set the display order of the table column headings.

Context panes
A Context pane appears in the Detail page for an object and provides information about the object that is the focus of the Detail page. When you are looking at the details of associated objects, use the Context pane to remind you of the key information about the object that is the focus of the Detail page.

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 in a Context pane (see "Including and excluding fields in navigation and association views" on page 245)
- Set the display order of the fields (see "Setting the display order of fields in a view" on page 243)

Creation views

Creation views allow you users to add new objects using the Add New wizard.

In previous releases, the layout of the Add New wizard was driven by a single view definition, either an Activity View that is named Add New, or the Detail view. There was also no way to associate existing child objects to the object that is being created without a separate step.

Now, a category of view that is called Creation views allows the definition of multiple Add new view definitions for a single object type for a single profile.

For more information on using Creation views, see "Creating a Creation view" on page 256

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 214).
2. Click the name of a profile. The Detail page opens.
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. Optional: Configure the selected view:
   - To add or remove object types for display in an object-tree hierarchy on an Overview page, see "Including object types in a profile" on page 219 for details.
   - To add or remove fields for a specific view, see "Excluding object types from a profile" on page 219.
   - To control which view is displayed first to users when multiple views for a page are configured, see "Setting a default view" on page 242 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 and Grid view pages" on page 248 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.

About this task

- 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**, **Filtered List View**, and **Grid View** - when you disable these views, 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.

  Note: If you disable the Filtered List View for an object type, the **View Details** link (or **Show All** link, in older versions) for that object on the **Home** page might open the wrong view.

Procedure

1. Access the **Profiles** page (see “Accessing profiles” on page 214).
2. Click the name of a profile. The Detail page opens.
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

- 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. 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.

For example, if you have a Grid View, Folder View, and Filtered List View enabled for Control object types, you could set the Grid View page to display first when users select **Control** from the **Assessments** menu.

Procedure

1. Access the **Profiles** page (see “Accessing profiles” on page 214).
2. Click the name of a profile. The Detail page opens.
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.
6. To view the changes to the default view, users must log out and log back in to the application.

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 report fragment fields.

Note: The following field limitations apply 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.

When you reorder fields in a view, the change is immediately displayed 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 214).
2. Click the name of a profile. The Detail page opens.
3. From the **Object Types** table listing, click the name of the object type you want to modify.
4. Select one of the following views and complete the steps identified:

Table 78: Views

Navigate to this tab...	**To select a link for this view...**
Navigational views	**Folder**, **Filtered List**, or **Grid** If **Grid Views** are defined, click the name of a grid view link, and then click **Next** until the Specify Field Settings screen is displayed in the Grid View wizard.
Association views	**List** or **Context**
Object views	**Detail** or **Activity**. If **Activity Views** are defined, click the name of an activity view link, and then click **Next** until the **Specify Field Settings** pane is displayed.

5. On the **Included Object Fields** table, locate the field to change:
   a) In the **Order** field 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**, click **Next** and **Save**.

The fields are automatically reordered as specified.

e) For **Grid Views**, click **Save** .

The fields are automatically re-ordered as specified.

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.

Copy views for an object from one profile to one or more other profiles

You can copy the object views (Detail View and Activity View) and creation views for an object from one profile to one or more other profiles.

About this task

To access the Profiles menu item, you must have the **Profiles** application permission set on your account. For more information, see “Types of application permissions” on page 32.

Before you copy a view, keep the following points in mind:

- If an object in the source profile is missing from the target profile, the copy operation will not be successful.
- If fields, field groups, or filters in the source profile are missing from the target profile, they will be added to the target profile by the copy operation.
- Field properties for the object that you selected, such as display type and whether a field is required, are retained when the copy operation is complete. When fields are added to the target profile by the copy operation, they have the same properties as they have in the source profile.
- Fields that are related to the view but not included in it, are not automatically added to the target profile by the copy operation. For example, suppose that the view that you are copying has dependent fields. Unless the view also includes the controlling fields, the dependent fields are not copied to the target profile. As a result, the user of the target profile might have no way to set the value of the controlling fields, and dependent field behavior (Visible, Required, or Editable) might not work as expected. If the view you are copying has any controlling fields that are not included in the view, you should first determine whether those fields are included in the target profile. If they are not, determine whether you want to manually add them to the target profile. For more information, see “Modifying controllers for a dependent field” on page 200 and “Configuring dependent picklists” on page 207.
- If the view already exists in any of the target profiles, and you proceed with the copy, the existing view in the target profile is overwritten by the copied view. If the overwritten view was disabled or set as the default view in the target profile, it is still disabled or set as the default view when the copy operation is complete. The order of the overwritten view does not change in the target profile.
- If a view with the same name but of a different view type exists in the target profile, the view is not copied.
- Filters that are associated to the source view are copied to the target view. If you want the filters to be available in the Filtered List View or Home page in the target profile, you must manually add them. For more information, see “Tasks to define filters for an object type” on page 190.

Procedure

1. Enable System Admin Mode. For more information, see “Enabling and disabling System Administration Mode” on page 17).
2. Click **Administration** > **Profiles**.
3. Click the name of the source profile that includes the object with the view that you want to copy.

4. Click the name of the object that you want to copy views to.
   The **Profile** page for the object opens.
5. Click the **Object Views** or **Creation Views** tab, depending on which type of view you want to copy.
6. Click the **Copy** link beside the source view that you want to copy.
7. Select one or more target profiles to copy the source view to.
8. Click **Validate** to verify that the object types and fields exist in the target profiles that you selected.
   The **Validate** tab shows any warnings and errors.
   - If there are no issues, a checkmark  is displayed.
   - If fields, field groups, or filters that are in the source profile will be added to the target profile, an information message  is displayed.
   - If the view already exists in any of the target profiles, a warning  is displayed.
   - If an object in the source profile is missing from the target profile, an error  is displayed.
9. Click **Copy**.
10. Click **Done**.
    The **Results** tab displays the results of the copy operation.
    - If the copy was successful, a checkmark  is displayed. The view is copied to the target profiles that you selected.
    - If the copy was unsuccessful because one or more objects are missing from the target profile, an error  is displayed.

Including and excluding fields in navigation and association views

For each **Folder**, **Filtered List**, **List View**, **Grid View**, and **Context** pane that you configure for an object type within a profile, you can include, exclude, and set the order of fields. When you include or exclude object fields in a Folder, Filtered List, List, Context, Activity, or Grid view, the change immediately affects all users who are assigned that profile.

Fields can be object fields, computed fields, and 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 object types on an overview page” on page 247 and “Excluding object types from an overview page” on page 247for details.
- For Detail and Activity view pages, see “Configuring fields in Detail and Activity views” on page 257 for details.

For information and examples about these views, see the following topics:

- **Filtered List** and **Folder views** - see “Folder views and Filtered List views” on page 237
- **List views** - see “List views” on page 240
- **Context panes** - see “Context panes” on page 241
- **Grid views** - see “Folder views and Filtered List views” on page 237

Including fields in views

Before you can include an object field or reporting fragment field in a Navigational or Association view, the field must be visible in the object field or reporting 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 "Including fields in an object type" on page 219.

When you include object fields or reporting 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 reporting fragment fields is called Reports.

About this task

For List and Folder views, the user cannot adjust the column width or configure which columns will appear. It is a good practice to limit the number of columns you configure for those views.

For Grid and Filtered List views, the user can adjust the column width and can configure which columns are visible.

Procedure

1. Access the **Profiles** page (see "Accessing profiles" on page 214).
2. Click the name of a profile. The Detail page opens.
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 that you want.
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) 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 243.

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 214).
2. Click the name of a profile. The Detail page opens.
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 that you want.
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) Click **Exclude**.

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 GRC Platform 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 214).
2. Click the name of a profile. The Detail page opens.
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) 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 GRC Platform services.

For 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 OpenPages GRC Platform 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 214).

2. Click the name of a profile. The Detail page opens.
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: 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) Click **Exclude**.

Associating filters to Filtered List view and Grid view pages

When you associate a filter to a Filtered List View or a Grid View, the filter is displayed in the filter selector for that object type. By using a filter, you can narrow the scope of data that is returned in a Filtered List View or a Grid View for users who are assigned a specific profile.

Important: Before you can associate an object-specific filter to a Filtered List view or Grid View page, you must create a public filter for that object type by following the instructions in "Tasks to define filters for an object type" on page 190.

Procedure

1. Access the **Profiles** page (see "Accessing profiles" on page 214).
2. Click the name of a profile. The Detail page opens.
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. Complete the following actions:
   a) On the **Associated Filters** tab, click **Associate**. The filters selection page is displayed.
   b) Select the box next to each filter that you want to include.
   c) Click **Include**.

Disassociating filters from Filtered List view and Grid view Pages

If you have a filter that is no longer appropriate for display in the filter selector on a Filtered List view page or a Grid view page for an object type, you can remove it from the list.

Procedure

1. Access the **Profiles** page (see "Accessing profiles" on page 214).
2. Click the name of a profile. The Detail page opens.
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**.

Creating a Grid view

In IBM OpenPages GRC Platform, you can create a grid view of an object for the users who are assigned to a profile. You specify the fields that are editable so that users can perform a certain task, such as entering KRI values or performing a self-assessment update. Additionally, you can provide guidance in the grid view to these users.

About this task

The process of creating a grid view includes the following steps:

- Provide details about the grid view.
- Optionally, select the related objects that contain fields of information that the user will require to perform the task.
- Specify the settings for the object types.
- Configure fields for the grid view.

Procedure

1. Click **Administration** > **Profiles** and select a profile.
2. Select the object that will be at the root of the grid view.
3. Under **Navigational Views**, click **Add New**.
4. To provide details about the new grid view, complete the following actions:
   a) Add a name and description. Optionally, enter the translations for the name. The description is for administrators only.
   b) Add guidance to the users who are assigned to the profile, such as the methodology that the users should follow in performing the task. You can format the text.
   c) If the grid view is not ready for users to access now, clear the **Enabled** check box. The new grid view is enabled by default.
   d) Click **Next**.
5. If you want to select the related objects that contain fields of information that the user will require to perform the task, complete the following actions:
   a) Click **Choose Object Type**.
   b) Select an object type for the selected object.
   c) Click **Apply**.
   d) Repeat these steps for each object that you want to add.
   e) When you have added all the related objects, click **Next**.

   The related objects do not have to be direct child objects. You can skip levels. For example, the object model may be Process --> Risk --> Control --> Test Plan --> Test Result. You create a grid view that is Process --> Control --> Test Result.

   If you do not want to include related objects, just click **Next**.

   Note: Descendants of recursive object types, such as Business Entity, appear under all of their ancestors, not just the most immediate ancestor. For example, if the path is set to Business Entity/Preference and the hierarchy of objects is North America Division/US Region/Pref1, Pref1 appears as a descendant of both North America Division and for US Region.
6. If there are at least two paths between the selected objects, select one or more paths that you want to use.
7. To specify the sort criteria for the object, complete the following actions:
   a) Click **Specify Sort Criteria**.
   b) Click or Ctrl+click the fields and click the double arrow (>>).
   c) To change the order in which the fields appear, select the field and use the up arrow or the down arrow.
   d) To change how the fields are sorted, select each field and click the up triangle or the down triangle.
   e) Click **Apply**.
8. To apply a filter to the objects, complete the following actions:
   a) Click **Choose Filter**.
   b) Select a filter that was created for this object.
   c) Click **Apply**.

9. Click **Next**.
10. To configure fields for the grid view, complete the following actions:
    a) To select the fields that will be displayed, click **Choose Fields**, select the fields, and click **Apply**.
    b) To allow your users to control which fields are available in the grid view, select **Full Mode** to see the field available in the grid view for an object.

       Compact Mode is a subset of the fields that appear in Full Mode. For example, your users may want to hide the Description field in Compact Mode. To select **Compact Mode**, you must select **Full Mode** first to enable Compact Mode.

       All included fields will appear in the Info Card. A field with neither **Full Mode** nor **Compact Mode** selected will not appear in the grid view but it will be available for the user to make visible.
    c) To change the order in which the fields appear, drag the fields to a new location or change the sequence of numbers in the **Order** fields and click **Update Order**.
    d) Specify whether each field is **Read-Only**.
    e) To change the default column width for the fields, change the numbers in the **Column Width** fields.
    f) To delineate a set of fields on the Info Card, click **Insert Section** and enter a name for the section heading. In the **Insert before** field, select the field that the section heading will appear before. If you have translated text for the section heading, add it to each language as required. Click **Apply**.
    g) Repeat these steps for each additional object type that you have included.
11. Click **Finish**.

Results
The grid view is added to the list of navigational views, where you can make it the default navigational view, have it appear higher in the list of navigational views, disable or enable it, or delete it.

Creating Activity 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.

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 “Tasks to define filters for an object type” on page 190.)

Scenario

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.

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 icon to start the Activity View Wizard.

Table 79 on page 251 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 79: 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 254)	In the **Name** field, type the name: *Control Assessment by Risk Activity.* (For layout refer to pane "3" in Figure 17 on page 253.)
2. Select Object Types (for details, see "Task 2: Select object types" on page 254)	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 17 on page 253.) 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 17 on page 253.) **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: Specifying object type settings" on page 254)	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 17 on page 253.)

Table 79: Configuring a Sample "Control Assessment by Risk Activity" View (continued)	
On this screen in the Activity View Wizard...	**Do this...**
4. Specify Field Settings (for details, see "Task 4: Specify field settings" on page 255)	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 17 on page 253.) – 1 Description – 2 Inherent Risk Rating – 3 Category – 4 Subcategory • **Control** (mostly Read-only fields. For layout refer to pane "6" in Figure 17 on page 253.) – 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 17 on page 253.) – 1 Description – 2 Performed By – 3 Reviewed By – 4 Reviewer Conclusion – 5 Date Performed – 6 Test Result – 7 Exceptions – 8 Exception Description
5. Define Listing Columns (for details, see "Task 5: Define listing columns" on page 255)	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 17 on page 253.)

After the "Control Assessment by Risk Activity" view is saved, it becomes available as a selection in the **Current View** selection list on the Risk object detail page.

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.

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 17 on page 253 shows the basic layout of an Activity view page.

The panes labeled "1" and "2" in Figure 17 on page 253 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 17 on page 253 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 17 on page 253). Depending on the configuration, fields in the top-level object pane and in the hierarchical panes can be Read-only and/or editable.

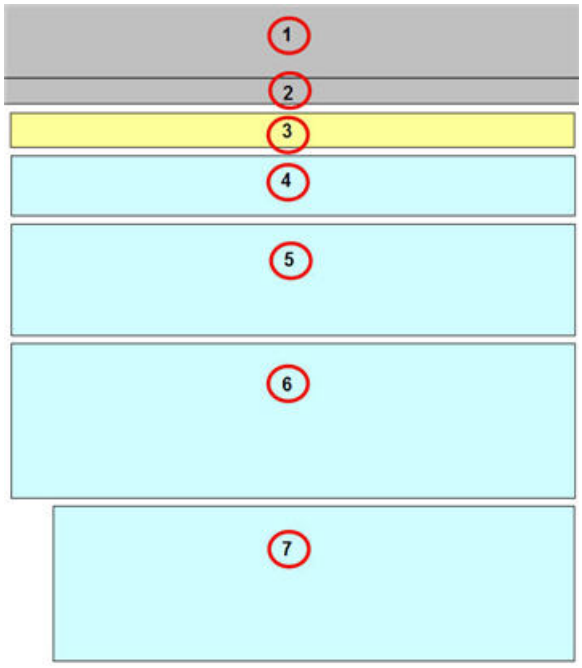


Figure 17: Layout of an Activity view page

The following numbered list describes the panes of an Activity view page as they are labeled in Figure 11.

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.

7. Child Hierarchy pane for children of the selected child object - unique to Activity views - contains fields configured for this object type.

Task 1: Specify view details
The text you enter in the **Name** field for this 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 or Grid 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 or Grid 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. Click **Next**.

Task 2: Select object types
Activity or Grid 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. Optional: 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. Click **Next**.

Task 3: Specifying 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 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, complete the following steps to specify the paths to use through the object hierarchy to retrieve data:
   a) Click the **Choose Paths** link under the **Actions** column in the row that contains the object type in Task 1 (if necessary, 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) Click **Apply**.

      The selected paths are listed in the **Paths** column.

      Note: Descendants of recursive object types, such as Business Entity, appear under all of their ancestors, not just the most immediate ancestor. For example, if the path is set to Business Entity/Preference and the hierarchy of objects is North America Division/US Region/Pref1, Pref1 appears as a descendant of both North America Division and for US Region.

2. To specify how objects types 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** field, complete the following steps:
   a) In the **Available Fields** pane, select each object field to use for sorting.

      Note: A sort field does not have to be displayed to in order to use the field for sorting a list or child hierarchy pane.

   b) Click the double arrows to move object fields forward (>>) or backwards (<<) between the **Available Fields** and the **Selected Fields** panes.
   c) In the **Selected Fields** pane, select a sort field and click any of the following icons:

Table 80: Sort icons	
Click this icon...	**If you want to...**
(triangle up)	Sort objects in ascending order. This value is the default setting.
(triangle down)	Sort objects in descending order.
(up arrow)	Move up the field in the list.
(down arrow)	Move the field down in the list.

   d) Click **Apply**.
4. To specify a filter for an object type, click **Choose Filter** in the **Actions** column that corresponds to the object type
5. In the **Choose Filter** field, select the filter to use and click **Apply**.
6. Click **Next**.

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 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. Optional: Insert a section. For details, see “Inserting section headings” on page 258.
3. Optional: Change the display order of the fields. For details, see “Setting the display order of fields in a view” on page 243.
4. Click **Next**.

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. Optional: Change the display order of the fields. For details, see “Setting the display order of fields in a view” on page 243.

3. 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 214).
2. Click the name of a profile. The Detail page opens.
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 wizard that corresponds with the type of change you want to make. Refer to "Creating Activity Views" on page 250 for an overview of tasks.
6. Click **Save**.

Creating a Creation view

In IBM OpenPages GRC Platform, you can create a creation view.

About this task

You can use Creation views to create multiple Add New view definitions for a single object type for a single profile.

Procedure

1. Click **Administration** > **Profiles** and select a profile.
2. Select the object that will be at the root of the creation view.
3. From the menu bar, click **Creation Views**.
4. In the **Creation Views** section, click **Add New**.
5. To provide details about the new creation view, complete the following actions:
   a) Add a name and description. Optionally, enter the translations for the name. The description is for administrators only.
   b) If the creation view is not ready for users to access now, clear the **Enabled** check box. The new creation view is enabled by default.
   c) Click **Next**.
6. To select the child objects to associate with the current object, complete the following actions:
   a) Under **Actions**, click **Choose Object Types**.
   b) Select the object types to associate.

      Only direct child objects are available to associate.
   c) Click **Apply**.
   d) Click **Next**.
7. Choose the objects that you want show on separate pages in the Add New wizard: check box
   a) For each object that you want to show on its own tab, select the **Separate page** check box.

      By default, any objects that do not have a separate page are shown together on the Associate tab.
   b) Click **Next**.
8. To configure fields for the creation view, complete the following actions:
   a) To select the fields that will be shown, click **Choose Fields**, select the fields, and click **Apply**.

b) To change the order in which the fields are shown, change the sequence of numbers in the **Order** fields and click **Update Order**.

c) Specify whether each field is **Read-Only**.

d) To specify a name for the object-specific tab, click **Insert Page** and enter a name for the section heading.

By default, the tab name is the Properties tab.

9. Click **Finish**.

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 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 include a field in a Detail or Activity view, the field must be visible in the object field list.

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

If the field is part of a field group, make sure you include the field group for the object type. For more information, see “Including field groups for an object type” on page 177.

Note: When dependent fields are included in a Detail or Activity view, make sure to include both the controlling field and required dependent fields. If the controlling field that requires that a user enter a value in a dependent field is included in a view and the required dependent field is excluded, the user cannot complete the operation. 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, you can set a field to span table columns.

Procedure

1. Access the **Profiles** page (see “Accessing profiles” on page 214).
2. Click the name of a profile. The Detail page opens.
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:

Table 81: Object views

For this type of view...	Do this...
Detail View	Click the Detail link.

Table 81: Object views (continued)	
For this type of view...	**Do this...**
Activity View	a. Click the name of the Activity view you want. b. In 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) 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 243.
7. To format the field so it spans table columns, see "Spanning table columns" on page 260.

Excluding fields from Detail and Activity views

When you exclude fields from a Detail or 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 report fragment fields.

With the exception of the **Name** field, you can exclude any field from an object view. For example, if you exclude the **Description** field from a Filtered List view for an object type, field is dynamically removed from the Filtered List view page and the change is immediately visible to 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 214).
2. Click the name of a profile. The Detail page opens.
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:

Table 82: Object views	
For this type of view...	**Do this...**
Detail View	Click the Detail link.
Activity View	a. Click the name of the Activity view you want. b. In 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 field, clear each field to remove from this view.
   c) Click **Apply** or **Save**.

Inserting section headings

Section headings are an optional formatting feature. Use section headings to delineate a set of fields on a page. Before you create a section heading, identify where to insert it on a Detail or Activity view page. A section heading is displayed on the page before whichever field you specify.

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

Procedure

1. Access the **Profiles** page (see "Accessing profiles" on page 214).
2. Click the name of a profile. The Detail page opens.
3. For the **Detail** view, click the **Detail** field.
4. For an **Activity** view, click the name of the Activity view and click **Specify Field Settings**.
5. To insert a section heading in the selected view:
   a) Select **Insert Section** for the object type.
   b) In the **Section Information** pane, provide the following information:

Table 83: Section information fields

Field	Action
Name	Required. Type a name for the section heading.
Insert before field	Select a field from the list. The section heading is displayed before the selected field.
language-specific (for example, Japanese)	Type a text string to use as the translated display text label for the section heading. If no translation text is entered, the entry in the Name field is displayed.

6. Click **Apply** or **Save**.

Modifying section headings

Section headings are an optional formatting feature. You can use section headings to delineate a set of fields on a page. 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 214).
2. Click the name of a profile. The Detail page opens.
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 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) Click **Apply** or **Save** to effect the change.

Deleting section headings

Section headings are an optional formatting feature. You can use section headings to delineate a set of fields on a page. You can remove section heading. After a section is deleted, it is permanently removed and cannot be restored.

Procedure

1. Click **Administration > Profiles**
2. Select the profile to modify.
3. From the **Object Types** listing, click the name of the object type to modify.
4. In the **Object Views** pane, click the Detail link or the Activity view to modify.
5. To delete the section in the Detail view, click **Delete** next to the section to delete.
6. To delete a section in an Activity view, click the **Specify Field Settings** link. Then, click **Delete** next to the section to delete.

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, computed 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 214).
2. Click the name of a profile. The Detail page opens.
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. Click **Save**.

Spanning table columns

In **Detail Views**, **Activity Views**, and **Context 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 214).
2. Click the name of a profile. The Detail page opens.

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:
   - Select **False** if you want the row containing the field to be displayed within a table column and not span the columns of the table.
   - Select **True** if you want the row containing the field to span the columns of the table.
7. Click **Save**.

Configuring the display type for reporting fragment fields

You can configure how reporting fragment fields are displayed to application users on Detail and Activity View pages. Reporting fragment fields are always read-only fields.

Reporting 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.

  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 "Report fragment settings" on page 321.

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 214).
2. Click the name of a profile. The Detail page opens.
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) Click **Save**.
6. Optional: For Automatic display types only. If the display type is On Demand, skip this step.
   You can 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) Click **Save**.
7. To make the row with the report fragment field span table columns, see "Spanning table columns" on page 260.

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 affects the display of this field in all profiles.

Procedure

1. Access the **Profiles** page (see "Accessing profiles" on page 214).
2. Click the name of a profile. The Detail page opens.
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 "Configure user and group selectors display types for simple strings" on page 266.
      - For a Business Entity Selector display type, see Configuring the Business Entity Selector display type for simple string fields.
      - For a rich text display type, see "Configuring rich text display types for simple strings" on page 262.
      - For a box and URL display types, see "Configuring text and URL display types for simple strings" on page 264.
      - For a plain text area display type, see "Configuring text area display types for simple strings" on page 266.
7. To have a row with a field span table columns, see "Spanning table columns" on page 260.
8. Click **Save**.

Results

Note: To change a field to **Read-Only**, see "Setting object fields as read-only or editable" on page 260.

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 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 84: 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** icon.
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** icon.

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 262.

Configuring the Business Entity Selector display type for simple string fields

For the Business Entity Selector display type, you can select a starting business entity, establish the number of levels that users can navigate, and determine whether to span columns.

To modify these settings, click **Edit** on the **Display Type Information** tab.

You can configure the following settings:

Table 85: Business Entity Selector display settings	
Setting	**Description**
Starting Business Entity	Click the icon beside the Starting Business Entity box, and use the **Recently Used**, **Browse** or **Search** tabs to select a starting business entity. Type a term in the **Search** field to find an exact match to the object name or description. **Note:** Optionally, if you want all Level 1 business entities displayed, enter a forward slash (/) in the Search box. If you leave this field blank, it will default to a slash when you save.
Number of Levels	Determines the number of levels that end users can navigate to from the starting business entity. For example, if you select Global Financial Services as your starting business entity and set the number of levels to 2, you can navigate to two levels below Global Financial Services (Global Financial Services/Asia Pac/Agency Services). Limit the number of levels to improve performance of the selector and help users select from the entities most appropriate for this field. The default value is 3.

Table 85: Business Entity Selector display settings (continued)	
Setting	**Description**
Span Columns	Determines whether to make a row span columns. The default value is false. This setting will be ignored by views that do not support column spanning. For more information, see Spanning table columns

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 262.

Known issue

A known issue exists when values in business entity selector fields are updated in the following scenario. A user in the OpenPages application chooses a business entity for a business entity selector field and saves it. The entity folder is correctly inserted in the business entity selector field. If the user then clicks **Action** > **Edit this Business Entity** and changes the name of the business entity, the value in the business entity selector field is not updated with the new name. If the user clicks **Action** > **Edit this Business Entity** again and selects the icon next to the business entity selector field, the select entity is now empty.

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 86: 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 262.

An alternative to using the URL display type is to use the rich text display type to display a user-friendly link name. For information, see "Configuring URL link names by using the rich text display type for simple strings" on page 265.

Configuring URL link names by using the rich text display type for simple strings

You can use the rich text display type to display a user-friendly link name as a field's default value. For example, you can configure a field's default value to display as **My Company** rather than **http://www.mycompany.com**. This feature is an alternative to using the URL display type, which can display only URL internet addresses.

About this task

When you use the rich text display type, you can define the URL by using the anchor tag, <a>. The anchor tag specifies the link name and styles you want to apply, such as font style and size. The `target="_blank` tag makes the URL open in a new tab.

For example, the following anchor tag displays the link name, **My Company**, and opens `http://www.mycompany.com` in a new tab:

```
<a href=" http://www.mycompany.com" target="_blank">My Company</a>
```

The following anchor tag applies a larger font and different color to the link name:

```
<a style="font-size:18px;font-family:comic sans ms,cursive;color:#FF0000"
href=" http://www.mycompany.com" target="_blank">My Company</a>
```

You can put multiple anchor tags in a single rich text field. For example, the follow anchor tags display two link names as a field's default value:

```
<a href=" https://www.ibm.com" target="_blank">Link to IBM</a>
<a href=" https://www.ibm.com/support/knowledgecenter/SSFUEU_7.4.0/main/welcome.html"
target="_blank">Link to IBM Knowledge Center</a>
```

Because you are using the rich text display type rather than the URL display type, the system does not check whether the URL is valid.

You can add fields that use the rich text display type for link names to all view types. However, on Filtered List and Grid views the link name is displayed above a glasses icon. Clicking the icon opens a window that contains the link.

Procedure

1. Click **Administration** > **Field Groups**.
2. Select a field group.
3. In the **Field Definitions** table of the field group, click **Add**.
   a) In **Data Type**, select Simple String.
   b) Click the double arrows (**>>**).
   c) In **Default Value**, enter the URL address as an anchor tag, for example:

   ```
   <a href=" http://www.mycompany.com" target="_blank">My Company</a>
   ```
4. Click **Administration** > **Profiles**.
   a) Select a profile.
   b) Select an object type.
   c) Click **Include** and choose the new field.
   d) Click the field in the **Object Fields** table and click **Edit**.
   e) In **Display Type**, select Rich Text.
5. Add the field to a view. Select **Read Only**.

What to do next

Create objects and use the new field. Since the URL is specified as a default value, the field does not display on existing object instances.

Configuring text area display types for simple strings

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 87: 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 262.

Configure user and group selectors display types for simple strings

You can configure a user, group, user/group, multi-valued user, multi-valued group, or multi-valued user/group selector display type for a simple string data type object field. An object field that has a selector display type allows an application user to click either an arrow and select user names from a drop-down list box or a magnifying glass icon and search for users or groups from a pop-up dialog box.

Object fields with a display type of user selector or multi-valued user selector only accept user names as valid values. For example, Control Owner is an object field for the control object.

The following selector display types are available for simple string data types:

Table 88: User and group display settings

Selector Display Type	Description
User Dropdown	On Detail and Activity views provides an arrow that users can click to display a drop-down list box of user names. On all other views provides a magnifying glass icon that users can click to display a search pop-up dialog box to search for a user.
User Selector	Provides a magnifying glass icon that users can click to display a search pop-up dialog box to search for a user.
Group Selector	Provides a magnifying glass icon that users can click to display a search pop-up dialog box to search for a group.

Table 88: User and group display settings (continued)	
Selector Display Type	**Description**
User/Group Selector	Provides a magnifying glass icon that users can click to display a search pop-up dialog box to search for a user or group.
Multi-Valued User Selector	Provides a magnifying glass icon that users can click to display a search pop-up dialog box to search for multiple users.
Multi-Valued Group Selector	Provides a magnifying glass icon that users can click to display a search pop-up dialog box to search for multiple groups.
Multi-Valued User/Group Selector	Provides a magnifying glass icon that users can click to display a search pop-up dialog box to search for multiple users or multiple groups.

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 89: 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. A value of **True**, when used in combination with a **Starting Group** value that contains many users, can result in slower search performance. • **False** - disabled user accounts are excluded from the selector listing. When this setting is selected, the **Minimum Access** setting is enabled. This setting generally applies to User (not Group) selectors. **Note:** There is a known issue with the **Include Disabled** setting. If the **Display Type** is **User Dropdown**, **Include Disabled** is set to **True**, and disabled users exist and should be listed, the disabled users are not listed and instead the message `No items to display` is shown.

Table 89: Additional selector display type settings (continued)	
Setting	**Description**
Starting Group	Controls which group displays at the beginning of the selection hierarchy. If the **Starting Group** value is blank, selectors search the system for all users and/or groups, depending on the display type. A blank **Starting Group** value used in combination with an **Include Disabled** value of **True** can result in improved search performance. 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. **Note:** There is a known issue with the **Starting Group** setting. In the Add New wizard, the **Starting Group** setting is not applied to fields that have **Display Type** set to **User dropdown**.
Include Subgroups	Controls whether subgroups are included or excluded from the User selector listing. **Note:** This setting applies only to the User/Group and Group selectors. If the **Include Subgroups** value is set to: • **True** - subgroups are included in the selector listing. • **False** - subgroups are excluded from the selector listing.

Table 89: Additional selector display type settings (continued)	
Setting	**Description**
Minimum Access • Read • Write • Delete • Associate	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, 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. If the **Read** box is: • Selected - only users with Read access are displayed on the user list. • Cleared - no filtering occurs. If the **Write** box is: • Selected - only users with Write access are displayed on the user list. • Cleared - no filtering occurs. If the **Delete** box is: • Selected - only users with Delete access are displayed on the user list. • Cleared - no filtering occurs. If the **Associate** box is: • Selected - only users with Associate access are displayed on the user list. • Cleared - no filtering occurs.

Changing the display type

Attention:

If you change the display type of the actor fields in the profiles, you must take action on the filters.

Table 90: Display type changes that require action		
If you change this display type	**To this display type**	**Take this action[1]**
User Selector	Group Selector or Multi-Valued Group Selector	A
	User/Group Selector or Multi-Valued User/Group Selector	B
User Dropdown	Group Selector or Multi-Valued Group Selector	A

Table 90: Display type changes that require action (continued)		
If you change this display type	**To this display type**	**Take this action[1]**
	User/Group Selector or Multi-Valued User/Group Selector	B
User/Group Selector	Group Selector or Multi-Valued Group Selector	A
	User/Group Selector or Multi-Valued User/Group Selector	B
Group Selector	Multi-Valued Group Selector	A
	User/Group Selector or Multi-Valued User/Group Selector	B
Multi-Valued User Selector	Multi-Valued Group Selector	A
	Multi-Valued User/Group Selector	B
Multi-Valued Group Selector	Multi-Valued User/Group Selector	A
Multi-Valued User/ Group Selector	Multi-Valued Group Selector	A

[1]Actions

- A: If you make this change, and if "End User" is set as the filter value for that actor field in the filter, the "End User" must be updated to the group so that the filters can return the expected results.
- B: If you make this change, re-save the filter so that it can return the expected results.

Additionally, you cannot change a Multi-Valued User Selector, Multi-Valued Group Selector, or Multi-Valued User/Group Selector display type to a single actor display type.

Controlling user selector performance

If your deployment has a large number of users, the performance of the User Selector or the Multi-Valued User Selector in opening and loading data may be sluggish. One way to improve the performance of the User Selector or the Multi-Valued User Selector is to configure it so it only retrieves users that have permission on the object being edited.

The supplied profiles in the IBM OpenPages GRC Platform application are configured such that the User Selector or Multi-Valued 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 or the Multi-Valued 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 214).
2. Click the name of a profile. The Detail page opens.
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) Optionally, select other permissions to further restrict the users that are available in the User Selector based on the users' permissions.
7. Click **Save**.

Modifying user and group selectors
On a small number of administrator screens, for example, **Administration** > **Object types** > **Add Filter** or **Edit Filter**, the pop-up dialog box for the User and Multi-Valued User Selectors displays user names in a phonebook style, and you can configure the number of users per category within the phonebook. Groups appear in a hierarchical tree style.

You can also configure the selector display types to open a search box instead of a phonebook style box. For more information, see “Actor selectors: Configure users and group selectors for search” on page 315.

For all the selector display types, you can configure additional display information for users, such as the user’s e-mail address or first or last name.

Modifying the phonebook
The User Selector and Multi-Valued User Selector display 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. For configuration details see, “Actor selectors: Configure the bucket size of the phonebook” on page 314.

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, “Actor selectors: Configure display columns in a selector dialog box” on page 314.

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.

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 283.

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 256000 bytes, but that can be increased by changing the **Platform** > **Repository** > **Resource** > **Large Text** > **Maximum Size** setting.

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

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.
```

The display types for medium long string data are: On Demand, On Demand Rich Text, Text Area, and Rich Text.

The display types for large long string data are: 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 "Data types" on page 143.

Procedure

1. Access the **Profiles** page (see "Accessing profiles" on page 214).
2. Click the name of a profile. The Detail page opens.
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 select the **Required** box to make the field required.
7. Click the **Display Type** arrow and select a value from the list to select a different display type:
   - For On Demand and On Demand Rich Text, see "Configuring the on demand display types for long string fields" on page 272. 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 273. 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 273. This applies only to medium long string fields.
8. Click **Save**.

   Note: To change a field to **Read-Only**, see "Setting object fields as read-only or editable" on page 260.

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 and on demand rich text. Both settings allow users to edit the 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 reports in PDF format, rich text fields do not render properly and the format is not preserved.
- Changing the display type setting will affect the display of this field in all profiles.

In **Detail Views** and **Activity Views**, fields are typically displayed on the page in rows within a two-column table format. To make the row containing the field span the table columns, see "Spanning table columns" on page 260.

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 91: 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 271.

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 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 92: 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** icon.
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** icon.
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 271.

Configuring a display type for enumerated strings

This is the procedure to configure 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.

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.

Procedure

1. Access the **Profiles** page (see "Accessing profiles" on page 214).
2. Click the name of a profile. The Detail page opens.
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 "Dependent field behavior" on page 198.

      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 "Localizing application text" on page 281.

   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 "Data types" on page 143.

Chapter 13. Localizing text

You can localize display text for object types and fields, and for a variety of application objects and custom return values. There is an administrative interface that you can use to manage localized text that displays to users for predefined object types, object fields that are supplied by IBM OpenPages GRC Platform or created by you, and application objects.

Locale codes

The OpenPages GRC Platform 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 or region code (for example, "FR" for France).

The following table lists the supported languages with their corresponding locale code.

Table 93: 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 reporting 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 “Set localization options” on page 345.

Configuring client systems to display Asian characters

You can install the East Asian language pack on Windows client machines.

Note: 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 GRC Platform users will notice that the browser title bar and some pop-up messages will contain unreadable characters.

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.

Language and locale support

If you are using IBM OpenPages GRC Platform in a language other than English, this information will help you to understand the language and locale settings.

Web browser language preference

The web browser language preference is the setting that you choose to specify the language that web pages can be displayed in. The web browser language preference affects only the OpenPages GRC Platform login page. The web browser language preference does not affect number and date formatting in OpenPages GRC Platform.

If the web browser language preference is set to a language other than one of the following languages, be aware that the OpenPages GRC Platform login page appears in English:

- German
- Spanish
- French
- Italian
- Japanese
- Portuguese
- Chinese
- English

Locale setting

The **Locale** list contains a list of product languages. This language setting controls the language of the product except for the login page.

Data formatting and report languages are available in the following cultures in the **Locale** list:

*Table 94: Languages in the **Locale** list and the cultures that they represent*

Language in the Locale list	**Culture**
French	French (France)
German	German (Germany)
Italian	Italian (Italy)
Japanese	Japanese (Japan)
Portuguese	Portuguese (Brazil)
Spanish	Spanish (Spain)

*Table 94: Languages in the **Locale** list and the cultures that they represent (continued)*	
Language in the Locale list	**Culture**
Simplified Chinese	Chinese (China)
Traditional Chinese	Chinese (Taiwan)
U.K. English	English (UK)
U.S. English	English (US)

Considerations for specific languages

When OpenPages GRC Platform is set to use U.S. English, dates are formatted as mm/dd/yy. For example, January 3, 2013, is formatted as 1/3/13 rather than 03/01/2013 in U.K. English.

When the product is set to use Spanish (Spain), numbers are formatted as 123.456,78, where the period is a thousands separator and the comma is used as a decimal separator. For example, the number twelve thousand and five hundred is formatted as 12.500 in Spanish (Spain) rather than 12,500 in Spanish (Mexico).

In several cultures, the convention is to place the currency symbol after the number. In OpenPages GRC Platform, currency symbols are always displayed before the number.

Date formatting can be unconventional as well.

Localizing 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, Chapter 13, “Localizing text,” on page 277.

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 280.
- 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:

- Only plain text should be entered as object text. Adding anything other than plain text to labels, such as HTML, line breaks, and carriage returns, is not supported.
- 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 S0XControl 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.

Important: Do not change or translate currency codes.

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 GRC Platform application interface wherever the particular object type displays, such as on a menu (for object types) or in object views.

Procedure

1. Click **Administration** > **Object Text**.
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. Click **Save**.

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 GRC Platform 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. Click **Administration** > **Object Text**.
2. On the **Object Text** page, expand the object type you want, expand the field group you want, and click the name of the object field that you want to modify. To modify enumerated string values, on the **Object Text** page, expand the enumerated object field you want, and click the name of the value 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.
5. Click **Save**.

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. Click **Administration** > **Object Text**..
2. On the **Object Text** page, expand the object type you want, expand the filters (icon), and 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:
5. Click **Save**.

Localizing system fields

You can change the system fields used for unassigned field groups that are specific to a locale. This change affects all object types and views.

For a list of supported locales, see Chapter 13, “Localizing text,” on page 277.

Procedure

1. Click **Administration** > **Object Text**.
2. On the **Object Text** page, expand **Unassigned Field Groups** > **System Fields**, and select the name of the field that you want to change.
3. On the **Locale Information** tab, click the name of the locale code you want to change (for example, en_US).
4. On the **Locale Code** detail page, make the required changes.
5. Click **Save**.

Localizing application text

Application text is the descriptive label names that display for objects such as icons, table headings and columns, and system object fields that are used throughout the application.

Application text is static, which means that it is unlikely to change over time. You can modify application text that is specific to a locale (for more information, see Chapter 13, “Localizing text,” on page 277 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.
- The format for the display of names and numeric data. For more information, see “Modifying display text in the application user interface” on page 282.

Note: Application text is limited to 4000 characters.

The following table shows the groupings by folder category for application text:

Table 95: Application text folder categories

This folder	Contains the label text for
Application Messages	Messages that are displayed for dependent fields and pick lists, and System Admin Mode.
Buttons	The icons that are used within the application. For example, com.button.back contains the text for the Back icon, button.copy contains the text for the Copy icon.
Column Headings	The table column headings that is used in the 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 more information, see “Creating a custom setting” on page 340.

Table 95: Application text folder categories (continued)	
This folder	**Contains the label text for**
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 display text in the application user interface" on page 282.
Labels	Objects that are not considered objects, such as administrative tasks, 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 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.

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 icons, labels, report names and descriptions, messages) in the IBM OpenPages GRC Platform user interface. The process for modifying display text is the same for all application objects, including reports.

Changes to the displayed text appear wherever the particular object is displayed in the application.

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 Cognos reports, see “Adding reports” on page 113.
- For reports that were manually published from the OpenPages GRC Platform 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 “The Custom folder” on page 286).

Procedure

1. Click **Administration** > **Application Text**.
2. On the **Application Text** page, open the folder that contains the label of the object field you want to modify (for example, Buttons or Miscellaneous), expand the folder, and 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. Click **Save**.

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: You can also modify the bucket size of the phonebook. For more information, see “Actor selectors: Configure the bucket size of the phonebook” on page 314.

Procedure

1. Click **Administration** > **Application Text**.
2. On the **Application Text** page, expand the **Formats** folder and 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}.

   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.
5. Click **Save**.

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 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. Click **Administration** > **Application Text**.
2. On the **Application Text** page, expand the **Formats** folder and 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. Click **Save**.

Example

To display the first and last name of users, you would enter the following codes in the Singular Label box: `%FN; %LN;`.

When the first and last names are used, the user name is shown with a hyphen. For example, User_JS - John Smith.

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.

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.

Procedure

1. Click **Administration** > **Application Text**.
2. On the **Application Text** page, expand the **Formats** folder and 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. Click **Save**.

   To view the changes in the browser, users must log out and then log back in to the application.

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}
```

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.

Procedure

1. Click **Administration** > **Application Text**.
2. On the **Application Text** page, expand the **Formats** folder and click the **menu.item.documentation.object.folder.view** 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 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. Click **Save**.

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`.

Modifying list view links

You can globally modify the format of the Business Entity List view navigational link on the Organization menu.

Procedure

1. Click **Administration** > **Application Text**.
2. On the **Application Text** page, expand the **Formats** folder and click the **menu.item.documentation.object.list.view** 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 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. Click **Save**.

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 GRC Platform user interface for reports (such as reports that are manually published from the OpenPages GRC Platform server).

Typically, this folder is populated through the ObjectManager tool. 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 "Modifying display text in the application user interface" on page 282.

Adding new keys

You can add new keys to the Custom folder for localization.

Note: For Cognos report pages (or JSP report instances) that were manually created using the publishing facility on the IBM OpenPages GRC Platform 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.

Procedure

1. Click **Administration** > **Application Text**.
2. On the **Application Text** page, in the **Custom** folder, 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) 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) Click **Save**.

Modifying custom keys

You can modify custom keys.

Procedure

1. Click **Administration** > **Application Text**.
2. On the **Application Text** page, in the **Custom** folder 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) Click **Save**.

Chapter 14. Reporting periods, object resets, and rulesets

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. Object resets are a way to automatically modify objects that exist in the IBM OpenPages GRC Platform repository. Object resets are rule-based operations that are contained in a ruleset.

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. After a reporting period is created, the existing report is carried forward to the current reporting period and can be modified without altering the state of the earlier reporting period's data. Only one reporting period at a time can be "Active".

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. After all quarterly tasks are 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. 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.

Rather than 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 object resets work well with the reporting period capability of the OpenPages GRC Platform application, object resets do not require the existence of a reporting period to be used.

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.
  - When you use the Grid View, only the top level objects are displayed.
- 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 on object types that have their own folders (such as Business Entities, object types that are part of the security model, and self-contained object types):
  - Move operations
  - Rename operations
- The Delete operation cannot be performed during an active reporting period on any object types.

Finalized reporting periods

After 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.

Reporting period interactions

You can interact with the reporting schema, the ACL, and the change history for a reporting period.

Reporting schema interactions

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 91).

ACL interactions

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.

Change history interactions

When viewing a change history for an object, only the changes made during the currently selected reporting period are shown. You can view the change history for past reporting periods, but only the change activities for that reporting period will be shown.

You cannot view change histories 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 "Enabling and disabling System Administration Mode" on page 17) to either finalize or drop the active reporting period.
- If the reporting period is created after you create 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 specific application permissions. The amount of time after a reporting period is created in which the reporting period can be deleted is set in the *Delete Interval* setting

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.

Deletion period setting

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, "Modify the deletion interval for a reporting period" on page 311.

Creating a 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**.
2. Click the **Add Active** icon.
3. Enter the necessary information and click **Create**. 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 on 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 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** icon 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** icon.
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 GRC Platform 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.

To view active reporting periods, the end user must be a member of the `ActiveReportingPeriodAdministrators` group.

After you associate an end user with this group, the **Reporting Period** option becomes available after the user logs off and log on again.

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 “Enabling and disabling System Administration Mode” on page 17).

Procedure

1. Navigate to the business entity you want to be the root of the reapplied reporting period.
2. Select the active reporting period from the list and click the **View** icon.
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** icon 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

After 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.

After you finalize an entire reporting period, it ceases to be active. Only then can you create a new active reporting period. If even one business entity is not 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.
3. Click the **Finalize** icon to finalize the entire reporting period. 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 beginning of the page, select the active reporting period from the list and click the >> icon.

   c) Click the **Finalize** icon to prevent any further changes to the business entity and all of its child objects.

Deleting a reporting period

After you create 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).

IBM OpenPages GRC Platform supports deletion of reporting periods for a configurable amount of time after the reporting period is created. for details on this setting, see “Modify the deletion interval for a reporting period” on page 311.

If the deletion period has **expired**, then the active reporting period cannot be deleted.

If the deletion period has **not expired**, then the active reporting period can be deleted.

Note: The default period for deletion of a reporting period is seven days after creating an active reporting period.

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 reporting periods you want to delete.
3. Click **Delete** at the beginning of the page.

   You are returned to the Reporting Periods page and the deleted reporting period is removed from the table.
4. Click **Refresh** to update the current value of the Status field while the deletion is occurring.

Results

If you cannot delete a reporting period (you click the check box and the **Delete** icon does not activate), the deletion period for that reporting period has expired. However, you can retroactively change the deletion period setting.

Object resets

Object resets are a way to automatically modify objects that exist in the IBM OpenPages GRC Platform repository. Resets can be started by users with the proper permissions from the **Object Resets** 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. After 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 functionality to take your existing objects and modify their properties based on the rules in your ruleset.

While object resets work well with the reporting period capability of the OpenPages GRC Platform application, object resets do not require the existence of a reporting period to be used.

Object resets on file attachments

You can only use object resets to delete objects that are JSP-based, not attachments available when using the **Browse Files** option. For example, if you use an object reset on SOXDocument, you see the following error:

```
VALIDATION ERROR (Line: 8 Column: 55): Content Type (SOXDocument)
must be JSP-based to be referenced in an Object Delete rule.
```

Suppose that you have files that are attached to test results. You can configure the settings to delete attachments when test results are deleted. To delete the SOXDocument objects, you can add SOXDocument to the **Cascade Delete** setting to delete the files that are associated with the test results during the object reset rule to delete test results.

Object resets 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.

Object resets 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 an object reset is performed, you will need to perform a few tasks to help ensure that the reset procedure goes smoothly.

- Back up your OpenPages GRC Platform data before running an object reset.
- If you plan on archiving your changes to a reporting period, you will need to set up the reporting period before running the object reset.

Creating a ruleset

Object resets are rule-based operations on the objects in your IBM OpenPages GRC Platform repository. The rules that govern how an object reset will affect your data are contained in a ruleset file.

A ruleset is a set of rules contained in an XML loader file that is created outside of the OpenPages GRC Platform 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. After the ruleset is imported, it can be selected during the Specify Options step of the Object Reset guided action.

When you use ObjectManager loader tool to import security rules, the entire ruleset is loaded and replace existing security rules that have the same name as a imported rule. Before importing security rules, export your existing rules first.

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.

To create the ruleset file, create a new XML file. Save the file with the following naming convention:

```
<file-identifier>-op-config.xml
```

Sample ruleset

The following XML 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>
```

Ruleset tag library

Use the following XML tags 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:

- xmlFormatVersion

  Version of the IBM OpenPages GRC Platform 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 GRC Platform 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:

- name

  An identifying name for the ruleset. Will be displayed in the OpenPages GRC Platform 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 GRC Platform 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:

- 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:

- contentType

  Specifies the object type that the rule will be applied to. Must match a valid IBM OpenPages GRC Platform 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:

- 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:

- 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:

- 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:

- 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:

- 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>
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.

Use a maximum of three criterion within a single <criteria> tag. Adding additional criterion will increase the processing time required to complete the Reset.

Parent Tags: <criteria>

Child Tags: <propertyValue>

Syntax:

```
<criterion bundle=""
           property=""
           operator="[=|&lt;&gt;|&lt;=|&lt;|&gt;|&gt;=|like]"
  <propertyValue=""/>
 [<propertyValue=""/>]
</criterion>
```

Attributes:

- 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 (&lt &gt), greater than (&gt), less than (&lt), greater or equal to (&gt=), less than or equal to (&lt=), 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 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.

For SQL tool information, see "Database tool information" on page xxv.

Note: The <propertyValue> referenced in a <criterion> tag cannot be null (or empty).

<propertyValue>
Description: The <propertyValue> tag performs two functions, depending on its location. The Boolean property value must be all lowercase. For example, "true" is correct, "True" is incorrect.

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.

  Note: The <propertyValue> referenced in a <criterion> tag cannot be null (or empty).

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:

- name

  Specifies the value of the property. 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 GRC Platform system.

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".

Procedure

1. Open a command or shell window on the OpenPages GRC Platform server.
2. Navigate to the *<OP_Home>* directory.

   Where: *<OP_Home>* represents the installation location of the OpenPages GRC Platform application. By default, this is:

   - Windows - `C:\OpenPages`
   - AIX and Linux - `/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 OPAdministrator 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 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.

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.

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.

From the **Settings** link on the Administration menu, access the following Object Reset settings in the **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 332.
- **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 333.
- **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 333.
- **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 333.

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Starting the object reset

Start object resets from the **Administration** menu.

Before you begin

Complete the following procedure to start the object reset:

Procedure

1. Log on to the IBM OpenPages GRC Platform 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 **Administration** > **Object Resets**.
3. Click **Start New Reset** at the beginning of the table to create a new reset.
4. Enter a name and description for the new reset.
5. Select a ruleset from the list of available rulesets.
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. After you select the Business Entities, click **Start Reset** .

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 began.

End Date - The time and date the Reset finished.

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.

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 topic “Performing the object reset” on page 302.

Procedure

Click the **View Log** icon 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.

Refreshing the reporting database after the reset

After you perform an object reset, 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 GRC Platform reports will automatically see the changes.

For detailed information on performing a reporting database refresh, see Chapter 5, “Managing the reporting schema ,” on page 89.

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 GRC Platform server.

This procedure will export ALL defined rulesets. Exporting rulesets does not remove them from the OpenPages GRC Platform application; they will still be available for use after they are exported.

Procedure

1. Back up the `ObjectManager.properties` file.

   Note: The `ObjectManager.properties` file is located in the root installation folder of your OpenPages GRC Platform 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. 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 GRC Platform 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 OPAdministrator 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 15. Viewing the Configuration and Settings page

To access the **Settings** menu, you must have **Settings** application permission on your account.

Use this procedure to view the Configuration and Settings page. For more information, see “Types of application permissions” on page 32.

Procedure

1. Log on to IBM OpenPages GRC Platform with an account that has the Settings application permission.
2. From the navigation bar, select **Administration** > **Settings**.

   Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

   From the **Settings** page, view summary information about settings and access the Detail page.

Applications folder settings

On the Settings page, the Application folder settings represent a selected list of individual settings.

All of the following actions are accessed from the Applications folder.

To access the Applications folder settings menu item, you must have Settings application permission set on your account. From the navigation bar, select **Administration** > **Settings** > **Applications**.

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Modify 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.

If the number of nodes that are displayed exceeds the default of 10000, the additional nodes are not displayed. Each cached object requires 1600 bytes of memory.

Administration > Settings > Applications > GRCM > Caches

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: 10000

Value: In the **Value** box, type a new numeric value.

The new setting will take effect after you log out and log back in.

Configure the browser cache

Affect the behavior of the browser's back and forward icons by changing the value of the Disable Browser Cache setting.

Administration > Settings > Applications > Common > Configuration > Disable Browser Cache

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: **false**

Values:

- **true** - the browser's cache is disabled; using the back icon sometimes requires 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 might be whatever was cached in the browser.

Display the accessibility link

To display a client-specific page with information about accessibility for disabled users, configure the display of the **Accessibility** link in the header pane of the IBM OpenPages GRC Platform 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.

Administration > Settings > Applications > Common > Accessibility > URL

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: none

Value: In the **Value** box, type a URL.

For example, you create a page in HTML format that contained information about your company's accessibility policy for disabled users and want this policy to be available to all users through the application. 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 the following:

```
http://machine1:7009/openpages/custom_files/accessibility.htm
```

Display or hide field guidance

Show or hide field-specific guidance on the Add or Edit page of an object through the **Show Field Guidance** setting.

By default, the **Show 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.

Administration > Settings > Applications > Common > Configuration > Show Field Guidance

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: true

Values:

- **true** - the question mark icon and field guidance text is displayed to users.

- **false** - the question mark icon and field guidance text is hidden from users.

Display or hide system generated field guidance

The **Show System Generated Field Guidance** setting controls whether information about field dependencies and dependent picklists is appended to field guidance.

For this setting to have effect, the **Show Field Guidance** setting must be set to true. If **Show Field Guidance** is false, then no guidance would be shown in any event. For details, see"Display or hide field guidance" on page 308.

Administration > Settings > Applications > Common > Configuration > Show System Generated Field Guidance

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: true

Values:

- **true** - shows system-generated dependencies information.
- **false** - suppresses system-generated dependencies information.

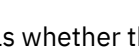
Disable the Add New wizard from various launch points

You can disable the **Add New** capability for any or all objects from several launch points within the product. There is a different registry setting for each of the launch points.

These launch points do not prefill parent information. If users find it difficult to select the most appropriate parent information for particular object types, you can disable the **Add New** capability.

Note: The **Object Types Disabled** setting overrides these settings. If an object type is disabled everywhere, there is no need to disable the Add New wizard individually for each launch point. For more information about the **Object Types Disabled** setting, see "Controlling the availability of object types in the Add New wizard" on page 204.

Table 96: Disabling the Add New wizard

Setting name	Description
Disable Add New Global Launch Point	Controls whether the **Add New** button  appears on the menu bar of every page.
Disable Add New Home Page Filtered List Global Launch Points	Controls whether the **Add New** icon  appears in a pane on the **My Work** tab on the Home page. When you disable this launch point, users can still use the **Add New** capability from a row in a pane.
Disable Add New Filtered List View Page Global Launch Points	Controls whether the **Add New** icon  appears on the Filtered List View/Grid View toolbar. Also controls whether the **Add New** menu item is displayed in the **Grid Actions** menu. When you disable this launch point, users can still use the **Add New** capability from a row in the grid.
Disable Add New Home Page Dashboard Launch Points	Controls whether the **Add New** capability is enabled from the Home page Dashboard panel launch point.

Administration > Settings > Applications > GRCM > Add New Wizard > Disable Add New Global Launch Point

Default: none

Values: In the **Value** box, type the names of the objects that you want to disable. Separate each object type with a comma (,). Use the object names and not the object labels. A value of ALL disables the launch point for all object types.

Administration > Settings > Applications > GRCM > Add New Wizard > Disable Add New Home Page Filtered List Global Launch Points

Default: none

Values: In the **Value** box, type the names of the objects that you want to disable. Separate each object type with a comma (,). Use the object names and not the object labels. A value of ALL disables the launch point for all object types.

Administration > Settings > Applications > GRCM > Add New Wizard > Disable Add New Filtered List View Page Global Launch Points

Default: none

Values: In the **Value** box, type the names of the objects that you want to disable. Separate each object type with a comma (,). Use the object names and not the object labels. A value of ALL disables the launch point for all object types.

Administration > Settings > Applications > GRCM > Add New Wizard > Disable Add New Home Page Dashboard Launch Points

Default: none

Values: In the **Value** box, type the names of the objects that you want to disable. Separate each object type with a comma (,). Use the object names and not the object labels. A value of ALL disables the launch point for all object types.

Set a default object view

If an object view for an object type is configured to display both a Folder View and Filtered 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 Filtered List views for an object type, see "Folder views and Filtered List views" on page 237.

Administration > Settings > Applications > GRCM

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: filter

Values:

- **filter** - the Filtered List View tab is displayed first to users.
- **folder** - the Folder View tab is displayed first to users.

Configure 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** icons by changing the value of the **Enable File Checkout** setting.

Administration > Settings > Applications > GRCM

Tip: In the user interface, the OpenPages folder is hidden in the Administration Settings folder hierarchy. To author an XML settings path, include the OpenPages folder after the Settings folder in the path.

Default: true

Values:

- **true** - the file check-out and check-in feature is enabled and the corresponding icons 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 icons are hidden.

Configure the sort order of object list views by modification date

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.

For example, 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 that are 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**.

Administration > Settings > Applications > GRCM > List View > Sort by Modification Date

Tip: In the user interface, the OpenPages folder is hidden in the Administration Settings folder hierarchy. To author an XML settings path, include the OpenPages folder after the Settings folder in the path.

Default: false

Values:

- **true** - objects in a list view are sorted by their last modification date.
- **false** - objects in a list view are sorted by name. This is the default setting value.

Modify 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. After the specified interval, the reporting period can no longer be deleted.

Administration > Settings > Applications > GRCM > Reporting Periods > Delete Interval

Tip: In the user interface, the OpenPages folder is hidden in the Administration Settings folder hierarchy. To author an XML settings path, include the OpenPages folder after the Settings folder in the path.

Default: 7 days

Value: In the **Value** box, edit the number of days you want for the deletion interval.

Show hidden settings

Some settings are hidden to protect these settings from being modified. To display hidden settings, change the value in the **Show Hidden Settings** setting.

Administration > Settings > Applications > Common > Configuration

Tip: In the user interface, the OpenPages folder is hidden in the Administration Settings folder hierarchy. To author an XML settings path, include the OpenPages folder after the Settings folder in the path.

Default: false

Values:

- **true** - show hidden settings.
- **false** - hide hidden settings.

User provisioning settings

Administrators can configure the behavior of the Create User wizard and the Users page with the following settings.

To access the user provisioning settings menu items, you must have the Settings application permission set on your account. From the navigation bar, select **Administration** > **Settings** > **Applications.**.

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Copy Access From Inactive
Determines whether inactive users can be the source for the Copy Access From operation.

Administration > Settings > Applications > Common > Administration > User Provisioning > Copy Access From Inactive

Default: true

Values:

- **true** - allows you to select inactive users to copy access from.
- **false** - inactive users cannot be selected to copy access from.

Copy User Info Attributes
Determines the default behavior for the Locale, Profiles, Group Memberships, Direct Role Assignments, and Direct Reports Access attributes during the Copy Access From operation. A name=value pair is used for each attribute, such as Locale=Yes. Name=value pairs are separated by a comma.

Administration > Settings > Applications > Common > Administration > User Provisioning > Copy User Info Attributes

Default: Locale=Yes,Profiles=Yes,Group Memberships=Yes,Direct Role Assignments=Yes,Direct Reports Access=Yes

Values: If a name pair is missing, the copy operation is not available. For example, if Profiles=Yes is not listed in the **Value** box, profiles are not copied during the copy operation.

- **Yes** - by default, the attribute is copied.
- **No** - by default, the attribute is not copied. If a name=value pair is missing, No is assumed. For example, if Profiles=Yes is not listed in the Value box, profiles are not copied by the copy operation.
- **Not available** - the attribute cannot be copied.
- blank - if the **Value** box is empty, the Copy Access From operation is not available.

Copy User Info Choice
Determines whether the Copy Access From operation adds to or replaces a user or group's existing attributes.

Administration > Settings > Applications > Common > Administration > User Provisioning > Copy User Info Choice

Default: Replace

Values:

- **Replace** - existing attributes are overwritten by the Copy Access From operation.
- **Add** - new attributes are merged with existing ones and duplicates are removed. No validation is done after the merge to ensure that there are no conflicts.
- **Choice** - means you can choose between Add or Replace each time that you do a Copy Access From operation.

- **Not Available** - you cannot perform the Copy Access From operation.

Default Allowed Profiles
Determines the default value or values for the Allowed Profiles.

Administration > Settings > Applications > Common > Administration > User Provisioning > Default Allowed Profiles

Default: blank

Values: Possible values are any profiles in the system. Use a dollar sign and semicolon ($;) to separate profile names in the list. If the value is blank, the Default Profile is used as the Allowed Profile.

Note: Disabled profiles cannot be used as an Allowed Profile, even if they are included in this list.

Default User Change Password
Determines the default change password behavior when you create a new user.

Administration > Settings > Applications > Common > Administration > User Provisioning > Default User Change Password

Default: blank

Values:

- blank - if the **Value** box is empty, the password expires in 90 days, and the user can change the password then.
- **cannot** - user cannot change password. Using this value forces **Password never expires**, and ignore the **Default User Password Expiration** setting.
- **must** - user must change password at next logon.

Default User Password Expiration
Determines the default password expiration behavior.

Administration > Settings > Applications > Common > Administration > User Provisioning > Default User Password Expiration

Default: blank

Values:

- blank - password expires in 90 days.
- *n* - password expires in *n* days, where *n* is an integer in the range 1 - 99.
- **never** - password never expires

New User Default Locale
Determines the default value for the locale.

Administration > Settings > Applications > Common > Administration > User Provisioning > New User Default Locale

Default: en_US

Values: Allowed values are any of the OpenPages supported locale codes, such as de_DE, en_US, and it_IT.

Reports Access Page Size
Determines the number of rows that are listed per page in the Reports Access table.

Administration > Settings > Applications > Common > Administration > User Provisioning > Reports Access Page Size

Default: 20

Values: In the **Value** box, type a positive integer. If the number of rows is less than this number, there is no paging.

Users Can Copy Access From
Determines which users can be used as source for the Copy Access From operation.

Administration > Settings > Applications > Common > Administration > User Provisioning > Users Can Copy Access From

Default: blank

Values: In the **Value** field, type a comma-separated list of users that can be used as source for the Copy Access From operation. If the value is blank, no users can be used as source for the copy operation. A value of **ALL** means that any user can be used as source. Use the **Copy Access From Inactive** setting to determine whether inactive users can be used. For more information, see "Copy Access From Inactive" on page 312.

Configure actor table page size

Use the **Page Size** setting to control the number of rows that are listed per page. This setting applies to the following administrative areas within the IBM OpenPages GRC Platform application: user and group management, role assignments, profile user association, and custom security.

Administration > Settings > Applications > Common > Administration > Users and Groups > Page Size

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: 100

Values: In the **Value** box, type a number.

Actor selectors: Configure 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.

For information about the phonebook, see "Modifying the phonebook" on page 271.

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.

Administration > Settings > Applications > Common > User Selector > Bucket Size

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: 10

Values: In the **Value** box, type a numeric value for the number of users you want displayed per bucket.

Actor selectors: Configure 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.

This setting applies when a phonebook style user or group selector dialog box is open on certain pages, including when:

- assigning a user or group administrator permissions from a Security Domain page
- selecting the starting group when configuring display type attributes for a user or group field in a profile

For information about selector dialog boxes, see the topic "Modifying the selector dialog box" on page 271.

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.
- 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).

Administration > Settings > Applications > Common > Actor Selector > Fields

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: If no values are present in the **Fields** setting, the **Name** and **Description** column headings are displayed by default.

Values: 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:

Table 97: Column heading display codes

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.

For example, to display the email address of users followed by a description of the user, type 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.

Actor selectors: Configure users and group selectors for search

Deprecated.

Administration > Settings > Applications > GRCM > Detail Page > Use Actor Search Only

Menus: Update administration menus

Customize the administration menus for your users by adding custom menu items.

Attention: Users do not see changes to menus until the next time they log in.

Administration > Settings > Applications > GRCM > NavigationMenu > Administration > SubItems

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: none

Values:

For example, *`YourCustomMenuItem`*`,Security,Schema,Application,Management`.

Menus: Modify the order of menus

The navigation bar in IBM OpenPages GRC Platform contains various menus that represent categories for grouping views and object types. 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.

Administration > Settings > Applications > GRCM > NavigationMenu > Items

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: **MyOpenPages** is typically displayed as the first menu item on the navigation bar, and **Administration** as the last menu item.

Values: 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.

  In the following example, the menus on the navigation bar are 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.

Changes to menus do not appear until users log out and then log back in to the application.

Menus: Modify submenus

The navigation bar in the IBM OpenPages GRC Platform 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.

Administration > Settings > Applications >

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: none

Values:

Note:

- The list of submenu items must be comma delimited.
- You can 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.

Object auto-naming settings

For most object types, you can auto-generate their names when they are created or copied. 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 might want all business entities and processes to be named by users, but all risks, controls, and test plans named automatically by the IBM OpenPages GRC Platform application.

Note: Auto-naming is not supported for the following object types: SOXDocument and SOXSignature.

Although auto-naming is not supported for SOXDocument objects, you can control how duplicate file names are handled. For information, see "SOXDocument object auto-naming settings for duplicate file names" on page 320.

Administration > Settings > Applications > GRCM > Auto Naming

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: none

Values: For each object type, you can modify the following settings:

Table 98: Auto-naming settings to modify

Setting name	Description
Auto-named folder	Flags this folder as using auto-naming.

Table 98: Auto-naming settings to modify (continued)	
Setting name	**Description**
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**.
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 “Configure the format of object names” on page 318.

Configure 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 that are described in the following table to format the auto-generated name.

Administration > Settings > Applications > GRCM > Auto Naming

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: none

Values:

- In addition to the variables, you can include any valid text in the auto name.
- The name of an object:
  - Must be 252 bytes or less.
  - Cannot contain forward slashes (/), backslashes (\), or the ellipsis character (...).

– Must contain either the %Nn or the %Rn token.

Table 99: 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.
%Rn; [5.5.1 added - OPX]	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.

Name examples

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"

SOXDocument object auto-naming settings for duplicate file names

Use the Auto Remediate Duplicate File Names setting to control auto-naming for SOXDocument objects.

Within a folder, file names for SOXDocument objects must be unique. This setting controls what happens when a duplicate file name is added. The system can add a numeric suffix to the file name or force the user to rename it.

Administration > Settings > Applications > GRCM > Auto Naming > SOXDocument > Auto Remediate Duplicate File Names

Tip: In the user interface, the OpenPages folder is hidden in the Administration Settings folder hierarchy. To author an XML settings path, include the OpenPages folder after the Settings folder in the path.

Default: true

Values:

- **true** - adds a numeric suffix to the file name.
- **false** - forces users to rename the file.

In infrequent user applications, such as questionnaire assessments and IBM OpenPages Loss Event Entry, this setting is ignored and duplicate file names are automatically renamed.

In Folder View, this setting is ignored and an error is issued when a user saves a duplicate file name in the folder. The user must manually rename the file.

Environment migration settings

If your organization has multiple IBM OpenPages GRC Platform environments, you can move data from one environment to another without needing physical access to either environment. Migration means exporting from a source environment and importing into a target environment. The following Application settings support environment migration:

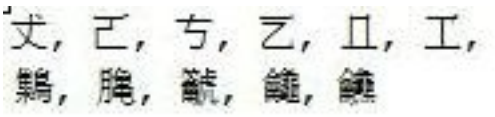
For details, see Chapter 22, “Migrating OpenPages GRC Platform environments,” on page 575.

Administration > Settings > Applications > GRCM > Environment Migration

Tip: In the user interface, the OpenPages folder is hidden in the Administration Settings folder hierarchy. To author an XML settings path, include the OpenPages folder after the Settings folder in the path.

Table 100: Environment Migration Settings

Setting	Definition
Allow ObjectManager XML	Controls whether ObjectManager XML files can be imported through **Administration** > **Import Configuration**. The default is false.
Asynchronous Timeout	The timeout value (in seconds) for AJAX calls on environment migration pages. The default is 120.

Table 100: 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. 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 in the Export File Name Prefix. The special characters to avoid are: 
Maximum String Items	Controls how many rows are displayed in the **Review selected items** box when exporting items with environment migration. Permissible values are any integer greater than zero. The default is 10000. Certain categories of items that can be exported with Environment Migration (such as Application Text) contain many tens of thousands of items. To reduce the page size and make Internet Explorer more responsive when reviewing these categories, you can now set a limit on the number of items that are shown. When a limit is set you can still use the search feature to find items beyond the row limit.
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 special characters are checked while validating names of metadata. The default is **true**. Set to **false** to preserve legacy special character rules.

Report fragment settings

For all profiles, you can globally configure 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 101 on page 322.

Report fragment fields with a display type of On Demand always display Cognos 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 - Cognos 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 My Work tab on the Home page - Cognos 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.

Administration > Settings > Applications > Common > Report Fragments > Popup

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Values: Click one of the settings to open its detail page. In the **Value** box for the selected setting, change the existing value to a new number (must be greater than zero).

Table 101: Settings for reporting fragment pop-up windows

Setting	Description	Default 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

Set the mail server address

Use the **Mail Server** setting to configure your mail server so you can automatically send email notifications to users from your JSP-based reports or the Notification Manager utility.

The **Mail Server** setting is also used to do mail routing for objects that use lifecycles, for example, questionnaire assessments and incidents. Email notifications are sent to lifecycle assignees when a lifecycle starts and with every transition except for close transitions.

For emails generated by lifecycle triggers, the sender address is specified in the `trigger.xml` file. The default is donotreply@openpages.com. For more information about lifecycle triggers, see the *IBM OpenPages GRC Solutions Guide*.

Depending on your environment, you can configure the following settings:

- `SMTP Password`
- `SMTP Port`
- `SMTP Security Type`
- `SMTP User Name`
- `SOCKS Proxy Private IP Address`

Define `SMTP Port` and `SMTP Security Type` if you use a third-party SMTP provider. Valid values for `SMTP Security Type` are SSL/TLS and STARTTLS. You must also import the SSL certificate from the SMTP server provider. Refer to the SMTP provider's documentation and import it by using IBM WebSphere administrative console. Leave `SMTP Port` and `SMTP Security Type` empty if you have an unencrypted connection that uses the default port number. In this case, the SMTP servers are behind a firewall and a third-party SMTP provider is typically not used.

Some settings might be hidden. For information about unhiding settings, see “Show hidden settings” on page 311.

Note: Override this global setting by entering the name of a mail server in the notification Mail Server parameter.

Administration > Settings > Applications > Common > Email

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: mail.yourcompany.com

Values: In the **Value** box, enter the values for **Mail Server**, **SMTP Password**, **SMTP User Name**, and **SOCKS Proxy Private IP Address**, as required by your mail system.

In **Mail Server** enter a fully qualified server host name, for example, `mail.openpages.com`.

For more information if you have legacy or older JSP reports and want to send email notifications to users from these legacy JSP-based reports or the Notification Manager utility, go to "Configure self-contained object types" on page 343.

Optimize file uploads

To enhance the performance of large files for upload to the IBM OpenPages GRC Platform application, you can enable the **Optimized File Upload** setting.

You can only optimize the upload if you are using the **Edit/Upload this File** option. You cannot optimize the upload if you use the **Add New** option.

When enabled, this feature provides the following functions:

- Compresses the selected file on the user machine before uploading it to the OpenPages GRC Platform repository.
- Displays additional Optimized File Upload text and a **Browse and Save** icon to users for attaching files.

  Note:

  – The file upload applet requires the Java Runtime Environment version 7 on the client browser.

  – When using the Chrome browser, if the registry setting **Administration** > **Settings** > **Applications** > **Common** > **Optimized File Upload** is set to `true`, the setting is ignored by the Chrome browser. For **Optimized File Upload** to be available, you must use Microsoft Internet Explorer.

By default, this value is disabled.

Administration > Settings > Applications > Common > Optimized File Upload

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: false

Values: In the **Value** box, type true or false

- `true` - The Optimized File Upload **Browse and Save** icon is displayed to users in addition to the standard file upload icon.
- `false` - Only the standard file upload icon is displayed to users.

Number of objects in listing pane

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.

Administration > Settings > Applications > GRCM > List View > Page Size

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: 20

Values: In the **Value** box, type a number greater than zero.

If the number of child objects that are returned exceed the set value, a Rev and Next link is displayed.

Set copy operations

You can 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 “Configure self-contained object types” on page 343).
- 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.

Administration > Settings > Applications > Common > Configuration > Copy Options

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Table 102: 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>". **Note:** Consider carefully whether to use **overwrite** or **copyof** when you copy objects that have the same name coming from different hierarchies. The end result if you use **overwrite** will be a single object with many versions. However, if you use **copyof**, it will be many objects with one version. • **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. 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**.
Max Object Trees Copied Interactive	This setting is a positive integer that determines when the copied objects are created. If the user chooses to copy the objects and their descendants, and the number of selected objects is less than or equal to the value of this setting, the dialog stays open until the copies are complete, blocking other actions. If the number of selected objects is greater than the value of this setting, then the copies are created in the background. The user receives an email when the copy process has completed. The default value is 20.
Max Top-level Objects Copied Interactive	This setting is a positive integer which determines when the copied objects are created. If the user chooses to only copy the objects themselves without any descendants, and the number of objects to be copied is less than or equal to the value of this setting, then the copies are created while the user waits. If the number of objects to be copied is greater than the value of this setting, then the copies are created in the background. The user receives an email when the copy process has completed. The default value is 250.

Table 102: Copy Operations Configuration Settings (continued)	
Setting	**Description**
Show Copy Options Page	This setting is only used when the Use Legacy Copy option is true. 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**.
Show Name Conflict Resolution Options	Specifies whether to display the name conflict resolution options in the Copy Wizard options tab. If the options are not displayed to the user, the value from the Conflict Policy setting is used. The default value is true.
Show Object Copy Options	If this value is set to true, the user is allowed additional control of what is copied with the selected objects. Users are able to choose if just the objects themselves are copied, or if descendants of the object are copied as well. By default, descendants are copied as well. Even if they choose to copy descendants, by default files and issues are not copied. If this option is set to true, users have the opportunity to also include files and issues. The default value is true.
Use Legacy Copy	Controls whether the copy operation uses the new interface or the legacy interface. Permissible values are true or false.

Date field display format

The **Date field display format** setting controls how date fields are displayed for GRC objects. It does not affect dates that appear in other areas of the system. It affects only how date fields are displayed and not the format when users enter date values.

The **Date field display format** setting and the locale determine how date fields are displayed. The examples below illustrate how the date, October 25, 2016, is displayed given different date formats and locales:

Table 103: Date field display format		
Locale	**Date field display format**	**Result**
US English	SHORT	10/25/16
US English	MEDIUM	Oct 25, 2016

Table 103: Date field display format (continued)		
Locale	**Date field display format**	**Result**
US English	LONG	October 25, 2016
UK English	SHORT	25/10/16
UK English	MEDIUM	25-Oct-2016
UK English	LONG	25 October 2016
Simplified Chinese	SHORT	16-10-25
Simplified Chinese	MEDIUM	2016-10-25
Simplified Chinese	LONG	2016年10月25日

Administration > **Settings** > **Applications** > **GRCM** > **Date Field Display Format**

Default:

The values are:

- **short** - dates are displayed in Java Locale SHORT format.
- **medium** - dates are displayed in Java Locale MEDIUM format.
- **long** - dates are displayed in Java Locale LONG format.

Configuring large files for upload

By default, the maximum upload size for files in IBM OpenPages GRC Platform is 250 MB. If you have files that are larger than this limit, you can configure the system to upload larger files. Files greater than 2 GB are not supported.

Procedure

1. Log on to the application server as a user with administrative privileges.
2. Click **Administration** > **Settings** > **Applications** > **Common** > **Max File Upload Size**

   Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.
3. In the **Value** field, type the maximum upload size as a numeric value followed by a single letter to represent the unit. For example: 200K, 500M or 1G.
4. Click **Save**.
5. Restart the OpenPages GRC Platform application service.

   For details on starting services, see Chapter 20, “Starting and stopping servers,” on page 549.

Disabling the Files of OPX

You can use the **Disable the Files of OPX** setting to temporarily enable management of system files in the OPX administrative interface. System folders and files can also be accessed by using **Administration** > **Manage System Files**.

Administration > Settings > Applications > Common > Disable the files of OPX

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: true

Values:

- **true** - the Files menu item in the OPX administrative interface is hidden.
- **false** - the Files menu item in the OPX administrative interface is displayed. Users access it to manage system folders and files.

Signature and lock settings

IBM OpenPages GRC Platform allows users to create "signatures" on objects. A signature is a note that signifies the user agreement that the object meets with the user approval. It has no enforcement powers, and does not prevent the item from being modified after approval is given.

A signature lock is a lock that is placed on an object and its descendants. It prevents the objects from being modified. The lock is activated by placing a signature on an object. After the signature is added, the lock is active. The signed object and all of its associated child objects 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.

All of the following actions are accessed from the Applications folder.

To access the Application folder settings menu item, you must have the Settings application permission set on your account. From the navigation bar, select **Administration** > **Settings**.

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Signatures

Signatures are added on the Detail page of an object type by clicking the **Signatures** field. If configured, users can add, edit, and revoke signatures for the specified object type from the **Actions** menu on the **Signature** pane.

The **Actions** menu is hidden from users who do not have the correct permissions.

When you configure signatures for a specific object type (such as **Processes** or **Accounts**), you grant permission to a group of users to add a signature. The group is able to add, edit, or revoke a signature for the specified object types to which they have Read access.

To enable a user group to add or revoke signatures directly on an object, you must configure the **Permission** setting for the specified object type. For details, see “Configure signatures” on page 328.

Configure signatures

When you add a group to an object type setting for signatures, sign-off is enabled for objects of that type. Users who belong to the group can add and revoke signatures. Click **Actions** on the **Signatures** pane to add a signature to the object type.

Note: Only groups that are defined in object type can sign off on objects of that type. Sub groups of a group do not inherit the sign-off permission.

Administration > Settings > Applications > GRCM > Signature > Permission

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: enabled

Values: In the **Value** box on the setting detail page, complete the following steps:

- To configure groups to add a signature to an object type, type the name of the group 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 is defined as follows: **Auditors,Managers**

- To disable one or more user groups from adding a signature to the selected object type, delete the group name.

Configure 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 creates a lock on the object. It prevents further changes to the object and any object that is associated with it. Revoking a signature removes the associated lock.

Note: When the locking feature is enabled, users can create signatures only on items to which they have Write privileges.

Administration > Settings > Applications > GRCM > Signature > Mode

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: none

Values: In the **Value** field, type one of the following values:

Table 104: Lock values

Value	Action
None	No lock is applied to the object when a signature is added.
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, "Configure signatures" on page 328).

Configure cascading signatures

When a signature is added to a parent object, you can automatically apply signatures to all associated objects in the hierarchy, below the signed object. For example, signing a process applies the signature to any sub processes, accounts, risks, controls, and tests that are associated with the process.

This feature is turned off by default. It is enabled through the **Cascade** setting.

Note: To enable cascading signatures, the **Mode** setting must have the **Cascade** value set (for details see, "Configure signature locks" on page 329).

Administration > Settings > > GRCM > Signature > Cascade > <object>

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: none

Values: In the **Value** box on the setting detail page, complete the following steps:

- 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 is set to the following value: **SOXSubprocess,SOXAccount,SOXRisk**

- To remove a cascading signature from child objects, delete the name of the child object type.

Lock and unlock objects

Locks can be applied to objects without the use of signatures.

Users lock entire object hierarchies by adding a signature, if Autolock is enabled, or by selecting **Lock this** on the Actions menu of an detail page.

The **Lock** and **Unlock** application permissions control whether users can lock and unlock objects. For details, see “Configure the Lock and Unlock application permissions ” on page 330.

Note: Unlocking an object using the **Actions** > **Unlock this** menu item does NOT revoke the signature.

For information about globally unlocking business entities, see “Globally unlock business entities” on page 332.

Access privileges for locking

By default, "Read" permission is required to lock an object. This setting can now be configured through a 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 can 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.

Configure the Lock and Unlock application permissions

The **Lock** and **Unlock** application permissions control whether users can lock and unlock objects.

The **Lock** application permission allows a user to lock any unlocked object, as long as the user has Write permission to the object and all 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 down the hierarchy.

You assign application permissions either to a role template or to a user group that a user belongs to.

- On a role template, the **Lock** and **Unlock** application permissions are defined in:
  - **Administration** > **Role Template** > **<role template>** > **Role Permissions** > **Files** > **Lock**
  - **Administration** > **Role Template** > **<role template>** > **Role Permissions** > **Files** > **Unlock**
- On a user group, the **Lock** and **Unlock** application permissions are defined in:
  - **Administration** > **Users, Groups and Domains** > **<group>** > **Permissions** > **Files** > **Lock**
  - **Administration** > **Users, Groups and Domains** > **<group>** > **Permissions** > **Files** > **Unlock**

For more information, see “Defining application permissions” on page 31.

Configure the Lock menu item for object types

You can configure the display of the **Lock this** menu item on the **Actions** menu for various object types through the **Display Lock Button** setting. This setting applies to manual and automatic signature locking.

For users to see the **Lock this** menu item on the **Actions** menu of an object type, the user must be assigned the **Lock** application permission. For details, see “Configure the Lock and Unlock application permissions ” on page 330.

Administration > Settings > Applications > GRCM > Locks > Display Lock Button

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: none

Values:

- To add an object type, type the name of the object type that is separated by a comma.

For example: SOXBusEntity, SOXAccount, SOXSubaccount, SOXProcess, SOXSubprocess, SOXControlObjective, SOXRisk, SOXControl, SOXTest, SOXTestResult, SOXSignature, SOXIssue, SOXTask, SOXDocument, SOXExternalDocument.

- To remove an object type, delete the name of the object type from the list.

Lock child objects when a parent 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.

For example, you want to lock child Process objects whenever a business entity is locked. You would enter SOXProcess in the setting Value box for SOXBusEntity. When a business entity is locked, users would not be able to add, associate, copy, and disassociate processes to the locked business entity. The child objects of that process 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.

Administration > Settings > Applications > GRCM > Locked Objects > Lock Child Types

Tip: In the user interface, the OpenPages folder is hidden in the Administration Settings folder hierarchy. To author an XML settings path, include the OpenPages folder after the Settings folder in the path.

Default: none

Values: 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.

Find the exact object name listed under the **Allowed Associations** folder.

Note: If there are multiple child object types, you must add a comma to separate each object name. For example: SOXProcess, SOXControl,SOXIssue,SOXDocument,SOXExternalDocument,SOXSignature

Enable icons 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** icons 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 icons (Add New, Associate, Copy From, and Disassociate) *only* on the Processes and Loss Events tabs. Note that the Associate icons also display on the SOXProcess and LossEvent detail pages.

Configure the registry to enable associations of child objects

You can make objects available to users for association when a parent object is locked.

For object types that are defined in the **Allowed Associations** setting, the **Add New**, **Associate**, **Copy From**, and **Disassociate** actions are enabled and **Delete** is disabled.

For object types that are not defined in the **Allowed Associations** setting, the **Add New**, **Associate**, **Copy From**, **Disassociate**, and **Delete** actions are disabled.

Administration > Settings > Applications > GRCM > Locked Objects > Allowed Associations

Tip: In the user interface, the OpenPages folder is hidden in the Administration Settings folder hierarchy. To author an XML settings path, include the OpenPages folder after the Settings folder in the path.

Default: none

Values: In the **Value** field, type the exact name of one or more child object types.

Find the object name listed under the **Allowed Associations** folder (for example, SOXBusEntity).

Note: If you have multiple object types, add a comma to separate each object type name.

When a Business Entity is locked, users can add, associate, copy, and disassociate processes to the locked Business Entity.

Note: The **Disassociation** action is not enabled on a detail page until you select the object you want to disassociate.

Globally unlock 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** icon 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.

Procedure

1. Go to **Administration** > **Users, Groups and Domains** and select the **Workflow, Reporting and Others** page.
2. Add a new group 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**.

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 if locks are ignored. These settings 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.

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.

Administration > Settings > Applications > Common > Object Reset > Logging Level

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: high

Values:

- `low` - Only error messages are displayed.
- `medium` - Both error and warning messages are displayed.
- `high` - Errors, warnings, and informational or diagnostic messages are displayed.

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.

Administration > Settings > Applications > Common > Object Reset > Continue on Error

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: true

Values:

- `true` - Errors are logged and processing continues.
- `false` - Errors are logged and processing is halted.

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.

Administration > Settings > Applications > Common > Object Reset > Check ACL

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: true

Values:

- `true` - Includes all objects within the scope of the reset session.
- `false` - Includes only those objects within the reset session to which the user has access.

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 locks are ignored during an object reset session.

Administration > Settings > Applications > Common > Object Reset > Ignore Locks

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: false

Values:

- `true` - Locks on objects will be ignored when running the reset session.
- `false` - Locked objects will not be modified by the reset session.

Home page settings

For profiles, you can globally configure the display of predefined tables, the number of embedded reports, the number of objects in a table, and the number of report listings.

For configured home page filtered lists, you can set the view definition that determines which fields are displayed, the target view of the **Name** hyperlink, and the target view of the **View Details** hyperlink.

Define target of View Details hyperlink on a home page filtered list
You can use the **Show All Link** setting to specify the FLV or grid view to be used for **View Details** targets on home page filtered lists.

Administration > Settings > Applications > GRCM > Home Page

Open the profile folder that you want to customize filtered lists for (for example, OpenPages PCM 7.4.0 Master), add a new folder, and name the folder with the same name as the filter. Then, add the **Show All Link** setting.

If the settings are not available or the setting values are blank, the profile settings are used.

Tip: If you delete and then add the filtered list back to the home page, or when you add a new filtered list to the home page, the folders and settings for the filtered list are created automatically.

Note: These settings do not apply to the predefined lists on the home page (**My Checked-Out Files** and **My Reports**).

Default: blank

Values: In the **Value** box, type `Filtered List` or the name (not the label) of a specific grid view for the **View Details** target.

Order predefined panes on home page

You can use the **Items** settings to control how predefined panes are displayed on a home page. The order of the items determines the order of the corresponding HTML panes.

You can configure the following **Items** settings:

- A global **Items** setting (**Administration** > **Settings** > **Applications** > **GRCM** > **Home Page** > **Items**)
- Profile-level **Items** settings (**Administration** > **Settings** > **Applications** > **GRCM** > **Home Page** > **<profile>** > **Items**)

The following rules apply:

- The global **Items** setting defines all possible home page items and their sequence. The default is `myCheckedOutFiles,myReports`. If you remove an item from the global **Items** setting, the pane is suppressed for all users regardless of how the profile-level **Items** settings are defined.
- The profile-level **Items** settings define home page items and their sequence for users who belong to the profiles. If you remove an item from a profile-level **Items** setting, the pane is suppressed for all users who belong to the profile. Items that are not included in the global **Items** setting cannot be included in a profile-level **Items** setting.
- If you reorder the sequence of items in a profile-level **Items** setting, it overrides the global **Items** setting for users who belong to the profile.

The following examples illustrate how the settings work together.

Table 105: Examples of the Items setting at global and profile levels

If the global Items setting is...	And the profile-level Items setting is...	The result is...
`myCheckedOutFiles, myReports`	blank	None of the panes display on the specified profile.

Table 105: Examples of the Items setting at global and profile levels (continued)		
If the global Items setting is...	**And the profile-level Items setting is...**	**The result is...**
`myCheckedOutFiles, myReports`	`myCheckedOutFiles, myReports`	`myCheckedOutFiles, myReports` display for the specified profile.
blank	`myCheckedOutFiles, myReports`	None of the panes display because the global setting is blank.
`myCheckedOutFiles, myReports`	`myReports, myCheckedOutFiles`	Panes are reordered to `myReports, myCheckedOutFiles`

Administration > Settings > Applications > GRCM > Home Page > Items

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: **My Checked-Out Files** (`myCheckedOutFiles`), **My Reports** (`myReports`)

Values: In the **Value** field, add, remove, or reorder the items.

Administration > Settings > Applications > GRCM > Home Page > <profile> > Items

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: is from the global **Items** setting

Values: In the **Value** field, add, remove, or reorder the items.

Allow users to personalize the My Work home page
You can use the **My Work Home Page Can Be Personalized** setting to globally control whether users are allowed to personalize their My Work home page portlets by determining which portlets appear and in what sequence. The user can only choose to make portlets appear that are configured for display on their home page in their profile.

Administration > Settings > Applications > GRCM > Home Page > My Work Home Page Can Be Personalized

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: true

Values:

- true - users are allowed to personalize their My Work home page portlets.
- false - users are not allowed to personalize their My Work home page portlets.

Maximum number of embedded reports on the home page
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.

Administration > Settings > Applications > GRCM > Home Page > Maximum Embedded Reports

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: 2

Values: In the **Value** field, type a number greater than zero.

Note: Setting this value too high will negatively impact performance.

Maximum objects allowed in a home page pane
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.

Administration > Settings > Applications > GRCM > Home Page > Maximum Objects

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: 5

Values: In the **Value** box, type a number greater than zero.

Maximum reports allowed on the home page
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.

Administration > Settings > Applications > GRCM > Home Page > Maximum Reports Listing

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: 5

Values: In the **Value** box, type a number greater than zero.

Define target of Name hyperlink on a home page filtered list
You can use the **Detail Link** setting to customize the fields that are displayed and specify the detail or activity view to be used for hyperlink targets on home page filtered lists.

Administration > Settings > Applications > GRCM > Home Page

Open the profile folder that you want to customize filtered lists for (for example, OpenPages PCM 7.4.0 Master), add a new folder, and name the folder with the same name as the filter. Then, add the **Detail Link** setting.

If the settings are not available or the setting values are blank, the profile settings are used.

Tip: If you delete and then add the filtered list back to the home page, or when you add a new filtered list to the home page, the folders and settings for the filtered list are created automatically.

Note: These settings do not apply to the predefined lists on the home page (**My Checked-Out Files** and **My Reports**).

Default: blank

Values: In the **Value** box, type `Detail` for the detail view, or the name (not the label) of an activity view for the hyperlink target.

Define view definition used to determine fields displayed on a home page filtered list
You can use the **Fields** setting to customize the fields that are displayed on home page filtered lists.

Administration > Settings > Applications > GRCM > Home Page

Open the profile folder that you want to customize filtered lists for (for example, OpenPages PCM 7.4.0 Master), add a new folder, and name the folder with the same name as the filter. Then, add the **Fields** setting.

If the settings are not available or the setting values are blank, the profile settings are used.

Tip: If you delete and then add the filtered list back to the home page, or when you add a new filtered list to the home page, the folders and settings for the filtered list are created automatically.

Note: These settings do not apply to the predefined lists on the home page (**My Checked-Out Files** and **My Reports**).

Default: blank

Values: In the **Value** box, type `Detail` or the name (not the label) of a specific activity view to determine which fields are shown.

Define target of View Details hyperlink on a home page filtered list

You can use the **Show All Link** setting to specify the FLV or grid view to be used for **View Details** targets on home page filtered lists.

Administration > Settings > Applications > GRCM > Home Page

Open the profile folder that you want to customize filtered lists for (for example, OpenPages PCM 7.4.0 Master), add a new folder, and name the folder with the same name as the filter. Then, add the **Show All Link** setting.

If the settings are not available or the setting values are blank, the profile settings are used.

Tip: If you delete and then add the filtered list back to the home page, or when you add a new filtered list to the home page, the folders and settings for the filtered list are created automatically.

Note: These settings do not apply to the predefined lists on the home page (**My Checked-Out Files** and **My Reports**).

Default: blank

Values: In the **Value** box, type `Filtered List` or the name (not the label) of a specific grid view for the **View Details** target.

Filtered List View settings

You can globally configure the following Filtered List View page settings.

Attention: If you create a new filter that uses the character % as the value, for example `Name Contains %2`, the Name Contains value field appears empty after you load the filter: the % character does not appear. However, the filter runs properly.

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 "Modifying export settings to optimize FastMap performance" on page 653 and "Limiting the rows for import to optimize FastMap performance" on page 653.

Initial results configuration of Filtered List View

Use the **Show All Objects** setting to control whether results are displayed on a **Filtered List View** page the first-time users select an object type. By default, no results are displayed to users until a filter is selected or added.

Administration > Settings > Applications > GRCM > Filtered List > Show All Objects

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: false

Values:

- `true` - displays all available results (if any). No filter is applied.
- `false` - no results are displayed until a filter is selected or added.

Note: Users can type the percentage symbol (%) in the **Quick Filter** filed then click **Apply** to return all available results.

Advanced filters field configuration for Filtered List View

Use the **Filter on all fields in profile** setting to control whether the fields in a **Detail View** or in a user profile are available for creating an **Advanced Filter** on a **Filtered List View** page. By default, only the fields included in an object type **Detail View** page are available for creating an **Advanced Filter**.

For example, you might exclude certain system fields (such as **Creation Date** and **Created by**) and custom fields from a **Detail View** of an object type, but include these fields in the user's profile. If you wanted to make all fields included in the user's profile available for creating an **Advanced Filter**, you would set the value of the **Filter on all fields in profile** setting to `true`.

Administration > Settings > Applications > GRCM > Filtered List > Filter on all fields in profile

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: false

Values:

- `true` - all fields that are included in the user's profile are available for creating an **Advanced Filter**.
- `false` - only fields that are included in an object type **Detail View** are available for creating an **Advanced Filter**.

Maximum number of objects to export to Microsoft Excel on the Filtered List View

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.

If the number of objects that are being exported exceeds the defined number, then the user is prompted to refine their filter.

Administration > Settings > Applications > GRCM > Filtered List > Maximum Export Size

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: 1000

Values: In the **Value** field, type a number greater than zero.

Enable object type and field export choices in the Filtered List View
Use the **Enable Object Type and Field Export Choices** setting to allow users to choose which object types and fields to export.

Administration > Settings > Applications > GRCM > Filtered List > Enable Object Type and Field Export Choices

Default: true

Values:

- `true` - choosing object types and fields to export is enabled.
- `false` - choosing object types and fields to export is disabled.

Exclude object types to export in the Filtered List View
Use the **Object Types to Exclude in Export** setting to exclude object types from an export unless they are included in the Filtered List View.

Administration > Settings > Applications > GRCM > Filtered List > Object Types to Exclude in Export
Default: SOXSignature

Values: In the **Value** field, type a comma-separated list of object type names that you want to exclude. For example, if you wanted to exclude Process and Risk Assessment object types, you would type: SOXProcess,RiskAssessment.

Number of levels to export in the Filtered List View

Use the **Number of Levels to Export** setting to determine how many total levels of object types the user can choose to export, including the top-level object that is exported.

This setting is useful for limiting the growth of the tree of objects that a user can export. The number of records that are exported grows exponentially as a user selects more object types to export. For example, if a user selects a single object type, such as Process, and chooses to export its Risks, the Controls under Risks, the Test Plans under Controls and the Test Results under Test Plans, it might result in hundreds or thousands of exported records. Unless the number of levels is limited, the export might take a long time, and might impact system performance for other users.

This setting is hidden by default. For information about unhiding settings, see "Show hidden settings" on page 311.

The **Enable Object Type and Field Export Choices** setting overrides **Number of Levels to Export**. For more information, see "Enable object type and field export choices in the Filtered List View" on page 338.

Administration > Settings > Applications > GRCM > Filtered List > Number of Levels to Export
Default: View+2

Values: Possible values are View, View+1 and View+2. For example:

- If a user's **Grid View** is Process - Risk - Control, and this value is View, they can export Processes, their Risks, and their Controls. If this value is View+1, the user can export Processes, their Risks, and their Controls, and one more object type that is a direct child of Controls. If this value is View+2, the user can export one more object type that is a direct child of the first additional object type chosen.
- If a user's **Filtered List View** is for Processes, and this value is View, they can export only Processes. If this value is View+1, the user can export Processes and one more object type that is a direct child of Process. If this value is View+2, the user can export one more object type that is a direct child of the first additional object type chosen.

Note: This setting is case sensitive and there must be no spaces between the View value and the characters +1 or +2.

Maximum concurrent export requests in the Filtered List View
Use the **Concurrent Exports** setting to control the maximum number of Export to Excel (in `.xls` format) requests that are handled at the same time.

Administration > Settings > Applications > GRCM > Filtered List > Concurrent Exports

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: 10

Values: In the **Value** field, type a number greater than zero.

Editable fields in a Filtered List View
Use the **Editable** setting to control whether users can edit the fields on a **Filtered List View** page.

A value of false makes all fields in the Filtered List View read-only. A value of true enables all fields in the Filtered List View to be edited. Actual ability to edit is controlled by security settings and field dependencies. Possible values are true or false.

Attention: If you change the registry settings to allow the Filtered List View to be editable, then *all* of the fields in the Filtered List View become editable. If there are any fields in the Filtered List View that you do not want to be editable, do *not* make the Filtered List View editable.

Administration > Settings > Applications > GRCM > Filtered List > Editable

Default: true

Values:

- `true` - all fields can be edited in a Filtered List View.
- `false` - no fields can be edited in a Filtered List View; the fields are read only.

Custom settings

When enabling new content types and creating your own reports, you may need to create your own custom setting within the **Settings** menu. By default, you cannot create or delete settings until you enable the feature.

Administration > Settings > Common > Configuration > Allow Create and Delete Settings

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: false

Values:

- **true** - enable the creation and deletion of custom settings.
- **false** - disable the creation and deletion of custom settings.

Creating a custom setting

After enabling **Allow Create and Delete Settings**, you can create custom settings entries in new or existing folders.

Complete the following procedure to create a custom setting:

Procedure

1. Navigate to the folder where you want to create the new setting and select the folder.
2. Click **Add Setting**.
3. On the Settings page, type a setting name and value.
4. Select **Encrypted** if you want the value of the setting to be encrypted.
5. Click **Create** to add the new setting to the current folder.

Deleting a custom setting

After enabling **Allow Create and Delete Settings**, 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 cause unexpected behavior in the application if they are removed.

Procedure

1. Navigate to the folder that contains the setting to be deleted. Select the desired setting. The **Delete** icon becomes active.

   Note: If you select a folder, all settings within that folder are deleted.
2. Click **Delete**.
3. Click **OK**.

Copying settings and folders

You can copy individual settings to another location and copy folders to new folders. When you copy a folder, you can give the new folder a name. The settings and subfolders in the folder are copied to the new folder.

Procedure

1. Select the setting or folder that you want to make a copy of.
2. Click **Copy To**.
3. Select the folder in which the new setting or folder will be positioned.
4. If you are coping a folder, scroll down and enter the name of the new folder in **New Folder Name**.
5. Click **OK**. The new setting or folder is created.

Common folder settings

On the Settings page, in the Common folder is a selected list of individual settings.

From the navigation bar, select **Administration** > **Settings** > **Common**.

Use legacy associate

Controls whether associate operations use the new interface or the legacy interface.

You can use a registry setting to revert to using the legacy associate features in Activity Views and Detail Views only. This is to allow time to ensure that the new implementation meets your needs before you retire the old implementation.

Administration > Settings > Applications > Common > Configuration > Use Legacy Associate
The default value is false.

Permissible values are true or false.

Exclude 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 add an asterisk (*) as a value to this setting, the application validates the user name for that character before it was created. If it detects an asterisk (*) in the user name, such as Test*User, it displays an error message.

Administration > Settings > Common > Security > User Name > Illegal Characters

Tip: In the user interface, the OpenPages folder is hidden in the Administration Settings folder hierarchy. To author an XML settings path, include the OpenPages folder after the Settings folder in the path.

Default: none

Values: 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** field.

Set the system security model

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. 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 IBM OpenPages GRC Platform Professional Services.

Administration > Settings > Common > Security > Model

Tip: In the user interface, the OpenPages folder is hidden in the Administration Settings folder hierarchy. To author an XML settings path, include the OpenPages folder after the Settings folder in the path.

Default:

Values: Type the object type names you want to use as security points.

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

Disable 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.

Administration > Settings > Common > Security > Role Templates > Disable Role Group

Tip: In the user interface, the OpenPages folder is hidden in the Administration Settings folder hierarchy. To author an XML settings path, include the OpenPages folder after the Settings folder in the path.

Default: false

Values:

- `true` - Users and groups who were previously assigned that role, will lose their access control and application permissions. A disabled role template is removed from the role assignment selection list and cannot be used for further role assignments.
- `false` - Users and groups who were previously assigned that role, will retain their access control and application permissions.

Related tasks

"Enabling and disabling a role template" on page 53

Configure 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.

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 or defined using the **Self Contained Object Types** setting.

For information about the **Model** setting, see "Role-based security model" on page 43.

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 GRC Platform 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.

Administration > Settings > Common > Self Contained Object Types

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: none.

Values: In the **Value** field, 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`.

Enable the CodeCogs Equation Editor in Rich Text fields

When you enable the CodeCogs Equation Editor with the **Enable CodeCogs(r) Equation Editors** setting, users can enter mathematical equations in Rich Text fields. The equations are rendered in all views. They are also represented in Cognos reports in HTML output.
In all Rich Text fields you can click the new **fx** icon in the toolbar to open a dialog where you can enter or update a mathematical equation. You can save and render an equation on the screen in both read only and edit mode. You can load or update them in a Rich Text field with ObjectManager and Fastmap. You can also export them to Microsoft Excel from a Filtered List View or Grid.

The equation editor is only available in English.

There is source downloaded from a third-party web site, codecogs.com. If the equation editor is enabled, this site is automatically added to the security whitelist. The LaTeX version of a formula is sent to the CodeCogs web site, which returns an image of the formatted formula. If SSL is used, the formula is encrypted in transit. However, CodeCogs has access to your formula.

The formulas are displayed only in the Change History under the Source tab, not the Changes tab. In the Change History, an inserted or changed equation is highlighted in color in the Source tab. However, the color highlight is not currently supported for equations in the Changes tab.

Administration > Settings > Applications > Common > Rich Text Editor > Third Party plugins > Enable CodeCogs(r) Equation Editors

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: false

Values:

- true - equation editor is enabled.
- false - equation editor is disabled.

Platform folder settings

On the **Settings** page, the Platform folder settings represent a selected list of individual settings.

From the navigation bar, select **Administration** > **Settings** > **Platform**.

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Compare Environments tool settings

You can configure the Compare Environments tool.

From the navigation bar, click **Administration** > **Settings** > **Platform** > **CompareEnvironments** .

Java heap size for the Compare Environments tool
Use the **Max Memory** setting to configure the maximum Java heap size, in megabytes, for the Compare Environments tool.

Administration > Settings > Platform > CompareEnvironments > Max Memory
Default: 4096

Values: In the **Value** field, type a number greater than zero.

Maximum number of rows to export from the Compare Environments tool
Use the **Export Max Rows** setting to control the maximum number of rows that can be exported to Microsoft Excel (in `.xlsx` format) from the Compare Environments tool.

If the number of rows to be exported exceeds the value of this setting, the results are truncated.

The maximum value of this setting is 1048576, which is the maximum number of rows that is supported by Microsoft Excel.

The default value of this setting is 100000. If you increase the value, you might need to increase the **Max Memory** setting to avoid errors.

Administration > Settings > Platform > CompareEnvironments > Export Max Rows
Default: 100000

Values: In the **Value** field, type a number greater than zero and less than or equal to 1048576.

Set localization options

You can configure settings in the Globalization folder to audit translation label changes and set a default language for IBM OpenPages GRC Platform.

Auditing

Administration > Settings > Platform > Globalization > Auditing Enabled

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: true

Values: Enable auditing of changes that are made to translated object and application label text.

- **true** - auditing enabled.
- **false** - auditing disabled.

This option must be set to true to allow new application strings to load.

Default locale

Administration > Settings > Platform > Globalization > Default Locale

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: en_US

Values: Set the language to use to display the application user interface by default.

Note: Users can override the default locale setting by choosing another language in the **My Settings** menu item option that is located under the user name.

The following list identifies 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)

For example, to set the default language of the application interface to German, type de_DE in the **Value** field.

Configure primary associations

When a child object has multiple parent objects, the **Association Heuristic** setting controls how the system reassigns a new primary parent. The parent is assigned 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.

Administration > Settings > Platform > Repository > Resource > Association Heuristic

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: **Chronological**

Values: Type one of the following values:

- **Chronological** - the reassignment of a primary parent is based on the earliest creation date and time of an association.
- **Folder Context** - the reassignment of a primary parent is based on the folder path within the context of the business entity.

  For example, control C1 has multiple risk parents: R1, R2, R3, and R4 (primary parent) and the object associations were created in the following chronological order:

Table 106: Parent folder path and associated child folder path

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 is 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, the chronological order is used.

Configure the legacy move behavior

The Legacy Move Behavior setting controls how IBM OpenPages GRC Platform handles storage locations when a self-contained object is moved.

Administration > Settings > Platform > Repository > Resource > Move > Self-Contained Object Types > Legacy Move Behavior

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: true

Values:

- **true** - objects that are stored within the self-contained object hierarchy are moved to a corresponding folder in the new location. Objects that are stored outside of the self-contained object hierarchy are left in their original location. Use this option if the location of the objects plays an important role in security or object management.
- **false** - the system uses hierarchical based logic when a self-contained objects is moved. All objects with primary associations are moved to the logical location dictated by the object relationship hierarchy. Use this option to allow the system to reorganize object storage so that it mirrors the relationship hierarchy.

Configure the host setting

If you have older JSP reports and want to send email notifications to users from these older JSP-based reports or the Notification Manager utility, configure the host setting.

Note: This setting is only used for backward compatibility.

Administration > Settings > Platform > Publishing > Mail

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: none

Values: Click the name of a setting that is listed in the following table to open its detail page, and change the value as follows.

Table 107: Host settings

Setting	Description
Enabled	Set the value to `true`.
From Address	Verify or enter the email address of the sender using a valid email 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`

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 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.

For example, in the following example hierarchy , 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 is maintained if the **Cross context sharing** setting is enabled (set to true). If the setting is disabled (set to false), the copied tree ends 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. The non-primary association from R2 to C1 falls within the context of the copy operation.

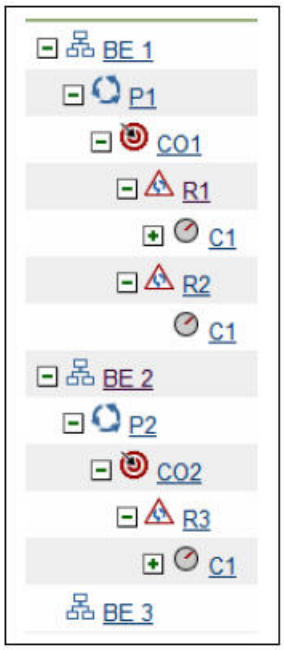


Figure 18: Sample Hierarchy

Administration > Settings > Platform > Repository > Resource > Copy > Cross context sharing

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: false

Values: In the **Value** field, type one of the following values:

- `true` - Cross-context sharing is enabled and the copy operation maintains any non-primary links to objects that are outside the scope (context) of the copy.
- `false` - Cross-context sharing is disabled and the copy operation ignores any non-primary links to objects that are outside the scope (context) of the copy.

Platform Reporting Framework folder settings

The settings in the **Administration** > **Settings** > **Platform** > **Reporting Framework V6** folder apply to the reporting framework used by Cognos Analytics.

Note: In reference to Reporting Framework V6, V6 refers to the latest framework version, not to any specific OpenPages release number.

For more information, see the following topics:

- Chapter 25, “Configuring and generating the reporting framework,” on page 659
- “Configuring settings that apply to all framework models” on page 665
- “Configuring framework models ” on page 669

Reporting Schema folder settings

The reporting schema folder settings represent a selected list of individual settings.

From the navigation bar, select **Administration** > **Settings** > **Platform** > **Reporting Schema**.

Add indexes for fields in the reporting schema

You can add an index to any RT_ table in the database through the **Create Index on Fields** setting.

Before configuring this setting, complete the following tasks:

- Review this task with your database administrator and your IBM representative.
- Test the change by manually creating the index in the database before making a permanent change in IBM OpenPages GRC Platform.

You can create a string up to 4000 characters.

Configure this setting only after careful analysis of your data query patterns. Adding too many indexes to a table can harm performance.

Administration > Settings > Platform > Reporting Schema > Create Index on Fields

Default: none.

Values: In the **Value** field, 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.

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 information, see "Changes that require the reporting schema to be regenerated" on page 89.

Example 1: Adding an index on name and reporting period
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
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.

Security settings

The security settings represent an individual settings to configure settings.

All of the following actions are accessed from the Platform Security folder.

From the navigation bar, select **Administration** > **Settings** > **Platform** > **Security**.

Redirect the security logoff link

By default, click **Log Off** in the header pane to log the user out of IBM OpenPages GRC Platform.

If you are using single sign-on (SSO), you can change the page that is displayed after you log off by modifying the value of **Logout URL**.

Note: If you are not using single sign-on, you cannot redirect the logout link.

Administration > Settings > Platform > Security > Logout URL

Default: none

Values: In the **Value** field, type a qualified URL.

Configure security for user logon

Configure settings to prevent users from logging in to IBM OpenPages GRC Platform.

Locking a user account prevents the user from logging in to OpenPages GRC Platform. However, the user is still an active user in the system, and can be selected through the user selector.

Users can be locked automatically if they exceed a set number of unsuccessful login attempts. If the user is locked out because they forgot their password, you can unlock their account and reset their password from the **View, Edit, or Disable User** page. For more information, see "Modifying user accounts" on page 28. If there is concern that the login attempts are malicious, contact your security department.

The **User Locking** folder contains the following settings that control the locking behavior of OpenPages GRC Platform.

Administration > Settings > Platform > Security > User Locking

Values: Click a setting to open its detail page, and type a value in the **Value** field.

Table 108: Locking values

Value	Description
Enabled	Sets whether the User Locking settings are active. When the value is set to `true`, users are locked after they unsuccessfully log in more than the allowed amount.
Maximum Allowed Attempts	Sets the maximum times that a user can unsuccessfully log in to the application before the account is locked.
Timeout	Sets the amount of time (in minutes) that the user account is locked.
Unsuccessful Login Window	Sets the amount of time (in minutes) that must elapse before a reset is allowed.

Security cross-site scripting filter settings

Cross-site scripting (XSS) is a 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 IBM OpenPages GRC Platform. The **Cross-site Scripting Filter** setting enables basic filtering of common attacks. The **Advanced XSS Filter** setting turns on more aggressive filtering of JavaScript actions. The **IE XSS Filter** setting is used to set the X-XSS-Protection header on a request. However, the preferred approach is to use the **X-XSS-Protection** header setting.

For more information about the **X-XSS-Protection** header setting, see “Configure the HTTP response headers” on page 353. If there is a conflict between the **IE XSS Filter** and **X-XSS-Protection** settings, the one that enables the header is used.

To allow certain HTML elements or attributes to pass through this filter, see “Configure the security safe tags setting” on page 352.

Attention: The XSS filter blocks attempts to save text fields that contain JavaScript. The XSS filter also blocks updates to items that were created and saved with JavaScript when the XSS filter was disabled. Text fields that contain JavaScript are not supported.

Note: These settings are hidden by default. To display them, see “Show hidden settings” on page 311.

Administration > Settings > Platform > Security > Cross-site Scripting Filter

Default: `true`

Values: In the **Value** field, type one of the following values:

- `true` - Cross-site filtering is enabled.
- `false` - Cross-site filtering is disabled.

Restart all application servers in your cluster to enable the change. For information, see Chapter 20, “Starting and stopping servers,” on page 549.

Administration > Settings > Platform > Security > Advanced XSS Filter

Default: `true`

Values: In the **Value** field, type one of the following values:

- `true` - Advanced XSS filtering is enabled.
- `false` - Advanced XSS filtering is disabled.

Restart all application servers in your cluster to enable the change. For information, see Chapter 20, “Starting and stopping servers,” on page 549.

Administration > Settings > Platform > Security > IE XSS Filter

Default: `false`

Values: In the **Value** field, type one of the following values:

- `true` - XSS filtering at the browser level is enabled.
- `false` - XSS filtering at the browser level is disabled.

Restart all application servers in your cluster to enable the change. For information, see Chapter 20, “Starting and stopping servers,” on page 549.

Configure the security safe tags setting

When the **Cross-site Scripting Filter** setting is enabled, certain HTML elements are blocked by that filter.

For more information on enabling this filter, see “Security cross-site scripting filter settings” on page 351. You can use the **Safe Tags** setting to globally allow certain HTML elements to pass through the filter.

For example, your company uses embedded forms to capture information that is 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 is 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
```

Administration > Settings > Platform > Security > Safe Tags

Default: By default, the HTML `style` element is the only element that is allowed through the XSS filter.

Values: In the **Value** field, type the name of an HTML element or attribute. Multiple values must be separated by a comma.

Restart all application servers in your cluster to effect the change. For details, see Chapter 20, "Starting and stopping servers," on page 549.

Configure the HTTP response headers

Administration > **Settings** > **Platform** > **Security** > **Headers**

Configure the HTTP response header settings to add security that controls what a browser renders on a page. There are four settings:

- Content-Security-Policy

  Controls from where the page can download source. If enabled, the value of this setting is merged with the value set by the system and added as a header to all page responses. The X-Content-Security-Policy header will also be set. The system value also includes the host name of the reporting server and some other settings required by the application.

  Example value: `default-src myserver.com:100`
- X-Frame-Options

  Controls where a page can get source to render in a frame. This header is added to all page responses. The value here overrides the default, which is `SAMEORIGIN`.

  Example value: `DENY`
- X-Content-Type-Options

  Prevents the browser from trying to determine the content-type of a resource that is different than the declared content-type. This header is added to all page responses. To override the default, enter an invalid string, for example, a space character.

  Default: `nosniff`
- X-XSS-Protection

  Enables X-XSS-Protection header on server responses. If X-XSS-Protection is set to true, the X-XSS-Protection header is set to `1; mode=block`. Using the X-XSS-Protection header setting is preferred to using the IE XSS Filter setting. If there is a conflict between the IE XSS Filter and X-XSS-Protection settings, the one that enables the header is used. For more information about the IE XSS Filter setting, see "Security cross-site scripting filter settings" on page 351.

  Default: false

Workflow implementations settings

The settings in the Platform Workflow Implementations folder control aspects of the integration of IBM OpenPages GRC Platform and IBM Business Process Manager.

From the navigation bar, select **Administration** > **Settings** > **Platform** > **Workflow Implementations** > **IBM BPM**.

When you create the toolkits during the IBM Business Process Manager installation, the following values for the workflow implementation settings are defined in the `op-bpm-registry-entries-opconfig.xml` file:

- **Enable Login SSO** is set to true.
- **Portal Page Path** contains the URL of the default Process Portal page that is customized for OpenPages.

- **Server URL** contains a URL for the BPM process center. It is generated based on your configuration. If the OpenPages GRC Platform application server is integrated with the BPM process server, you must set this value to the URL for the BPM process server.

You must override the default values delivered with the system with the values in the `op-bpm-registry-entries-opconfig.xml` file. To do this, you can use the Object Manager to load the entries from the `op-bpm-registry-entries-opconfig.xml` file. For more information, see Chapter 23, "The ObjectManager tool," on page 589. Alternatively, you can manually copy the default values from `op-bpm-registry-entries-opconfig.xml` to the settings.

Set auto-login

With the **Enable Login SSO** setting, you can control whether auto-login is used. If it is enabled, OpenPages users can access the IBM BPM menu items in OpenPages without having to log in to IBM BPM.

Administration > Settings > Platform > Workflow Implementations > IBM BPM > Enable Login SSO
Default: false

Values:

- `true` - to enable auto-login from OpenPages to IBM BPM.
- `false` - to disable auto-login from OpenPages to IBM BPM.

Customize the Process Portal Page Path

With the **Portal Page Path** setting, you can customize the page that is displayed when users click the **Process Portal** tab on the Home page. The system appends the value in the **Portal Page Path** setting to the base value entered in the **Server URL** setting to create the full URL.

There are three ways to configure the **Process Portal** tab on the Home page:

- Use the default BPM Process Portal page. On this page, the **Log out** icon in the navigation pane is displayed but is non-operative. If a user clicks **Log out**, they are not logged out of BPM.
- Use the default Process Portal page that is customized for OpenPages. On this page, the **Log out** icon in the navigation pane on the **Process Portal** tab is hidden.
- Create your own customized page. If you do this, hide the **Log out** icon.

Administration > Settings > Platform > Workflow Implementations > IBM BPM > Portal Page Path
Default: *<default value>*

Values: In the **Value** box, set to blank or type the path of the customized Process Portal page.

- blank - use the default BPM Process Portal page.
- `<default value>` - use the default Process Portal page that is customized for OpenPages from the `op-bpm-registry-entries-opconfig.xml` file or use your own customized page.

Configure the IBM BPM server URL
With the **Server URL** setting, you can configure the IBM BPM server URL. **Server URL** contains the base URL of the BPM installation. Use the `https` protocol rather than `http` in the URL. Additionally, if you provide a URL, the IBM BPM menu items in OpenPages are displayed. The menu items are displayed after you log out and log back in. If you do not provide a URL, the menu items are hidden.

Administration > Settings > Platform > Workflow Implementations > IBM BPM > Server URL
Default:

Values: In the **Value** box, type the name of your IBM BPM server URL, for example, `https://bpmserver:9443/`.

If you are using auto-login, the **Server URL** and the `logout.url.ibmbpm` setting in the `aurora.properties` file must use the same hostname/FDQN.

Integration with BPM Process Center and BPM Process Server

If the OpenPages GRC Platform application server is integrated with the BPM process center, set **Server URL** to the URL for the BPM process center. The **Administration** > **IBM BPM Process Center** menu item is displayed and opens the URL you enter.

If it is integrated with the BPM process server, set **Server URL** to the URL for the BPM process server. You must also hide the **Administration** > **IBM BPM Process Center** menu item:

1. Click **Administration** > **GRCM** > **NavigationMenu** > **Administration** > **Management** > **Subitems**.

   The setting contains a comma-separated list, for example:

   ```
   ReportingSchema,Search,__separator__,ObjectReset,ReportingPeriods,
   __separator__, IBM_BPM_ProcessCenter, IBM_BPM_ProcessInspector,
   IBM_BPM_ProcessAdmin, __separator__, CognitiveServices,
   __separator__, RCA_Integration,__separator__,
   LdapConfiguration
   ```

2. Remove `IBM_BPM_ProcessCenter` from the list, for example:

   ```
   ReportingSchema,Search,__separator__,ObjectReset,ReportingPeriods,
   __separator__, IBM_BPM_ProcessInspector, IBM_BPM_ProcessAdmin,
   __separator__, CognitiveServices, __separator__, RCA_Integration,
   __separator__, LdapConfiguration
   ```

3. Save the change.

User Preferences folder settings

The User Preferences folder settings represent a selected list of individual settings in the `User Preferences` folder.

All of the following actions are accessed from the `Platform` folder.

From the navigation bar, select **Administration** > **Settings** > **User Preferences**.

Set alert notification behavior

Set which alert notifications are displayed to application users in the `Alerts` folder. You can select various alert notification settings in the **Alerts** page.

Application users can change these default settings through their **My Settings** pane.

Administration > Settings > User Preferences > Alerts

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Default: false.

Values: Select the name of a setting on the **Alerts** pane to open its detail page. In the **Value** box, type one of the following values:

- `true` - An alert is displayed to application users.
- `false` - No alert is displayed to application users.

For example, 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.

Chapter 16. Configuring the global search feature

To optimize the performance of the IBM OpenPages GRC Platform global search, you can enable or disable what can be searched, tune the registry settings, and change other properties in the properties file.

About this task

For more information about using global search, see the topic *Searching for objects* in the *IBM OpenPages GRC User Guide*.

Attention:

- Security rules and evaluating security rules adds a level of overhead to user operations, including global search. The more complex the rule, the more time it takes to evaluate the rule. The number of rules that are being implemented also affects performance.

  In the case of global search, a security rule that extends read access can increase search time for users who do not have sufficient read access for an object type. Similarly, a security rule that restricts read access can increase search time for users who do have access to that object type through role-based security.
- Global search must be disabled before running the OPBackup and OPRestore utilities.

This video demonstrates how to use the OPAdminConsole to add a Global Search server to an existing environment:

https://youtu.be/qm8Am4sHwAM

For information about configuring global search to use Secure Sockets Layer (SSL), see the following topics:

- "Setting up SSL for the global search service" on page 519
- "Enabling SSL database connection between the search server and the database server" on page 521
- "Disabling the SSL database connection between the search server and the database server" on page 522

Setting up global search

Before you use IBM OpenPages GRC Platform global search in production (or even in a test environment against a large set of data), it is recommended that you first set up global search for a small set of data, such as a few thousand records in a test environment, and using the default settings.

About this task

You can set up search on the same server as the one hosting the IBM OpenPages GRC Platform application. Make sure that the server has at least 12 GB of RAM to host both the IBM OpenPages GRC Platform application and search feature.

Procedure

1. Install IBM OpenPages GRC Platform using the default settings. Make sure that you also install the Search Server component. Specify the default values for all the fields. For more information, see the topic *Search server post installation tasks* in the *IBM OpenPages GRC Installation and Deployment Guide*.
2. Follow the steps in the topic *Copying database driver files to the search server* in the *IBM OpenPages GRC Installation and Deployment Guide* to copy the JDBC database driver and start the search server.
3. Log in to IBM OpenPages GRC Platform with administrative privileges.

4. Click **Administration** > **Global Search**
5. Click **Create** and periodically click **Refresh** to get progress updates.

   The size of your data set, the configuration of your hardware, CPU speed, network speed, and available memory all influence the time it takes to set up global search. The process takes a few minutes on small sets of data (such as a few hundreds records) up to several hours on larger sets of data (such as a few million records).
6. After search setup is completed, the search box is available beside the **Reporting Period** drop-down box. In the search box, type some text that you want to search on and press Enter. The result of your search appears in the result view. You can refine your search by typing more or fewer terms, or by selecting the object types to limit the search.

   For more information about using global search, see the topic *Searching for objects* in the *IBM OpenPages GRC User Guide*.

   For more information about administering global search, see "Customizing global search" on page 363

Setting login information for the search server

You can set the user names and passwords that the search server uses to access the database server and the IBM OpenPages GRC Platform global search service (Apache Solr). You can set the login information before you enable global search.

About this task

When you set up passwords, they are encrypted automatically to ensure secure and authenticated access.

If you have enabled global search and you want to change the login information, see "Changing the database connection information for the search server" on page 365.

Procedure

1. On the search server, open a command prompt.
2. To change the login information that the search server uses to login to the database, enter the following commands:

   On Microsoft Windows operating systems,

```
cd <SEARCH_HOME>/OPSearch/opsearchtools/
opsearchtool.cmd setdbuserpassword -username current-username
  -password current-password -newusername new-username
  -newpassword new-password
```

   On UNIX operating systems,

```
cd <SEARCH_HOME>/OPSearch/opsearchtools/
./opsearchtool.sh setdbuserpassword -username current-username
  -password current-password -newusername new-username
  -newpassword new-password
```

Table 109: Parameters to change the database login information

Parameter	Description
current-username	The database username The value is the username that you entered in the OpenPages installation app when you configured the search server.

Table 109: Parameters to change the database login information (continued)	
Parameter	**Description**
current-password	The password of the database user The value is the password that you entered in the OpenPages installation app when you configured the search server.
new-username	The new database username
new-password	The new password for the database user

For example, the following command changes the password to `dbNEWpassword`, but keeps the same database username:

```
opsearchtool.cmd setdbuserpassword -username dbuser
-password dbpassword -newusername dbuser -newpassword dbNEWpassword
```

The following command changes both the database username and the password:

```
opsearchtool.cmd setdbuserpassword -username dbuser
-password dbpassword -newusername dbNEWuser -newpassword dbNEWpassword
```

3. To change the login information for the global search service (Apache Solr), enter the following commands:

   On Microsoft Windows operating systems,

   ```
   cd <SEARCH_HOME>/OPSearch/opsearchtools/
   opsearchtool.cmd setsolruserpassword -newusername new-solr-username
       -newpassword new-solr-password
   ```

   On UNIX operating systems,

   ```
   cd <SEARCH_HOME>/OPSearch/opsearchtools/
   ./opsearchtool.sh setsolruserpassword -newusername new-solr-username
       -newpassword new-solr-password
   ```

Table 110: Parameters to change the global search service login information	
Parameter	**Description**
new-solr-username	The new username for the Solr service The Solr user does not need to be an OpenPages user.
new-solr-password	The new password for the Solr user

Note: You do not need to provide the current username and password to change and encrypt the password for the global search service. The script uses the current login information of the database server for authentication before it allows the change. The default username and password is `OpenPagesAdministrator` / `OpenPagesAdministrator`.

For example, the following command sets the username to `solruser` and the password to `solrpassword`:

```
opsearchtool.cmd setsolruserpassword -username solruser
-password solrpassword
```

4. Start the global search services.

For more information, see “Starting the global search services by using a script” on page 553.

5. If required, set up SSL for the Solr service.

   For more information, see “Setting up SSL for the global search service” on page 519

What to do next

When you update the user name and password, the changes are applied only to the search server. You must update the database server as well to ensure the login information is synchronized.

Changing the login information for the search server

You can change the user names and passwords that the search server uses to access the database server and the global search service (Apache Solr).

About this task

When you change the passwords, they are encrypted automatically to ensure secure and authenticated access.

Procedure

1. Log on to OpenPages as a user with administrative privileges.
2. Click **Administration** > **Global Search**.
3. Click **Disable** to disable the global search component.
4. Stop the global search service.

   For more information, see “Stopping the global search services by using a script” on page 554 or “Stopping the global search services” on page 555.
5. Change the database user name or password.

   For more information, see "Changing password references" in the *IBM OpenPages GRC Platform Administrator's Guide*.
6. Change the login information to use for the database server and Apache Solr.

   For more information, see “Setting login information for the search server” on page 358.
7. Start the global search services.

   For more information, see one of the following topics:

   - “Starting the global search services by using a script” on page 553
   - “Starting the global search services on Windows” on page 554
   - “Starting the global search services on Linux or AIX” on page 555
8. From OpenPages, click **Administration** > **Global Search**
9. Click **Enable** to enable the global search component.
10. If required, set up SSL for the global search service.

    For more information, see “Setting up SSL for the global search service” on page 519 in the *IBM OpenPages GRC Installation and Deployment Guide*.

What to do next

When you update the user name and password, the changes are applied only to the search server. You must update the database server as well to ensure the login information is synchronized.

Using OPBackup and OPRestore when global search is enabled

Before you run OPBackup or OPRestore, global search must be disabled.

About this task

OPBackup is the IBM OpenPages GRC Platform backup utility that backs up the necessary product 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 GRC restore utility (OPRestore).

Procedure

1. Disable global search:
   a) Log in as an administrator.
   b) Click **Administration** > **Global Search** > **Disable**.
2. Perform OPBackup or OPRestore. For more information, see "The OPBackup utility" on page 387.
3. Enable global search:
   a) Log in as an administrator.
   b) Click **Administration** > **Global Search** > **Enable**.

   Attention: If you run the OPRestore utility, the search index becomes out of sync with the restored data in the OpenPages database. As a result, global search results might be inaccurate and incomplete. To prevent this, you must re-create the global search index. You can re-create the global search index before or after the database restore operation.
4. To re-create the global search index:
   a) Log in as an administrator.
   b) Click **Administration** > **Global Search** > **Disable**.
   c) Click **Administration** > **Global Search** > **Drop**.
   d) Click **Administration** > **Global Search** > **Create**.

Enabling and disabling global search

You can enable or disable global search.

About this task

For example, if your organization stipulates that you update passwords periodically, you can disable the global search component, reset user names and encrypt passwords, then enable the global search component.

Note: If the Global Search component is not enabled, then the Global Search Widget is not available for users to add to their **Dashboard** tabs. If you disable the Global Search component for a profile, then any existing Global Search widgets are removed from users' **Dashboard** tabs the next time they log on to OpenPages.

Procedure

1. Log on to OpenPages GRC Platform as a user with administrative privileges.
2. Click **Administration** > **Global Search**.
3. Click **Disable** to disable the global search component.
4. Click **Enable** to enable the global search component again.

Enabling and disabling file attachment searching

From the global search administration page, you can toggle between enabling and disabling the file attachment search component for all search-enabled file types.

Before you begin

You must make sure that the `openpages-storage` location is accessible to the global search server before enabling file attachment search. For more information, see "Setting the root path location for file attachment search" on page 379.

About this task

In a fresh installation, file attachment search is enabled by default. In an upgrade installation, file attachment global search is disabled.

Procedure

1. Log on to OpenPages GRC Platform as a user with administrative privileges.
2. Click **Administration** > **Global Search**.
3. Click **Disable File Search** to disable the file search component.
4. Click **Enable File Search** to enable the file search component again.
5. Click **Check for Updates**.
6. When the check for updates is completed, click **Update** for the changes to take effect.

Enabling attachment file types for global search

From the SOXDocument detail page, you can specify which MIME (Multipurpose Internet Mail Extensions) types are enabled or disabled for file attachment global search.

About this task

The column **Global Search** indicates for each file type whether it is enabled for global search.

Procedure

1. Log on to OpenPages GRC Platform as a user with administrative privileges.
2. Click **Administration** > **Object Types** > **SOXDocument**.
3. Under **File Types Information**, specify whether the file types selected by check box in the **Name** column are enabled or disabled for file attachment global search.
   - Click **Enable Search**. Selected file types that are disabled become enabled, and selected file types that are already enabled stay enabled.
   - Click **Disable Search**. Selected file types that are enabled become disabled, and selected file types that are already disabled stay disabled.

   Note: Files might still be discovered after the file type of these files is disabled from search if the file type is associated with more than one MIME type. Files of this type are still discovered until all associated MIME types are excluded or are disabled from search. Follow the procedure "Removing a file type from other object types" on page 187 with each associated MIME type to remove the types from searches.
4. Click **Administration** > **Global Search**.
5. Click **Check for Updates**.
6. When the check for updates is completed, click **Update** for the changes to take effect.

Attention: Do not enable global search for file types that are binary, or that are media such as images, audio, and video. Global search ignores these file types, even if enabled.

The administrator must add or include a file type by using the **Add New** or **Include** pages before its global search setting can be changed.

Newly added or included file types are set to be disabled for file attachment global search by default.

Customizing global search

You can customize and configure global search to meet your organizational needs and policies.

Before you enable global search, you might want to evaluate your IBM OpenPages GRC Platform database schema and based on your organizational policy, determine which object types and their fields should be enabled for global search. As your IBM OpenPages GRC Platform database schema evolves, such as when you add or remove object types or fields, you can update global search to reflect those changes.

For information about configuring global search the first time you use it, see "Example: customizing global search on initial enablement" on page 364. For information about configuring global search after initial enablement, see "Example: adding or removing object types and fields with an already-enabled global search" on page 365.

Enabling or disabling object types or fields for global search

Most object types and fields that are already enabled for global search. You can change which object types and fields are enabled for global search before or global search is enabled.

About this task

For an example, see "Example: customizing global search on initial enablement" on page 364.

Changes to global search by enabling or clearing the **Global Search** check-box do not take effect until you use the **Check for Updates** command, followed by the **Update** command.

- After you add an object type or field to OpenPages schema, you must decide whether the object type or field is enabled for global search or not. After you enable or clear **Global Search**, you must use the **Check for Updates** command, followed by the **Update** command.
- After you enable or disable file attachment search, or after you add or remove MIME types from file attachment search, you must use the **Check for Updates** command, followed by the **Update** command. For more information, see "Enabling and disabling file attachment searching" on page 362 and "Enabling attachment file types for global search" on page 362.
- If you enable encryption on a field that is enabled for global search, you must disable global search before you can enable it for encryption. For more information, see "Enabling and disabling global search" on page 361. After you enable encryption, you must use the **Check for Updates** command, followed by the **Update** command.
- If you import object types and fields by using FastMap, and the imported data either has new object types or fields, or makes changes to existing object types or fields to the global search setting, you must use the **Check for Updates** command, followed by the **Update** command.
- If you import object types and fields by using Environment Manager or Object Manager, and the imported data has new object types or fields, or makes changes to existing object types or fields to the global search setting, you must use the **Check for Updates** command, followed by the **Update** command.
- If you delete an object type or a field, you must use the **Check for Updates** command, followed by the **Update** command.

Note: Anytime you click **Update**, some sort of reindexing takes place. However, when you click **Check for Updates**, no indexing occurs.

For example:

- When you add or remove fields from an object type, or add or remove MIME type from file search, this results in reindexing affected object types. The time this takes depends on how many records are under the affected object type.
- When you add a new object type, this results in reindexing the newly added object type. The time this takes depends on how many records are under the affected object type.
- Removing an object type does not result in reindexing that object type, other than the object type is removed from the index. This occurs immediately.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. From the menu bar, click **Administration** > **Object Types**.
3. Select the object type or field for which you want to enable or disable global search.
4. Click **Edit**.
5. Enable or clear **Global Search**.
6. Click **Save**.
7. Click **Administration** > **Global Search**.
8. Click **Check for Updates**.
9. When the process completes, check the logs for changes such as added or removed object types and fields. You can go back and make more changes and click **Check for Updates** to see a log of updated changes.
10. When you are satisfied with your changes, click **Update** to force the changes onto the global search index.

Example: customizing global search on initial enablement

You can customize global search to meet your requirements when you first enable it.

About this task

This example assumes that you have not yet enabled global search. You decide to eliminate the object type **SOXSubaccount** and the field **Owner** of the object type **SOXRisk** from being searchable in global search.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. From the menu bar, click **Administration** > **Object Types**.
3. Select the object type **SOXSubaccount**.
4. Click **Edit** and clear **Global Search**.
5. Click **Save**.
6. From the menu bar, click **Administration** > **Object Types**.
7. Select the object type **SOXRisk**.
8. Under **Included Field Groups**, click **OPSS-Risk**.
9. Under **Field Definitions**, click **Owner**.
10. Click **Edit** and clear **Global Search**.
11. Click **Save**.
12. From the menu bar, click **Administration** > **Global Search** and click **Create**.

    Create appears only on initial enablement.
13. Click **Refresh** periodically to get progress updates and notification of when the operation is complete. This process can take from several minutes to several hours, based on how much data you have.

Example: adding or removing object types and fields with an already-enabled global search

After global search is enabled, you can add or remove object types and fields.

About this task

This example assumes that you have enabled global search based on the example in "Example: customizing global search on initial enablement" on page 364. You now need to make changes such as adding to global search the object type **SOXSubaccount** and the field **Owner** of the object type **SOXRisk** so they are searchable. This example also assumes that you want to remove the field **Additional Description** from the field group of **MRG-BusEnt** of the object type **SOXBusEntity**.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. From the menu bar, click **Administration** > **Object Types**.
3. Select the object type **SOXSubaccount**.
4. Click **Edit** and enable **Global Search**.
5. Click **Save**.
6. From the menu bar, click **Administration** > **Object Types**.
7. Select the object type **SOXRisk**.
8. Under **Included Field Groups**, click **OPSS-Risk**.
9. Under **Field Definitions**, click **Owner**.
10. Click **Edit** and enable **Global Search**.
11. Click **Save**.
12. From the menu bar, click **Administration** > **Object Types**.
13. Select the object type **SOXBusEntity**.
14. Under **Included Field Groups**, click **MRG-BusEnt**.
15. Under **Field Definitions**, click **Additional Description**.
16. Click **Edit** and clear **Global Search**.
17. Click **Save**.
18. From the menu bar, click **Administration** > **Global Search** and click **Check for Updates**. You can look at the logs based on **Check for Updates** to find out what changes occurred.
19. Periodically, click **Refresh** to get progress updates and notification of when the operation is complete. This process can take from several minutes to several hours, based on how much data you have.
20. Click **Update** to start an update operation so that your global search index is synced with the changes you made.
21. Click **Refresh** periodically to see how far from completion the process is. This process can take from several minutes to several hours, based on how much data you have and the kind of changes you made.

    Global search is now updated and ready for use.

    During the **Update** operation, global search is offline. Any user who attempts to use global search receives a message to this effect. Plan an update during off-hours, and communicate the scheduling of the update to your users.

Changing the database connection information for the search server

You can change the connection information that the search server uses to access the database server.

Procedure

1. Disable global search and stop the global search services.

For more information, see “Stopping the global search services by using a script” on page 554 or “Stopping the global search services” on page 555.

2. Log on to the search server as a user with administrative privileges.
3. Go to *<SEARCH_HOME>*/OPSearch/opsearchtools/.
4. Open the openpages_search.properties file in a text editor.
5. Modify the database connection properties to meet the needs of your environment.

   Use the following examples as a guide.

   IBM DB2

   ```
   # Database connectivity information
   OPSearchTool.DatabaseType = DB2
   OPSearchTool.DbaseHostName = OP73-WIN-DB2
   OPSearchTool.DatabasePort = 50000
   OPSearchTool.DatabaseName = OPX
   OPSearchTool.DatabaseUserID = openpages_db_user_id
   OPSearchTool.DatabasePassword = openpages_db_password
   ```

   Oracle

   ```
   # Database connectivity information
   OPSearchTool.DatabaseType = Oracle
   OPSearchTool.DbaseHostName = OP73-WIN-ORACLE
   OPSearchTool.DatabasePort = 1521
   OPSearchTool.DatabaseName = OPX
   OPSearchTool.DatabaseUserID = openpages_db_user_id
   OPSearchTool.DatabasePassword = openpages_db_password
   ```

6. Encrypt the database password in the search properties file.

   The database password that you entered in the openpages_search.properties file is in plain text. Change the password to encrypt it. For more information, see “Setting login information for the search server” on page 358.
7. Start the global search services.

   For more information, see one of the following topics:

   - “Starting the global search services by using a script” on page 553
   - “Starting the global search services on Windows” on page 554
   - “Starting the global search services on Linux or AIX” on page 555

Displaying a custom field in global search results

The administrator can configure one additional custom field to be displayed in the search results for each object type.

About this task

By default, search results return the Name, Description, and Folder Path field values. For some object types, those fields might not contain enough details about the record to help users determine whether the record they are looking for is in the search result. As administrator, you can customize global search results to contain one additional field in the search results to help the user determine whether the record that is returned is the record for which they want the details.

This additional field is configured globally across profiles in registry settings.

The additional field supports text area and text box display types only. If any other display type is used, the search results might not display the field value correctly.

Procedure

1. Log on to OpenPages GRC Platform as a user with administrative privileges.
2. Click **Administration** > **Settings** > **Platform** > **Search** > **Result Fields**.

3. Locate the object type for which you want to add an additional field to the search result.

   If the object type for which you want to add the additional field is not listed, select **Result Fields** by clicking the check box next to it, and then click **Add Setting** to create it.
4. Select the registry setting key for which you want to add additional field for that object type.
5. Set or change the value by using the following format: *`Field-Group.Field-Name`*.

   The additional field value appears after the description system field on a new line in the items returned from a global search. For example, `OPSS-LossEv.What Happened` displays the text of the field 'What Happened' in the search result. If the field does not have any value, the field name is shown in the result, but with no value.

   Attention: You must provide the correct field-group and field-name for the additional field. If the formatting is wrong, or if the field-group or field-name do not match what is in your OpenPages schema, that additional field is not included in the search results.

   You can ensure that you use the correct field-group and field-name by going to the source. For example, you want to add a field to the Workpaper object type search results.

   a. Log on to OpenPages GRC Platform as a user with administrative privileges.
   b. Select your object type. Click **Administration** > **Object Types** > **Workpaper**.
   c. Select your field-group. From **Included Field Groups**, click the field group **OPSS-Work**.
   d. Select your field-name. From **Field Group Information**, find the name of the custom field you want to add. For example, **Audit Description**.
   e. Make sure that you have the field-group and field-name correct, for example, `OPSS-Work.Audit Description`. Follow the steps in the preceding procedure. For example, click **Administration** > **Settings** > **Platform** > **Search** > **Result Fields** > **Workpaper**.
   f. Set or change the value to `OPSS-Work.Audit Description` and click **Save**. The additional field value 'Audit Description' appears after the description system field on a new line in the items that are returned from a global search.

Global search registry settings

You can tune and customize global search to suit your organizational needs and policies.

Some settings are already optimized and do not need any changes. Some are preset on initial installation of IBM OpenPages GRC Platform. And some require attention if you make changes to global search. This section lists the available registry settings for global search, with a summary of what they do, and explains when you might need to make a change on keys that require an update.

There are also search properties that are not specified in the registry. For more information, see "The global search properties file" on page 377.

Attention: Where you are told 'Do not need to modify this registry setting unless you are instructed by customer support to do so', those registry keys must not be modified without consulting first with customer support. Changing these registry settings can result in global search not working or unexpected performance issues.

Many global search registry settings are set as hidden by default. You must unhide them first. For more information, see "Unhiding the hidden global search registry settings" on page 367.

Unhiding the hidden global search registry settings

Many global search registry settings are set as hidden by default. Before you can changes the global search registry settings, you must unhide them first.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.

2. Click **Administration** > **Settings** > **Applications** > **Common** > **Configuration** and select **Show System Generated Field Guidance**.
3. Change the value from false to true.

   You can now see all the registry settings in your IBM OpenPages GRC Platform environment.

Setting the Query Path to the global search administration server

Specifies the query path to the IBM OpenPages global search server that handles administration.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Click **Administration** > **Settings** > **Platform** > **Search** > **Admin** > **Query Path**.
3. Change the value as required.

Attention: Do not modify this registry setting unless you are instructed by customer support to do so. Changing this registry setting can result in global search not working or unexpected performance issues.

Setting the URL to the global search administration server

Specifies the URL path to the IBM OpenPages global search server that handles administration.

About this task

The value of this registry is set based on your initial installation of global search. If you decide to reinstall global search on a different server, or enable SSL, or select a different port value, you must make the appropriate change. If you enable SSL, then change `http` to `https`. If you change the server on which global search is installed, you must provide the server host name or the IP address. If you need to use a different port other than the default, you must specify the different port.

Attention: Before you change this registry key, make sure that global search is disabled. For more information, see "Enabling and disabling global search" on page 361.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Click **Administration** > **Settings** > **Platform** > **Search** > **Admin** > **Search Server Administration URL**.
3. Change the value as required.

Attention: If you are changing this registry because you want to enable SSL or because you want to change the server on which global search is installed, then you must also make the same change to the registry keys **Administration** > **Settings** > **Platform** > **Search** > **Index** > **Search Server URL** and **Administration** > **Settings** > **Platform** > **Search** > **Request** > **Search Server URL**.

Setting the progress refresh interval

Specifies the frequency (in seconds) of updating progress in the IBM OpenPages GRC Platform.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Click **Administration** > **Settings** > **Platform** > **Search** > **Index** > **Full** > **Progress Refresh Interval**.
3. Change the value as required. The default value is 30 seconds.

Attention: Do not modify this registry setting unless you are instructed by customer support to do so. Changing this registry setting can result in global search not working or unexpected performance issues.

Setting the number of records to cache

Specifies the total number of records to cache before sending to the Apache Solr server for indexing.

About this task

If you increase the value of this registry setting, the initial full index might take less time, depending on your system configuration and database provider. However, this might require more RAM, CPU, and network resources. See the section on global search properties settings on how to increase the available memory to offset out-of-memory issues if you make a change to this registry key.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Click **Administration** > **Settings** > **Platform** > **Search** > **Index** > **Full** > **Record Cache Size**.
3. Change the value as required. The default value is 100.

Attention: Do not modify this registry setting unless you are instructed by customer support to do so. Changing this registry setting can result in global search not working or unexpected performance issues.

Setting the polling interval

Specifies the polling interval (in seconds) to check for changes (added, modified, or deleted) in IBM OpenPages GRC Platform objects.

About this task

By default, global search checks every minute if your data changes in the IBM OpenPages GRC Platform database. If the database contains changes, global search syncs up the search index so that when users search, those changes are reflected in the search result.

Reducing the polling interval means that the search index is more in sync with the database changes. However, this might result in slower database performance that impacts other IBM OpenPages GRC Platform operations, as well as slower search performance due to more frequent updates. Based on the load of your system and available resources, you might find you must increase this value to 300 (5 minutes) to offset the load. If you change this value, you must disable and then enable global search for the change to take effect. For more information, see “Enabling and disabling global search” on page 361.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Click **Administration** > **Settings** > **Platform** > **Search** > **Index** > **Incremental** > **Polling Interval**.
3. Change the value as required. The default value is 60.

Setting the number of records to cache before sending to the server for indexing

Specifies the total number of records to cache before sending to the Apache Solr server for indexing.

About this task

If you increase the value of this registry, the initial full index might take less time, depending on your system configuration and database provider. However, this might require more RAM, CPU, and network resources. See the section on global search properties settings on how to increase the available memory to offset out-of-memory issues if you change this registry key.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Click **Administration** > **Settings** > **Platform** > **Search** > **Index** > **Incremental** > **Record Cache Size**.
3. Change the value as required. The default value is 100.

Attention: Do not modify this registry setting unless you are instructed by customer support to do so. Changing this registry setting can result in global search not working or unexpected performance issues.

Setting the Query Path to the Apache Solr server that handles Folder ACL indexing

Specifies the URL path to the Apache Solr server that handles Folder ACL indexing.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Click **Administration** > **Settings** > **Platform** > **Search** > **Index** > **Folder ACL Query Path**.
3. Change the value as required.

Attention: Do not modify this registry setting unless you are instructed by customer support to do so. Changing this registry setting can result in global search not working or unexpected performance issues.

Setting the language analyzer that is used by search

Specifies the two or three letter abbreviation for the language analyzer that is used by search, that is, the language that search is optimized for.

About this task

Search results might be of different quality for other languages. For best results, use one of the supported locale languages: en=English (US or UK), pt=Brazilian Portuguese, fr=French, de=German, it=Italian, ja=Japanese, es=Spanish, cjk=Chinese, Japanese, Korean, zh=Simplified Chinese.

The value of this registry is set based on your initial installation of global search. If after installing global search you decide to change the language locale of your database data, you must modify the value of this registry key to reflect the language of your text. If your data has mixed language text, such as English and Chinese, pick the language in which most of your data is created; this language becomes the main language for which global search is optimized.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Click **Administration** > **Settings** > **Platform** > **Search** > **Index** > **Language Analyzer**.
3. Change the value as required. The default value is en.

Attention: Before you make a change to this registry key, and if global search is already enabled, make sure to disable global search and drop the current index. For more information, see “Enabling and disabling global search” on page 361.

Setting the Query Path to the Apache Solr server that handles Folder ACL indexing

Specifies the URL path to the Apache Solr server that handles indexing.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.

2. Click **Administration** > **Settings** > **Platform** > **Search** > **Index** > **Query Path**.
3. Change the value as required.

Attention: Do not modify this registry setting unless you are instructed by customer support to do so. Changing this registry setting can result in global search not working or unexpected performance issues.

Setting the URL to the Apache Solr server that handles Folder ACL indexing

Specifies the URL for the search server index.

About this task

The value of this registry is set based on your initial installation of global search. If you decide to reinstall global search on a different server, or enable SSL, or select a different port value, you must make the appropriate change. If you enable SSL, then change `http` to `https`. If you change the server on which global search is installed, you must provide the server host name or the IP address. If you need to use a different port other than the default, you must specify the different port

Attention: Before you make a change to this registry key, make sure that global search is disabled. For more information, see “Enabling and disabling global search” on page 361.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Click **Administration** > **Settings** > **Platform** > **Search** > **Index** > **Search Server URL**.
3. Change the value as required.

Attention: If you are changing this registry because you want to enable SSL or because you want to change the server on which global search is installed, then you must also make the same change to the registry keys **Administration** > **Settings** > **Platform** > **Search** > **Admin** > **Search Server Administration URL** and **Administration** > **Settings** > **Platform** > **Search** > **Request** > **Search Server URL**.

Setting the number of records inserted per batch

Specifies the number of search results records that are inserted per batch.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Click **Administration** > **Settings** > **Platform** > **Search** > **Request** > **Batch Size**.
3. Change the value as required. The default value is 1000.

Attention: Do not modify this registry setting unless you are instructed by customer support to do so. Changing this registry setting can result in global search not working or unexpected performance issues.

Setting the Query Path to the Apache Solr server that handles Folder ACL search requests

Specifies the URL path to the Apache Solr server that handles Folder ACL search requests.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Click **Administration** > **Settings** > **Platform** > **Search** > **Request** > **Folder ACL Query Filter**.
3. Change the value as required.

Attention: Do not modify this registry setting unless you are instructed by customer support to do so. Changing this registry setting can result in global search not working or unexpected performance issues.

Setting the URL to the Apache Solr server that handles OpenPages search requests

Specifies the URL path to the Apache Solr server that handles search requests.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Click **Administration** > **Settings** > **Platform** > **Search** > **Request** > **Query Path**.
3. Change the value as required.

Attention: Do not modify this registry setting unless you are instructed by customer support to do so. Changing this registry setting can result in global search not working or unexpected performance issues.

Setting the number of attempts to fill the search results

Specifies the number of attempts to fill the search results defined in **Search Page Size** with viewable records after security is applied on **Result Cache Size** items.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Click **Administration** > **Settings** > **Platform** > **Search** > **Request** > **Result Cache Refill Attempts**.
3. Change the value as required. The default value is 5.

Attention: Do not modify this registry setting unless you are instructed by customer support to do so. Changing this registry setting can result in global search not working or unexpected performance issues.

Setting the number of search results records that are cached per user session

Specifies the number of search results records that are cached per user session. This value sets the upper limit for the number of results that are shown to the user.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Click **Administration** > **Settings** > **Platform** > **Search** > **Request** > **Result Cache Size**.
3. Change the value as required. The default value is 100.

Attention: Do not modify this registry setting unless you are instructed by customer support to do so. Changing this registry setting can result in global search not working or unexpected performance issues.

Setting the internal page size for search results

Specifies a two-number value that controls the total number of results that Apache Solr returns.

About this task

Results that come back from Solr are post processes, and only those results that meet the security rules of the user are kept and presented to the user. If a user has a restrictive security rule and policy, it is possible that most of what is in the initial page of 500 items might be eliminated in an attempt fill the

cache setting that is specified in **Administration** > **Settings** > **Platform** > **Search** > **Request** > **Result Cache Size**. If so, an additional 10,000 items are retired from Apache Solr and are post processed.

If your organization uses a complex security model, and many your users have restrictive security rules and policies, chances are they see fewer results than expected. Advise those users to refine their search terms. You can also help users by increasing the value of this registry key. Increasing the value of this registry key might impact search performance.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Click **Administration** > **Settings** > **Platform** > **Search** > **Request** > **Search Page Size**.
3. Change the value as required. The default value is 500|10000.

Attention: Do not modify this registry setting unless you are instructed by customer support to do so. Changing this registry setting can result in global search not working or unexpected performance issues.

Setting the URL to the Apache Solr server that handles search requests

Specifies the URL for search requests.

About this task

The value of this registry is set based on your initial installation of global search. If you decide to reinstall global search on a different server, or enable SSL, or select a different port value, you must make the appropriate change. If you enable SSL, then change `http` to `https`. If you change the server on which global search is installed, you must provide the server host name or the IP address. If you need to use a different port other than the default, you must specify the different port

Attention: Before you change this registry key, make sure that global search is disabled. For more information, see “Enabling and disabling global search” on page 361.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Click **Administration** > **Settings** > **Platform** > **Search** > **Request** > **Search Server URL**.
3. Change the value as required.

Attention: If you are changing this registry because you want to enable SSL or because you want to change the server on which global search is installed, then you must also make the same change to the registry keys **Administration** > **Settings** > **Platform** > **Search** > **Admin** > **Search Server Administration URL** and **Administration** > **Settings** > **Platform** > **Search** > **Index** > **Search Server URL**.

Setting a time limit to search before timing out

Specifies the approximate time (in milliseconds) for Apache Solr to search before timing out.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Click **Administration** > **Settings** > **Platform** > **Search** > **Request** > **Search Timeout**.
3. Change the value as required. The default value is 0.

Attention: Do not modify this registry setting unless you are instructed by customer support to do so. Changing this registry setting can result in global search not working or unexpected performance issues.

Setting an additional field in the search result set

Specifies an additional field for an object type to be returned as part of search result set.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Click **Administration** > **Settings** > **Platform** > **Search** > **Index** > **Result Fields** > ***<object type name>***.
3. For details on how to change or provide a new value, see "Displaying a custom field in global search results" on page 366.
4. If the object type for which you want to add the additional field is not on the list, you can create a new registry key for it. Select the **Result Fields** node and click **Add Setting**.

Setting whether to allow compression

Specifies if the data being passed between the Apache Solr server and the IBM OpenPages GRC Platform is compressed.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Click **Administration** > **Settings** > **Platform** > **Search** > **Allow Compression**.
3. Change the value as required. The default value is true.

Attention: Do not modify this registry setting unless you are instructed by customer support to do so. Changing this registry setting can result in global search not working or unexpected performance issues.

Setting the network connection request timeout

Specifies the network connection request timeout (in milliseconds) to the Apache Solr server.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Click **Administration** > **Settings** > **Platform** > **Search** > **Connection Timeout**.
3. Change the value as required. The default value is 5000.

Attention: Do not modify this registry setting unless you are instructed by customer support to do so. Changing this registry setting can result in global search not working or unexpected performance issues.

Setting whether to allow URL redirects

Specifies whether URL redirects are allowed.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Click **Administration** > **Settings** > **Platform** > **Search** > **Follow Redirects**.
3. Change the value as required. The default value is false.

Attention: Do not modify this registry setting unless you are instructed by customer support to do so. Changing this registry setting can result in global search not working or unexpected performance issues.

Setting the number of allowed connections from the platform

Specifies the number of allowed connections to the Apache Solr server from the IBM OpenPages GRC Platform.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Click **Administration** > **Settings** > **Platform** > **Search** > **Maximum Connections Per Host**.
3. Change the value as required. The default value is 100.

Attention: Do not modify this registry setting unless you are instructed by customer support to do so. Changing this registry setting can result in global search not working or unexpected performance issues.

Setting the number of allowed connections

Specifies the total number of allowed connections to the Apache Solr server.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Click **Administration** > **Settings** > **Platform** > **Search** > **Maximum Total Connections**.
3. Change the value as required. The default value is 1000.

Attention: Do not modify this registry setting unless you are instructed by customer support to do so. Changing this registry setting can result in global search not working or unexpected performance issues.

Setting the number of times a request is reattempted

On error, specifies the number of times a request is reattempted before reporting a request failure.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Click **Administration** > **Settings** > **Platform** > **Search** > **Request Retry Attempts**.
3. Change the value as required. The default value is 3.

Attention: Do not modify this registry setting unless you are instructed by customer support to do so. Changing this registry setting can result in global search not working or unexpected performance issues.

Setting the socket timeout for indexing

Specifies the socket connection timeout (in milliseconds) to the Apache Solr server for indexer use.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Click **Administration** > **Settings** > **Platform** > **Search** > **Socket Timeout (index)**.
3. Change the value as required. The default value is 1800000.

Attention: Do not modify this registry setting unless you are instructed by customer support to do so. Changing this registry setting can result in global search not working or unexpected performance issues.

Setting the socket timeout for searching

Specifies the socket connection timeout (in milliseconds) to the Apache Solr server for search use.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Click **Administration** > **Settings** > **Platform** > **Search** > **Socket Timeout (search)**.
3. Change the value as required. The default value is 5000.

Attention: Do not modify this registry setting unless you are instructed by customer support to do so. Changing this registry setting can result in global search not working or unexpected performance issues.

Setting the Apache Solr password

Specifies the Apache Solr password to authenticate against the user ID.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Click **Administration** > **Settings** > **Platform** > **Search** > **Solr Password**.
3. Change the value as required. The default value is encrypted text.

Attention: Do not modify this registry setting unless you are instructed by customer support to do so. Changing this registry setting can result in global search not working or unexpected performance issues.

Setting the Apache Solr user ID

Specifies the Apache Solr user ID to authenticate against the server.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Click **Administration** > **Settings** > **Platform** > **Search** > **Solr User ID**.
3. Change the value as required. The default value is 0.

Attention: Do not modify this registry setting unless you are instructed by customer support to do so. Changing this registry setting can result in global search not working or unexpected performance issues.

Setting the default number of search results to return per page

Specifies the default number of search results to return per page.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Click **Administration** > **Settings** > **Applications** > **GRCM** > **Search** > **Default Results Page Size**.
3. Change the value as required. Allowable values are 10, 25, and 50. The default value is 10.

Attention: If you change the value of this registry key to a value larger than 10, global search and overall IBM OpenPages GRC Platform performance might be impacted. This change is global to all users.

The global search properties file

To customize global search, you can specify settings in the global search properties file.

The property file is named `openpages_search.properties`, and is located in *<SEARCH_HOME>*`/OPSearch/opsearchtools/`. If you make changes to this file, you must disable and then enable global search for the change to take effect. For more information, see "Enabling and disabling global search" on page 361.

Some changes might require you to drop the global search index and re-create it.

Most properties in this file are set to the default value. Only those properties that you might need to interact with are documented; the rest must not be modified unless instructed to do so by customer support.

You can also use registry settings to tune and customize global search. For information about specifying the registry settings, see "Global search registry settings" on page 367.

Setting the error handling parameters for the indexer

Use this property to set error handling parameters for the indexer that it might run into.

About this task

During indexing (both full and incremental) the indexer can run into issues such as bad records, database errors, network issues, and so on. If so, the indexer attempts to recover from those issues and continue indexing instead of ending. It does so by entering an error-handler mode, indexing until it recovers from the error or reaches a number of retries. Those parameters are set by using four values of Major, Minor, Panic, and PanicLimit.

By default, indexing is performed on an object type by processing all records in that object type in one continuous process. If an error is encountered, the indexer enters an error-handler mode. In this mode, it processes a chunk of 100 records (the value for Major) at a time. If it still runs into an issue, it scales back to a chunk of 10 records (the value for Minor) and if it still runs into an issue, it scales back to a chunk of one record (the value for Panic). If it still runs into issues, it attempts up to PanicLimit times before giving up and skipping that record from the index, and it goes back to the chunk of Major after which it goes back to normal indexing without chunking.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Go to the *<SEARCH_HOME>*`/OPSearch/opsearchtools/` folder.
3. Open the `openpages_search.properties` file.
4. Change the OPSearchTool.IndexerErrorHandlerParameters property as required.

Attention: If you change to the `openpages_search.properties` file, you must disable and then enable global search for the change to take effect. For more information, see "Enabling and disabling global search" on page 361.

Setting the maximum opsearchtool.jar heap size

Use this property to set the maximum heap size, in megabytes, to be used by `opsearchtool.jar` for general operations.

About this task

You might need to increase the value of the OPSearchTool.SearchToolHeapSize property if you encounter out-of-memory issues during general `opsearchtool.jar` operations. The out-of-memory issues might be due to the complexity of an OpenPages schema that contains many profiles, object types, field groups, and fields.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Go to the *<SEARCH_HOME>*/OPSearch/opsearchtools/ folder.
3. Open the openpages_search.properties file.
4. Change the OPSearchTool.SearchToolHeapSize property as required.

Attention: If you change to the openpages_search.properties file, you must disable and then enable global search for the change to take effect. For more information, see "Enabling and disabling global search" on page 361.

Setting the maximum Apache Solr heap size

Use this property to set the maximum heap size, in megabytes, to be used by Apache Solr.

About this task

You might need to increase the value of the OPSearchTool.SolrHeapSize property if you encounter out-of-memory issues while indexing or searching. The out-of-memory issues might be due to the size of your records or the number of records that are indexed.

If you increase the heap size and you do not have sufficient free memory on the system, you might cause further out-of-memory issues and experience performance issues with global search.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Go to the *<SEARCH_HOME>*/OPSearch/opsearchtools/ folder.
3. Open the openpages_search.properties file.
4. Change the OPSearchTool.SolrHeapSize property as required.

Attention: If you change to the openpages_search.properties file, you must disable and then enable global search for the change to take effect. For more information, see "Enabling and disabling global search" on page 361.

Setting the maximum opsearchtool.jar heap size during indexing

Use this property to set the maximum heap size, in megabytes, to be used by the opsearchtool.jar file during indexing.

About this task

You might need to increase the value of the OPSearchTool.IndexerHeapSize property if you run into out-of-memory issues during full indexing or incremental indexing.

The out-of-memory issues might be due to the size of your records that are indexed.

If you increase the heap size and you do not have sufficient free memory on the system, you might cause further out-of-memory issues and experience performance issues with global search.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Go to the *<SEARCH_HOME>*/OPSearch/opsearchtools/ folder.
3. Open the openpages_search.properties file.
4. Change the OPSearchTool.IndexerHeapSize property as required.

Attention: If you change to the `openpages_search.properties` file, you must disable and then enable global search for the change to take effect. For more information, see "Enabling and disabling global search" on page 361.

Setting the maximum text extraction heap size during indexing

Use this property to set the maximum heap size, in megabytes, to be used for the extraction of text from file attachments during indexing.

About this task

You might need to increase the value of the OPSearchTool.TextExtractorHeapSize property if you encounter out-of-memory issues during full indexing or incremental indexing.

The out-of-memory issues might be due to the size and complexity of your file attachments.

If you increase the heap size and you do not have sufficient free memory on the system, you might cause further out-of-memory issues and experience performance issues with global search.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Go to the *<SEARCH_HOME>*`/OPSearch/opsearchtools/` folder.
3. Open the `openpages_search.properties` file.
4. Change the OPSearchTool.TextExtractorHeapSize property as required.

Attention: If you change to the `openpages_search.properties` file, you must disable and then enable global search for the change to take effect. For more information, see "Enabling and disabling global search" on page 361.

Setting the text extractor timeout limit

Use this property to limit how long, in milliseconds, to wait for the text extractor to extract text from file attachments during indexing.

About this task

You might need to increase the value of the OPSearchTool.TextExtractorTimeout property during full indexing or incremental indexing.

The timeout issues might be due to the size and complexity of your file attachments or the limits of your overall system performance.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Go to the *<SEARCH_HOME>*`/OPSearch/opsearchtools/` folder.
3. Open the `openpages_search.properties` file.
4. Change the OPSearchTool.TextExtractorTimeout property as required.

Attention: If you change to the `openpages_search.properties` file, you must disable and then enable global search for the change to take effect. For more information, see "Enabling and disabling global search" on page 361.

Setting the root path location for file attachment search

Use this property to set the file storage root path location for file attachment search.

About this task

When OpenPages search server is on a different server than the OpenPages application server, the search server must have access to the OpenPages file storage location in order for it to index file attachments. If the search server is on a Windows operating system, you can use either the Uniform Naming Convention (UNC) or Local File System (LFS) path. If the search server is on a UNIX operating system, you must use the LFS path.

Windows UNC path example:

```
\\\\OPAppServer\\shared\\OpenPages\\openpages-storage
```

Windows FLS path example:

```
C:\\shared\\OpenPages\\openpages-storage
```

UNIX FLS path example:

```
/shared/OpenPages/openpages-storage
```

Attention: You must double the "\" character in the UNC and FLS path on Windows, otherwise the path is not properly processed.

Procedure

1. Log in to IBM OpenPages GRC Platform with administrative privileges.
2. Go to the *<SEARCH_HOME>*`/OPSearch/opsearchtools/` folder.
3. Open the `openpages_search.properties` file.
4. Change the OPSearchTool.FileStorageRootPath property as required.

Global search FAQs

Questions are sometimes asked about global search and how it works.

Global search indexing

Q. How does the indexing work?

A. IBM OpenPages global search server includes an indexing service. When you click **Create** in the Administration UI, the indexing service queries the OpenPages database for records of object types and fields that are enabled for global search. Those records are read, formatted, and then indexed by Apache Solr. The index is later used for search when the global search feature is used from the OpenPages UI.

This one-time initial indexing is called full indexing. After full indexing is complete, the global search indexer service enters an incremental indexing mode. Incremental indexing mode queries the OpenPages database once a minute for modified records, newly added records, or deleted records of object types that are enabled for global search and reindexes them to keep the global search index in sync with the OpenPages data.

Q. Does global search crawl the network-attached storage (NAS) (`openpages-storage` location)?

A. OpenPages uses file storage, and shares the file storage location across all instances of OpenPages applications. By default, OpenPages global search is configured with file search enabled. So yes, if file search is enabled, access to `openpages-storage` location must be set for global search. For more information, see "Setting the root path location for file attachment search" on page 379 .

Q. Are there any regularly scheduled batch jobs?

A. Yes, there is a regularly scheduled batch job that runs. The indexer (when it is running in incremental indexing mode) runs as a regularly scheduled batch job.

Q. Are the indexes and logs stored on a local drive?

A. OpenPages global search index is a proprietary format of Apache Solr, and is stored on the local hard disk drive where the global search server is installed. OpenPages global search can be installed on any local hard disk drive on the system where you installed global search. For optimal performance, it is best to install global search on a separate solid-state drive, that is, not on the same drive as the operating system.

Q. How is the index used by the product?

A. The index is proprietary to Apache Solr, is used by Apache Solr only, and is stored on the local file system where global search is installed. The index is accessed and updated anytime global search is indexing in both full and incremental mode, and the index is looked up anytime an OpenPages user is running a search using global search.

Sizing and scaling

Q. The documentation mentions that global search can be run only as a single instance.

A. This is correct. A single instance of OpenPages global search server can handle all search requests from all OpenPages application servers.

Q. Can a single search server be shared by multiple environments, such as Development, Testing, Staging, or Production?

A. No. Each environment must have its own OpenPages global search server.

Q. We have two application servers and two Cognos servers for staging and production; do we need to have two global search servers?

A. A single OpenPages global search server works with all OpenPages application servers and Cognos servers. It is strongly recommended to have a separate global search server for staging and production.

Q. Is there a possibility of running global search when using F5 load balancing in an active-active scenario?

A. Because there is only a single instance of OpenPages global search server, there is no need for F5 load balancing.

Q. How does global search impact the database server?

A. During full indexing mode, the database server is used to serve records to the global search indexer. The same is true during incremental indexing mode, but the load on the database is less because only modified records and newly added records are read. When a user uses global search and complex security rules exist for that user, those rules are processed, so the complexity of the rules determines the impact on the database server.

Q. Do we have any metrics for indexing volumes? What is the speed? Do we have any indicative query response times?

A. There are several factors influence the indexing volume and duration. The number of object types and their fields you enabled for global search and the total number of records, as well as the data size in those records in your database, all influence how long it takes to complete the initial full indexing and how large the index size on disk is. Query response time is within seconds for most searches. In some cases, if a user has complex security rules, it's possible a search can take more than several seconds.

High Availability (HA) and Disaster Recovery (DR)

Q. We have two application servers; one acts as an active administration server and the other one is a passive disaster recovery (DR) server. Do the global search servers also need to be active and passive?

A. No. Because there is only one instance of OpenPages global search server, there is no active / passive setup for it.

Q. Indexing can be lost in a DR scenario. In a DR scenario, does global search require reindexing?

A. Yes. This requires you to fully reindex for the global search feature to become available again. However, all other OpenPages functionality continues to work as normal while the global search index is being re-created.

Maintenance

Q. Are there any backup and restore operations to be performed on the global search server?

A. There are no backup and restore requirements for OpenPages global search. However, if you restore the database from a backup, the global search index is now out of sync with the OpenPages database. In this scenario, you must re-create the global search index by first disabling global search, then dropping the index, and then creating the index.

Q. Are there any index optimizations?

A. There is no need to optimize the OpenPages global search index. Apache Solr dynamically and automatically optimizes the index over time. If you perform a bulk update that impacts over 50% of your records and you have many records - hundreds of thousands of records, for example - the automatic index optimization of Apache Solr can take several days to catch up. If you suspect search performance is suffering because of a bulk update, you can force an index optimization from the Apache Solr administration page.

Chapter 17. Using IBM OpenPages GRC Platform utilities with IBM DB2 databases

You can use the IBM OpenPages GRC Platform utilities to back up and restore the OpenPages GRC and Cognos files and configuration data.

Use the utilities that are provided with IBM DB2 to back up and restore databases in IBM OpenPages GRC Platform.

IBM DB2 and the OpenPages GRC Platform backup and restore utilities

The backup and restore utilities are installed during the IBM OpenPages GRC Platform installation.

Use the utilities that are provided with IBM DB2 to back up and restore databases in IBM OpenPages GRC Platform.

For information about developing a database backup and restore strategy, see the IBM DB2 Knowledge Center (http://www.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.admin.ha.doc/doc/c0005945.html).

For more information about backing up or restoring, see "DB2 databases for OpenPages GRC Platform backup and restore" on page 394.

Use the following utilities for backing up and restoring the IBM OpenPages environment:

- OpenPages GRC Platform backup (OPBackup) and restore (OPRestore)

  These utilities are used to backup and restore the application. For more information, see "The OPBackup utility" on page 387.

  Users can choose to run a live OPBackup. When you run a live OPBackup, OpenPages services are not stopped on the application server, which allows for maximum uptime of the OpenPages application. By default, OpenPages services are restarted.
- Cognos backup (OPCCBackup) and restore (OPCCRestore)

  These utilities are used to back up and restore OpenPages GRC Platform Cognos files. For more information, see "Using the Cognos Backup utility" on page 391.

Email notification for backup jobs

You can configure email notification when you complete an IBM OpenPages GRC Platform application backup or Cognos backup job.

Note:

- Log files for email notification are stored in the `logs` folder in the following location:
  - For OPBackup (OpenPages GRC Platform application backup):

    ```
    <OP_Home>|aurora|bin|logs with the timestamp on the log files.
    ```
  - For OPCCBackup (Cognos backup):

    ```
    <CC_Home>|tools|bin|logs with the timestamp on the log files.
    ```
- Make sure to set rules in your email client to never send emails from the OpenPages GRC Platform application server to the Spam or Junk mail folders.

Configuring backup job notification

Use this procedure to configure email parameters for IBM OpenPages GRC Platform and Cognos backup jobs.

Procedure

1. Open a command or shell window and do one of the following.
   a) For an OPBackup (OpenPages GRC Platform application backup,

      navigate to the `op-backup-restore.env` file in the `bin` directory as follows:

      - For Microsoft Windows, the bin directory is *<OP_Home>*`\aurora\bin`
      - For AIX and Linux, the bin directory is *<OP_Home>*`/aurora/bin`

   b) For a OPCCBackup (Cognos backup), navigate to the `op-cc-backup-restore.env` file in the `bin` directory where *<cc_home>* represents the installation of Cognos.

      - For Microsoft Windows, the back up path is `OPBackup <path-to-back-up-location>`
      - For AIX and Linux, the back up path is `OpBackup.sh <path-to-back-up-location>`

      where `<path-to-backup-location>` is the full path of the directory where the backed up files are located on the 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.
2. Open the selected `.env` file in a text editor.
3. Specify a value after the equal sign (=) for the parameters described in the following table and save the `.env` file.

Table 111: Backup email parameters

Parameter name	Description
BACKUP_EMAIL_NOTIFICATION _SERVER=	The host name of the outgoing mail server.
BACKUP_EMAIL_NOTIFICATION _TO_EMAIL_ID=	The name of recipients that will receive the email notification. Separate email addresses with a comma (,). **Note:** Do not type a comma after the last email 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 email in the `From:` field of the email. The email address is also used as the personal name.

Table 111: Backup email parameters (continued)	
Parameter name	**Description**
BACKUP_EMAIL_NOTIFICATION _SUCCESS_MSG_ FILE=BACKUP_SUCCESS_MSG.txt	The `BACKUP_SUCCESS_MSG.txt` file 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. The first line of the file is used as the email's subject.
BACKUP_EMAIL_NOTIFICATION _FAIL_MSG_FILE= BACKUP_FAIL_MSG.txt	The `BACKUP_FAIL_MSG.txt` file is the default file that contains the message text that is 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 email's subject.

Asynchronous background jobs and administrative functions

IBM OpenPages GRC Platform supports asynchronous execution of processes in the background.

The most common examples of these type jobs are FastMap web-based data import jobs, object resets, and reporting schema generation.

For example, after a user submits a data import file, that file is queued for loading and the import process occurs in the background. Because it is important for asynchronous background jobs to run to completion, certain administrative operations are suspended until all background jobs complete.

By default, the following administrative functions will not start until background jobs are complete:

- OPBackup command
- OPRestore command
- System Administrative Mode (SAM)

Note: To disable the default setting that checks for background jobs before you start `OPBackup` or `OPRestore`, see “Enabling and disabling asynchronous background processes checking” on page 386.

If asynchronous processes are found, error messages are written to the OPBACKUP restore log.

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 and Linux

```
/opt/OpenPages/openpages-backup-restore/op_backup_2010_07_26_09_35_42.log
```

Sample error log messages follow.

- For Oracle database environments, a sample error log message might look similar to this text:
  -
```
can-proceed:
[exec] declare
[exec] *
[exec] ERROR at line 1:
[exec] ORA-20001: There are existing processes running.
[exec] Please let them finish or terminate them before proceeding.
[exec] ORA-06512: at line 7
[exec]
```
  -
```
can-proceed:
[exec] declare
[exec] *
[exec] ERROR at line 1:
[exec] ORA-20001: There are existing object reset operations running.
[exec] Please let them finish or terminate them before proceeding.
[exec] ORA-06512: at line 7
[exec]
```
- For IBM DB2 environments, a sample error log message might look similar to this text:
  -
```
can-proceed:
[exec] ERROR near line 26:
[exec] SQL0438N Application raised error or warning with diagnostic
[exec] text: "There are existing processes running. Please let them
[exec] finish or termi".
```
  -
```
can-proceed:
[exec] ERROR near line 26:
[exec] SQL0438N Application raised error or warning with diagnostic
[exec] text: "There are existing object reset operations running.
[exec] Please let them finish or termi".
```

Enabling and disabling asynchronous background processes checking

By default, IBM OpenPages GRC Platform does not allow a backup (OPBackup) or restore (OPRestore) operation to start until all asynchronous background jobs are complete.

It is best to run all jobs to completion before you start a backup or restore operation. However, this check can be enabled or disabled as follows.

Procedure

1. Open a command or shell window on the OpenPages GRC Platform server.
2. Navigate to the `op-backup-restore.env` file in the `bin` directory.
   - For Microsoft Windows, the bin directory is *<OP_Home>*`\aurora\bin`
   - For AIX and Linux, the bin directory is *<OP_Home>*`/aurora/bin`
3. Open the `op-backup-restore.env` file in a text editor.
4. Set the `CHECK_BACKGROUND_PROCESSES` parameter in the file to true or false.
   Setting the value to true enables the asynchronous background job. If background processes are running, this value prevents OPBackup or OPRestore from starting. True is the default value. false disables the validation check for asynchronous background jobs. OPBack or OPRestore start even if background processes are running.

The OPBackup utility

OPBackup is the IBM OpenPages GRC Platform backup utility that backs up the necessary product 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 GRC restore utility (OPRestore).

When you use the OPBackup utility, the following OpenPages GRC Platform resources are backed up:

- The OpenPages GRC Platform application
- The OpenPages GRC Platform storage folder and its content
- The OpenPages GRC Platform application environment files

In a horizontal clustered environment, if the Backup Utility is run on a non-administrative server, the application database will not be included in the backup. To include this database in a backup file, run the Backup Utility on an administrative server.

OPBackup does not back up standard OpenPages tools by default. If you want to include additional files or directories, you must add them to a manifest file before you run the backup. For more information, see "Backing up custom OpenPages GRC Platform files" on page 387.

If you use IBM Business Process Manager, OPBackup does not back up the BPM database. BPM backups and restores are handled outside of the OpenPages OPBackup and OPRestore utilities. For more information, see the BPM documentation in the following topic: (http://www.ibm.com/support/knowledgecenter/SSFPJS_8.5.7/com.ibm.wbpm.admin.doc/topics/cadm_recovery_backup.html).

Depending on your configuration, if any asynchronous background jobs are detected, an OPBackup job will exit and possibly display errors (see "Asynchronous background jobs and administrative functions" on page 385).

You can also configure email notification upon completion of an OPBackup. For details, see "Email notification for backup jobs" on page 383.

Attention: If you have global search enabled, global search must be disabled before running the OPBackup and OPRestore utilities. For more information, see "Using OPBackup and OPRestore when global search is enabled" on page 360.

Backing up custom OpenPages GRC Platform files

Custom IBM OpenPages GRC Platform files, such as SiteSync or scheduled job files that are specific 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.

For example, you could add the following file to the manifest file:

- *OP_HOME*\aurora\lib\openpages-ext.jar

Before you begin

- 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 GRC Platform Customer Support.
- In a horizontal clustered environment, you must perform this procedure on each OpenPages GRC Platform Application Server in the horizontal cluster.

Procedure

1. Log on to the current OpenPages GRC Platform application server.
2. Navigate to the *OP_HOME* | aurora | bin directory and open the op_backup.manifest file in a text editor.
3. Type the full path name to all custom directory names or to 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 a live OpenPages GRC Platform backup

A live IBM OpenPages GRC Platform backup means that the application can continue running while the backup is in progress. The services are not stopped during the backup.

Note: Run live OpenPages GRC Platform backups during off-peak hours because the backup consumes processing resources.

You might encounter 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 may be 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 OpenPages GRC Platform application backup utility live, you run the `OPBackup` command with the `nosrvrst` option. This does the following:

- Backs up OpenPages GRC Platform application and environment files
- Exports the OpenPages GRC Platform application database

Procedure

1. Open a command or shell window on the OpenPages GRC Platform server.
2. Navigate to the `bin` directory as follows:
   - For Microsoft Windows, the bin directory is `\<OP_Home>\aurora\bin`
   - For AIX or Linux, the bin directory is `/<OP_Home>/aurora/bin`
3. Type the following backup command:

   Windows

   ```
   OPBackup <path-to-backup-location> nosrvrst
   ```

   AIX and Linux

   ```
   OPBackup.sh <path-to-backup-location> nosrvrst
   ```

   where:

   Windows
   <path-to-backup-location> is `<oracle_base>\admin\<SID>\dpdump`

   AIX and Linux
   <path-to-backup-location> is `<oracle_base>/admin/<SID>/dpdump`

OpenPages GRC Platform backed-up content

The backup process creates a ZIP file (`.zip`) in the `<backup-directory-name>` directory.

The ZIP file contains the following necessary backed up data files:

- IBM OpenPages GRC Platform properties files (such as `aurora.properties` and `sosa.properties`).
- Application server configuration files for IBM WebSphere.
- The `openpages-storage` directory.
- Pointers to the database schema dump extracts.
- Manifest-defined content (such as `solutions-sosa-files.zip` or `services-sosa-files.zip`).

Note:

- If a backup file is 4 GB or larger, 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 GRC Platform 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.

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.

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). After 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.
   - For Windows, the installation directory is `c:\<OP_Home>\aurora\bin`
   - For AIX or Linux, the installation directory is `<OP_Home>/aurora/bin`
2. Open the `op-backup-restore.env` file in a text editor of your choice.
3. Change the USE_GZIP_COMPRESSION= setting from `false` to `true`.

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 OpenPages GRC Platform server.
2. Navigate to the `op-backup-restore.env` file in the `bin` directory as follows.

Table 112: Installation locations

Operating system	Installation location
Windows	`<OP_Home>\aurora\bin`
AIX and Linux	`<OP_Home>/aurora/bin`

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:

Table 113: BACKUP_OP_STORAGE parameter values and their meanings	
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.

The OpenPages GRC Platform restore utility on the DB2 database

OPRestore is the IBM OpenPages GRC Platform restore utility that restores the necessary product files on the server from which it was originally run. The OPRestore utility uses a backup file that is created by the OpenPages backup utility (OPBackup).

Prerequisites

Important: Before you run the OPRestore utility, you must restore the IBM DB2 OpenPages database.

The OPRestore tool can be used only on an existing OpenPages database. It cannot be used on a database that does not have an OpenPages schema.

Restoring files

To back up or restore the IBM DB2 databases for IBM OpenPages GRC Platform, you must use the utilities that are provided with DB2. For more information about the databases in IBM OpenPages GRC Platform and backing up or restoring them, see Backing up and restoring DB2 database.

Note: To refresh a "test" environment, see “Refreshing a test environment from backup files” on page 441.

As part of the restoration process, the following OpenPages resources are restored:

- If the OpenPages storage folder was backed up, the storage folder and its content are restored.

  For information about enabling and disabling storage folder backup, see “Enabling and disabling storage backup” on page 389.
- The OpenPages application environment files are restored.
- The OpenPages database schema is populated with data restored from backup files.

Depending on your configuration, if any asynchronous background jobs are detected, an OPRestore job might exit and possibly display errors. See “Asynchronous background jobs and administrative functions” on page 385.

Running the OPRestore command

You can restore a backup using the OPRestore command.

Procedure

1. If you enabled the global search component during backup, recreate your search index so that your search results are synchronised.
   a) Click **Administration** > **Global Search**.
   b) Click **Disable** to disable the global search component.
   c) Click **Drop** to drop the search indexes.

d) Click **Create** to recreate the search indexes.

2. Stop the IBM Cognos service.
3. From a command or shell window, navigate to the bin directory as follows:
   - For Microsoft Windows, the bin directory is *<OP_Home>*\aurora\bin
   - For AIX and Linux, the bin directory is *<OP_Home>*/aurora/bin
4. Execute the following command:

   Windows

   ```
   OPRestore <backup-file-name> <path-to-backup-location>
   ```

   AIX and Linux

   ```
   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)

What to do next

Preferences related to the long string text index won't be exported by "Running the OPBackup command" on page 425, and therefore are not restored. You must "Create a long string index for an Oracle database" on page 452 pointing to the database server you are restoring to.

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 Cognos Backup utility

OPCCBackup is the Cognos utility that backs up the necessary Cognos files. The OPCCBackup utility creates a backup file that can be used by the Cognos restore utility OPCCRestore.

To back up or restore the IBM DB2 databases for IBM OpenPages GRC Platform, you must use the utilities that are provided with DB2. For more information about the databases in IBM OpenPages GRC Platform and backing up or restoring them, see Backing up and restoring DB2 database.

To back up or restore the IBM DB2 databases in the OpenPages GRC application, you must use the utilities that are provided with DB2.

When you use the OPCCBackup utility, the following Cognos resources are backed up.

- Cognos reports
- Branding and environment files

You can configure e-mail notification (with an attached log file) upon the completion of an OPCCBackup. For details, see "Email notification for backup jobs" on page 383.

The OpenPages GRC Platform file storage directory

By default, OP_DATAPUMP_DIRECTORY is the name of the directory used for storing Cognos 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.

Running the OPCCBackup command

When you use the Cognos 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 Cognos application.
   - For Microsoft Windows, navigate to *<CC_Home>*\tools\bin. By default, *<CC_Home>* is C:\OpenPages\CommandCenter.
   - For AIX or Linux, navigate to *<CC_Home>*/tools/bin.
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 Cognos 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).

   The default Content Store database export locations are:

   Windows: <oracle_base>\admin\<SID>\dpdump

   AIX: <oracle_base>/admin/<SID>/dpdump

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.

Cognos backed-up content

The Cognos backup process creates a ZIP file (.zip) in the <backup-directory-name> directory. This ZIP file contains the necessary report and environment files that can be used by the Cognos restore utility (OPCCRestore).

Note:

- If a backup file is very large (4 GB or larger), 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 IBM OpenPages GRC Platform 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). After 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 Cognos application..
   - For Windows, the bin directory is *<CC_Home>*`\tools\bin`. By default, *<CC_Home>* is `C:\OpenPages\CommandCenter`.
   - For AIX and Linux, the bin directory is *<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.
3. Change the `USE_GZIP_COMPRESSION=` setting in the file from `false` to `true`.

Using the Cognos Restore utility

OPCCRestore is the IBM OpenPages GRC Platform Cognos utility that restores the necessary Cognos files on the server from which it was originally run. The OPCCRestore utility uses a backup file created by the OPCCBackup utility.

Important: Before you run the OPCCRestore utility, you must restore the DB2 reporting database.

To back up or restore the IBM DB2 databases for IBM OpenPages GRC Platform, you must use the utilities that are provided with DB2. For more information about the databases in IBM OpenPages GRC Platform and backing up or restoring them, see Backing up and restoring DB2 database.

As part of the OPCCRestore restoration process, the following Cognos resources are restored:

- Cognos reports
- Branding and environment files

For information about refreshing a test environment, see “Refreshing a test environment from backup files” on page 441.

Running the OPCCRestore command

You can restore backed up Cognos data using the OPCCRestore utility as follows.

Procedure

1. Stop the Cognos service on the administrative server and any non-administrative servers in the cluster. For details, see “Starting and stopping the Cognos services” on page 560.
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 Cognos application.

Table 114: Installation location of the Cognos application

Operating system	Installation location
Windows	*<CC_Home>*`\tools\bin` By default, *<CC_Home>* is `C:\OpenPages\CommandCenter`

Table 114: Installation location of the Cognos application (continued)	
Operating system	**Installation location**
AIX and Linux	*<CC_Home>*/tools/bin By default, *<CC_Home>* is /opt/OpenPages/CommandCenter

4. On the administrative Cognos 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 Cognos 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 Cognos service on the administrative server and on any non-administrative servers in the cluster. For details, see "Starting and stopping the Cognos services" on page 560.

The OPCCRestore log file

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.

DB2 databases for OpenPages GRC Platform backup and restore

You must use the utilities that are provided with IBM DB2 to back up and restore DB2 databases in the IBM OpenPages GRC Platform product.

For information about developing a back up and restore strategy, see the IBM DB2 Knowledge Center (http://www.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.admin.ha.doc/doc/c0005945.html).

DB2 databases in OpenPages GRC Platform

There are two databases in the IBM OpenPages GRC Platform that require backup:

- The OpenPages GRC Platform database

  This database is the main application database that is created in the DB2 instance with Oracle Compatibility mode enabled.

- The IBM Cognos Controller database

  This database is created in another normal DB2 instance without the Oracle Compatibility feature.

OpenPages GRC Platform DB2 database backup

To accomplish a complete backup of the IBM OpenPages GRC Platform and the IBM Cognos Controller databases, you must back up each database from each of their instances. The best approach is to do an offline backup of your DB2 databases.

1. Make sure that no OpenPages GRC Platform services are running for any long running background processes (such as, object reset jobs).
2. Stop the OpenPages GRC Platform servers. For information, see Chapter 20, "Starting and stopping servers," on page 549.
3. Open a command or shell window and connect to the DB2 database.

   For Windows users only, you must use the `db2cmd` command in the **Command Prompt** window to initialize the DB2 command line processor (CLP).
4. Start the DB2 instance by using the `db2start` command.
5. Do the offline backup.

   For example, on a Microsoft Windows operating system, to back up a database with the alias name of `sample` to `c:\Db2backup`, you could use `db2 backup db sample c:\Db2backup`. A backup image will be created in the specified backup location in the following format:

   database_name`.`*backup_type*`\`*instance_name*`\`*database_partition*`\`*catalog_partition_number*`\`*backup_date_time*`\`*time_image_sequence_number*. For example, `OPX.0\DB2INST1\NODE0000.\CATN0000\20121129\131259.01`.

   On an AIX or Linux operating system, to back up a database with the alias name of `sample` to `/opt/db2backup`, you could use `db2 backup db sample /opt/db2backup`. A backup image will be created in the specified backup location in the following format:

   database_name`.`*backup_type*`.`*instance_name*`.`*database_partition*`.`*catalog_partition_number*`.`*backup_date_time*`.`*time_image_sequence_number*. For example, `OPX.0.DB2INST1.NODE0000.CATN0000.20121129.131259.001`.

   For information about backing up your DB2 database, see the IBM DB2 Knowledge Center (http://www.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.admin.ha.doc/doc/c0006150.html).
6. Stop the DB2 instance by using the `db2stop force` command.
7. Start the OpenPages GRC Platform servers.

OpenPages GRC Platform DB2 database restore

You can use a DB2 database backup from your production system to restore a DB2 database to a previous state in the same environment.

Use this process as a guide for restoring a IBM OpenPages GRC Platform DB2 database:

1. Stop the OpenPages GRC Platform servers. For information, see Chapter 20, "Starting and stopping servers," on page 549.
2. Open a command or shell window and connect to the DB2 database.

   For Windows users only, you must use the `db2cmd` command in the **Command Prompt** window to initialize the DB2 command line processor (CLP).
3. Restore the DB2 database.

   For example, on a Windows operating system, to restore a database with the alias name of `sample` from the backup location `c:\Db2backup` with a backup timestamp of `20121129131259`, you could use `db2 restore db sample from c:\Db2backup taken at 20121129131259`.

On an AIX or Linux operating system, to restore a database with the alias name of `sample` from the backup location `/opt/db2backup` with a backup timestamp of `20121129131259`, you could use `db2 restore db sample from /opt/db2backup taken at 20121129131259`.

For information about restoring your DB2 database, see the IBM DB2 Knowledge Center (http://www.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.admin.ha.doc/doc/c0006237.html).

Restoring backed up production data in a new DB2 environment

You can use a IBM DB2 database backup from your production environment to restore data to a DB2 database in a new test or development environment.

The process of restoring data involves the following tasks in this order:

1. Back up your DB2 production databases then restoring these databases to the new environment.

   When you create the IBM OpenPages GRC Platform application database, you must run scripts to enable Oracle compatibility and update configuration data. You run these scripts before you restore the OpenPages GRC Platform application production database to the new environment. These scripts are not required for the Cognos database.
2. Back up your production application and reporting data files then restore these files to the new environment.
3. Update the storage folder location in the new environment.

For information about refreshing a test environment on an existing test system, see "Refreshing a test environment from backup files" on page 397.

Before you begin

Make sure that your new test or development environment meets the following prerequisites:

- OpenPages GRC Platform is installed in the new test or development environment.
- The operating system user names in the new environment match the operating system user names in your production environment.

Procedure

1. Back up your OpenPages GRC Platform application production DB2 database.
   For more information, see "OpenPages GRC Platform DB2 database backup" on page 395.
2. Back up your IBM Cognos Controller production DB2 database.
   For information about backing up the IBM OpenPages application database, see "OpenPages GRC Platform DB2 database backup" on page 395.
3. Create the OpenPages GRC Platform application database instance in the new environment.
   For more information about creating a DB2 database, see the IBM DB2 documentation.
4. On the new OpenPages GRC Platform application database only, run the `enable-ora-compatibility` script to enable Oracle Compatibility Mode.

   In the output, look for the DB2 profile variable, `DB2_COMPATIBILITY_VECTOR`, with the value of ORA. For example, `DB2_COMPATIBILITY_VECTOR=ORA`.

   a) On Microsoft Windows, from the **Start** menu, click **All Programs > IBM DB2 > DB2COPY1 > Command Window - Administrator**, and type the following command: `enable-ora-compatibility.bat`

   Note: If you have multiple instances of DB2 on the server, make sure that you choose the DB2COPY of the OpenPages database instance.

   b) On AIX and Linux, type the following command: `./enable-ora-compatibility.sh`

Note: DB2 compatibility features are enabled at the instance level and cannot be disabled. Keep the selected compatibility level for the life of the OpenPages database. To confirm that Oracle Compatibility Mode is set, type the following command: `db2set -all`

5. On the new IBM OpenPages application database only, update the database manager configuration.
   a) For Windows users only, type the following command in the **Command Prompt** window to initialize the DB2 command line processor (CLP):

      ```
      db2cmd
      ```

   b) In the DB2 CLP, run the `opx-dbm-cfg` script:

      - On Windows, type:

        ```
        opx-dbm-cfg.bat
        ```

      - On AIX and Linux, type:

        ```
        ./opx-dbm-cfg.sh
        ```

6. Use the OpenPages GRC Platform application database backup from your production system to restore the DB2 database to your new environment.

   For more information, see "OpenPages GRC Platform DB2 database restore" on page 395.
7. Create the IBM Cognos Controller database instance in the new environment without the Oracle Compatibility feature.

   For more information about creating a DB2 database, see the IBM DB2 documentation.
8. Use the IBM Cognos Controller database backup from your production system to restore the DB2 database to your new environment.

   For more information, see "OpenPages GRC Platform DB2 database restore" on page 395.
9. Use the OpenPages GRC Platform backup and restore utilities to back up the product files on the production server then restore these files to your new environment.

   For more information about using the OpenPages GRC Platform backup utility, see "The OPBackup utility" on page 387.

   For more information about using the OpenPages GRC Platform restore utility, see "The OpenPages GRC Platform restore utility on the DB2 database" on page 390.
10. Use the Cognos backup and restore utilities to back up your reporting files on the production server then restore these files to your new environment.

    For more information about using the Cognos backup utility, see "Using the Cognos Backup utility" on page 391.

    For more information about using the Cognos restore utility, see "Using the Cognos Restore utility" on page 393.
11. Update the OpenPages storage folder location on the new test or development database.

    For more information about updating the storage folder location, see "Update the OpenPages GRC Platform storage location in the DB2 database" on page 400.

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.

You can use this procedure to refresh any test server by using the backup files from any other IBM OpenPages GRC Platform server.

Prerequisites:

- Make sure that you have access to both the production or "source" and test or "target" servers.

- The operating systems must match between source and target servers.

Prerequisites to refreshing a DB2 test environment

There are some prerequisites to refreshing a test environment.

The following are required:

- The test or "target" server and production or "source" server must have the same installed version of the IBM OpenPages GRC Platform application - including patches.
- You must have access to the following DVD either on your installation media or from a shared network drive:

  ```
  OP_n.n.n_Non_Embedded_DVD_1
  ```

  Where *n.n.n* represents the current version number of the OpenPages GRC Platform release.

Backup of production databases in OpenPages GRC Platform on the DB2 server

You must use the utilities that are provided with IBM OpenPages GRC Platform to back up the production databases in the application. The exported DB2 production databases are used later to refresh the OpenPages GRC Platform application databases on the test or target server.

For more information about the databases in OpenPages GRC Platform and backing up DB2 databases, see “DB2 databases for OpenPages GRC Platform backup and restore” on page 394.

Backing up and copying OpenPages GRC Platform application production files for a DB2 database

The IBM OpenPages GRC Platform backup utility backs up the application files. The exported data from the production backup file is used later to refresh data on the test or target server.

Procedure

1. Log on to your production OpenPages GRC Platform server as a user with administrative permissions.
2. Run the OpenPages GRC Platform backup utility (`OPBackup`) to back up the application files.
   For more information, see “The OPBackup utility” on page 387.
3. Copy the backup `.zip` or `.tar.gz` file to your test server.

Backup of OpenPages GRC Platform databases on the test server

You must use the utilities that are provided with IBM DB2 to back up the test or target databases in IBM OpenPages GRC Platform.

For more information about the databases in OpenPages GRC Platform and backing up DB2 databases, see “DB2 databases for OpenPages GRC Platform backup and restore” on page 394.

Backing up OpenPages GRC Platform application files on your test server

Run the IBM OpenPages GRC Platform backup utility to back up the application files on your test or target server.

Procedure

1. Log on to your test OpenPages GRC Platform server as a user with administrative permissions.
2. Run the backup utility (`OPBackup`) as described in “The OPBackup utility” on page 387 to backup the OpenPages GRC Platform application files.

Running the OPCCBackup command

When you use the Cognos backup utility, you run the `OPCCBackup` command in a command or shell window.

Procedure

1. From a command or shell window, navigate to the `bin` directory as follows:

   For Microsoft Windows:*<CC_Home>*`\tools\bin` By default, *<CC_Home>* is `C:\OpenPages\CommandCenter`

   For AIX or Linux, type *<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 and Linux: `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 Cognos 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.

Drop the DB2 Database for the application on the test system

You must drop the IBM OpenPages GRC Platform database on the test server. Dropping the IBM DB2 database for IBM OpenPages GRC Platform on the test system deletes all object data.

The DB2 database includes OpenPages GRC Platform application data.

Procedure

1. If necessary, log on to your IBM OpenPages GRC Platform test server as a user with administrative permissions.
2. Open a command or shell window.
3. ForWindows users only, type the following command in the **Command Prompt** window to initialize the DB2 command line processor (CLP):

   `db2cmd`
4. In the DB2 CLP, type the following command to drop the DB2 test database:

   `db2 drop db <DATABASE_NAME>`

   Where <DATABASE_NAME> is the name of the test database.

   For example, if the name of the test database is op, type `db2 drop database op`.

Copy and restore the application production DB2 database backup file to the test DB2 database server

You must use the utilities that are provided with IBM DB2 to restore the IBM OpenPages GRC Platform application database on the test system.

The OpenPages GRC database backup file from the DB2 production server includes both OpenPages GRC Platform application data.

Before you begin

The operating system user names in the test environment must match the operating system user names in your production environment.

Procedure

1. Copy the OpenPages GRC Platform database backup file from the DB2 production server to the test database server.
2. Copy the Java UDF class files from the DB2 production server folders to the folders on the test database server.
   For example:
   - On Windows systems, copy the class files from `C:\IBM\SQLLIB\FUNCTION` on the production database server to the DB2 database server on the test system.
   - On AIX and Linux systems, copy the class files from `/home/db2inst1/sqllib/function` on the production database server to the DB2 database server on the test system.
3. Restore the DB2 database to the test server. For more information, see "OpenPages GRC Platform DB2 database restore" on page 395.

Update the OpenPages GRC Platform storage location in the DB2 database

After you restore the `openpage-storage` files from the production backup, you must update the IBM OpenPages GRC Platform storage location on the test database.

Procedure

1. Log on to a system as a user with administrator privileges. You can use any system with access to CLPPlus that can connect to the OpenPages database server.
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`.

Table 115: Installation location of the OpenPages GRC Platform application	
Operating system	**Installation location**
Windows	By default, *<OP_Home>* is `C:\OpenPages`
AIX and Linux	By default, *<OP_Home>* is `/opt/OpenPages`

3. Open a command or shell window and do the following tasks:
   a) Either go to the `OP_n.n.n_Non_Embedded_DVD_1` on your network drive or insert the DVD from your installation kit.
   b) Go to the `INSTALL_SCRIPTS` directory at the following location:

      ```
      OP_n.n.n_Configuration|Database|DB2|INSTALL_SCRIPTS
      ```

      Where *n.n.n* is the version number of the IBM OpenPages product.
4. ForWindows users only, type the following command in the **Command Prompt** window to initialize the DB2 command line processor (CLP):

   `db2cmd`
5. From the `INSTALL_SCRIPTS` directory, run the `update-storage` SQL wrapper script with the following parameters to update the `openpages-storage` directory location in the database:

   ```
   clpplus -nw <op_db_user>/<op_db_password>@<database_host>:<database_port>/
   <database_name> @sql-wrapper update-storage <log-file> <database_host>
   <database_port> <data_base_name> <op_db_user> <op_db_password> <storage-
   type> <storage-server-name> <host-name> <os-type> <path-or-UNC-name>
   ```

   Where:

Table 116: Update Storage Wrapper Script Parameters	
Parameter	**Description**
op_db_user	OpenPages user name for accessing the OpenPages database.
op_db_password	The OpenPages password for accessing the OpenPages database.
database_host	Name of the DB2 server host machine that contains the OpenPages database.
database_port	Port number of the DB2 database instance that is installed on the database server. ForDB2, the default port is `50000`.
database_name	Name of the OpenPages database.
log-file	The name of the log file that the script creates and writes information to.
storage-type	The type of file storage to be used. Valid values are as follows: • LFS (local file system) • `UNC` (Universal Naming Convention) - for Windows only. **Note:** After you move from LFS to UNC, you cannot go back to using LFS.
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 as follows: • `Windows` • `Unix`
path-or-UNC name	The file path of the storage location.

Examples

- LFS (AIX and Linux)

```
clpplus -nw openpages/apassword@testdbserver:50000/opx @sql-wrapper update-
storage /home/op/upd-storage-output.log testdbserver 50000 opx openpages
apassword LFS aix11 aix11 Unix /usr/opdata/openpages-storage
```

- UNC (Windows)

```
clpplus -nw openpages/apassword@testdbserver:50000/opx @sql-wrapper update-
storage c:\temp\upd-storage-output.log testdbserver 50000 opx openpages
apassword UNC storageserver eng11 Windows \\storageserver\openpages-storage
```

Back up the Cognos Database on the DB2 production and test servers

You must use the utilities that are provided with IBM DB2 to back up the IBM Cognos Controller database on both the production and test servers. The exported DB2 production database is used later to refresh the IBM Cognos Controller database on the test or target server.

For more information about the databases in IBM OpenPages and backing up DB2 databases, see "DB2 databases for OpenPages GRC Platform backup and restore" on page 394.

Back up Cognos configuration files on the DB2 production and test servers

You must run the Cognos backup utility to back up Cognos configuration files on both the production and test servers. The Cognos configuration file backup from the production server is used later to refresh Cognos configuration on the test server.

Before you begin

Before you run the Cognos backup utility (`0PCCBackup`) make sure to verify the following:

- You have access to both the source and target database servers.
- Full permission is granted to the `CommandCenter|tools|bin` folder on the target Cognos server.

Procedure

1. If necessary, log on to your production Cognos server as a user with administrative permissions.
2. Run the Cognos backup utility (`0PCCBackup`) to back up the Cognos configuration files on the production server.

   For more information, see "Using the Cognos backup utility" on page 430.

   Tip: If the mail server for notification email is not set up for running Cognos backups, the output from the `0PCCBackup` 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 if the step before the error says `BUILD SUCCESSFUL`.
3. Copy the production Cognos server backup `.zip` or `.tar.gz` file to the Cognos backup-restore directory on the test server.
4. Run the Cognos backup utility (`0PCCBackup`) to back up the Cognos configuration files on your test server.

   For more information, see "Using the Cognos backup utility" on page 430.

Update DB2 database connection references for Cognos

You must update the database connection references for the server on the Cognos Analytics portal.

Procedure

1. From a browser, log on to the Cognos Analytics portal as a user with administrative privileges, for example, OpenPagesAdministrator.

   By default, the URL is `http://<hostname>/ibmcognos/bi`

   Where `<hostname>` is the name of the Cognos server.
2. Click **Manage** > **Administration Console** to launch the **IBM Cognos Administration** page.
3. On the **Configuration** tab, click **Data Source Connections** (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 **CLI** tab, in the **DB2 database name** box, change the DB2 database name to the Catalog Database Name of the OpenPages GRC Platform database on the target environment.
8. On the **JDBC** tab, in the **Server name**, **Port number**, and **Database name** boxes, change the values to valid values for the OpenPages GRC Platform database on the target environment.

Modify SSO and LDAP configuration in the test environment

If you are using SSO or LDAP in the test environment, modify the configuration for each if needed. Otherwise, skip this task.

Copy and restore the Cognos production database backup file to the test database server

You must use the utilities that are provided with IBM DB2 to restore the IBM Cognos Controller reporting database on the test system.

Before you begin

The operating system user names in the test environment must match the operating system user names in your production environment.

Procedure

1. Copy the IBM Cognos Controller database backup file from the DB2 production server to the test database server.
2. Restore the DB2 database to the test server. For more information, see "OpenPages GRC Platform DB2 database restore" on page 395.

Drop the DB2 Database for Cognos on the Test Server

You must drop the IBM Cognos Controller database on the test server. Dropping the IBM Cognos Controller database on the test system deletes all object data.

Procedure

1. If necessary, log on to your IBM OpenPages GRC Platform test server as a user with administrative permissions.
2. Open a command or shell window.
3. ForWindows users only, type the following command in the **Command Prompt** window to initialize the DB2 command line processor (CLP):

   ```
   db2cmd
   ```
4. In the DB2 CLP, type the following command to drop the DB2 test database:

   ```
   db2 drop db <DATABASE_NAME>
   ```

   Where <DATABASE_NAME> is the name of the test database.

   For example, if the name of the test database is op, type `db2 drop database op`.

Copy custom deliverables to the test environment

If you are using custom deliverables, you must copy any custom files to the test environment.

Copy custom triggers

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 GRC Platform 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 "Backing up and copying the OpenPages GRC Platform application production files for an Oracle database" on page 442, 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.

Table 117: Installation location of the OpenPages GRC Platform application	
Operating system	**Installation location**
Windows	*<OP_Home>*\aurora\lib\openpages-ext.jar By default *<OP_Home>* is C:\OpenPages
AIX and Linux	*<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.

Copy other custom deliverables to the test environment

If you have other custom deliverables, such as UI helpers and JSP reports, copy these custom deliverables to their respective folders on the test or target machine.

If you have any questions about the location of your custom data, contact your IBM representative.

Procedure

1. From your application production backup .zip files, extract all custom files such as JAR files, JSP files, JavaScript files, and Image files.
2. Copy these files into their respective folders on the target machine. The target folders should match the folders on the source installation.

Starting the OpenPages GRC Platform in the test environment

When finished, start IBM OpenPages GRC Platform services on the servers in your test environment.

For details, see Chapter 20, "Starting and stopping servers," on page 549.

Update URL host pointers for Cognos reports

Modify the URL host pointer settings and then propagate these changes to the reporting schema on the application server (does not require services to be restarted).

For more information, see "Updating URL host pointers for reports" on page 478.

Utilities for filtering on long string field content in a DB2 database

You can filter based on the content of long string fields if the IBM DB2 Text Search feature is enabled. This feature is also known as full text searching.

Warning: Do not include long string fields that are encrypted using field level encryption in the search criteria because they can return unexpected results.

Long string fields allow users to enter values over 4 KB in length. To apply filters on the content of these long string fields, you must install and configure the DB2 Text Search feature, see "Install and configure DB2 text search" on page 405.

If the DB2 Text Search feature is not enabled, attempts to filter on the content of long string fields will not work. For details on setting up long text fields, see "Long string fields" on page 174.

The following SQL scripts are provided to help manage full text searching:

Note: Before running these scripts, make sure the DB2 Text Search feature is installed and configured.

- "Enable DB2 text search" on page 407

- “Create a long string index in a DB2 database” on page 408
- “Create a schedule job to synchronize a long string index in a DB2 database” on page 410
- “Drop a long string index” on page 411

For information about how to disable DB2 text search, see Disabling a database for DB2 Text Search (http://www.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.admin.ts.doc/doc/t0053097.html).

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 true, filtering is enabled on long string fields.

If the value is set to false, filter is disable on long string fields. The default values is false.

For details on working with settings, see Chapter 15, “Viewing the Configuration and Settings page,” on page 307.

Install and configure DB2 text search

Install and enable the optional IBM DB2 Search Text feature to filter based on the contents of fields with long string data types. Scripts are provided for Windows, AIX, and Linux.

About this task

DB2 Text Search is an optionally installable component in a DB2 Server installation.

Procedure

1. To install DB2 Text Search:
   a) Run the custom installation type from the DB2 Server setup CD.
   b) Select **Work on existing system**.

   Note: For other DB2 Text Search installation methods, see: Configuring DB2 Text Search (http://www.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.admin.ts.doc/doc/t0052968.html).
2. After the component is installed, log on to the operating system as the instance owner.
3. Stop the DB2 instance by running the following commands:

Table 118: Commands for stopping the DB2 instance

For this operating system...	Do this...

Windows	a. Open a command window, then run `db2cmd`.
	b. In the **DB2 CLP** window, run:
	`db2 force applications all`
	`db2stop`

AIX and Linux	Run:
	`db2 force applications all`
	`db2stop`

4. Navigate to the DB2 Text Search installation folder.

   An example folder on a Windows system is:

   ```
   D:\Program Files (x86)\IBM\SQLLIB\db2tss\bin
   ```
5. To configure the DB2 Text Search feature by using the default setting, run one of the following commands.

Table 119: Commands for configuring the DB2 Text Search feature by using the default setting	
For this operating system...	**Do this...**
Windows	`db2iupdt DB2 /u:`*`DB2_INSTANCE_OWNER_NAME`*`,`*`DB2_INSTANCE_OWNER_PASSWORD`*` /j:TEXT_SEARCH` Where *DB2_INSTANCE_OWNER_NAME* is the database instance owner account. Usually `db2admin` user. Where *DB2_INSTANCE_OWNER_PASSWORD* is the password for instance owner account. For example, `db2iupdt DB2 /u:db2admin,dbpassword /j:TEXT_SEARCH`
AIX and Linux	`db2iupdt -j "TEXT_SEARCH,`*`TEXT_SEARCH_Port`*`" `*`DB_Instance_Name`* Where *TEXT_SEARCH_Port* is the port number of the DB2 Text Search services. For DB2 Text Search, the default port is 55000. Where *DB_Instance_Name* is the name of the DB2 database instance where you want to add the Text Search service.

6. To manually configure the DB2 Text Search feature, do the following.
   a) Navigate to the *<DB2_Home>*`\db2tss\bin` directory.
   b) Run this command to generate the authentication token:

      ```
      configTool generateToken -configPath "<DB2_Home>\cfg\db2tss\config" -seed
      <DB2_INSTANCE_NAME>
      ```

      Note: The default value of `<DB2_INSTANCE_NAME>` is `DB2COPY1`.
   c) From the *<DB2_Home>*`\db2tss\bin` directory, run the following command to print the status and properties of text search collections:

      ```
      adminTool status -configPath ""<DB2_Home>\cfg\db2tss\config"
      ```

      For more details, see Configuring DB2 Text Search (http://www.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.admin.ts.doc/doc/t0052968.html).

   Note: If you must reconfigure the DB2 Text Search feature, stop the text search service first. You can run this command to stop the service: `db2ts STOP FOR TEXT`
7. Start the DB2 database:
   a) Log on to the operating system with the account that was used to create the database.
   b) If you have multiple databases on the server, use these commands to set the default database:

      Windows

      ```
      set DB2DBDFT==<DATABASE_NAME>
      ```

      AIX and Linux

      ```
      export DB2DBDFT=<DATABASE_NAME>
      ```
   c) Start the database by running the following command:

      ```
      db2start
      ```
8. Start DB2 Text Search services:
   a) Log on as the database instance owner.
   b) Run the following command:

      ```
      db2ts START FOR TEXT
      ```

Note: If you restart the DB2 server, the DB2 Text Search service does not start automatically. To automatically start the DB2 Text Search service:

Windows
From the **Start** menu, click **Run**, and type `services.msc`, and then change the **DB2TS** services to start automatically.

AIX and Linux
Edit one of the startup scripts to start **db2ts** when you restart the service. The command to start **db2ts** is `db2ts start for text`.

Enable DB2 text search

Enable the IBM DB2 Text Search feature to filter based on the contents of fields with long string data types.

Procedure

1. Log on to a system as a user with Administrator privileges. You can use any system with access to CLPPlus that can connect to the IBM OpenPages GRC Platform database server.

   Note: For SQL tool information, see "Database tool information" on page xxv.
2. Open a command or shell window, navigate to the text-indexing directory as follows:

   Windows
   <OP_HOME>`\aurora\bin\full-text-index`

   AIX and Linux
   <OP_HOME>`/aurora/bin/full-text-index`

   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 that the script invokes to the database server.
3. Run the following SQL script:

```
clpplus -nw @sql-wrapper CustomIndexing_Step1_AddTextIndexing_to_DB.sql
<LOG_FILE_NAME> <DB2_SERVER_NAME> <DB2_PORT_NUMBER> <DATABASE_NAME>
<DB2_INSTANCE_OWNER_NAME> <DB2_INSTANCE_OWNER_PASSWORD> <OP_DB_USER>
```

Table 120: Enable DB2 Text Search required script parameters

Required Parameter	Description
<LOG_FILE_NAME>	Name of the log file.
<DB2_SERVER_NAME>	Name of the DB2 server.
<DB2_PORT_NUMBER>	Port number of the DB2 database service
<DATABASE_NAME>	Name of the OpenPages database.
<DB2_INSTANCE_OWNER_NAME>	Database instance owner account. Usually `db2admin` user.
<DB2_INSTANCE_OWNER_PASSWORD>	Password for instance owner account.
<OP_DB_USER>	OpenPages user name for accessing the OpenPages database.

For example,

```
clpplus -nw @sql-wrapper CustomIndexing_Step1_AddTextIndexing_to_DB.sql
CustomIndexing_Step1_AddTextIndexing_to_DB.log server1 50000 op1 db2admin
dbpassword OPENPAGES
```

Results

The database is now enabled for indexing. Use "Create a long string index in a DB2 database" on page 408 script to create the index.

Create a long string index in a DB2 database

Create a long string text index to support filtering based on the contents of fields with long string data types. Scripts are provided for Windows, AIX, and Linux.

Important: In AIX or Linux operating systems, when using asterisks (*) as parameter values in long string search scripts, the asterisks must be properly escaped with a double quote, single quote combination: "'*'".

Before you begin

Complete the following tasks:

- "Enable DB2 text search" on page 407.
- Ensure that the DB2 text search server information is set up.

  For more information, see Updating DB2 Text Search server information (http://www.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.admin.ts.doc/doc/t0060367.html).

Procedure

1. Log on to a system as a user with Administrator privileges. You can use any system with access to CLPPlus that can connect to the IBM OpenPages GRC Platform database server.

   Note: For SQL tool information, see "Database tool information" on page xxv.
2. Open a command or shell window, navigate to the text indexing directory as follows.

   The following table identifies the installation location of the application on the Microsoft Windows, AIX, and Linux operating systems.

Table 121: Installation location of the full-text-index directory	
Operating system	**Installation location**
Windows	*<OP_Home>*\aurora\bin\full-text-index
AIX and Linux	*<OP_Home>*/aurora/bin/full-text-index

   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 that the script invokes to the database server.
3. Run the following script:

```
clpplus -nw @sql-wrapper CustomIndexing_Step2_IndexCreate.sql
   <LOG_FILE_NAME> <DB2_SERVER_NAME> <DB2_PORT_NUMBER> <DATABASE_NAME>
   <OP_DB_USER> <OP_DB_PASSWORD> <UPDATE_FREQUENCE_WEEKDAY>
   <UPDATE_FREQUENCE_HOUR> <UPDATE_FREQUENCE_MINUTE> <MINIMUM_UPDATES>
```

Table 122: Create DB2 long string index required script parameters	
Required Parameter	**Description**
<LOG_FILE_NAME>	Name of the log file.
<DB2_SERVER_NAME>	Name of the DB2 server.

Table 122: Create DB2 long string index required script parameters (continued)	
Required Parameter	**Description**
<DB2_PORT_NUMBER>	Port number of the DB2 database service
<DATABASE_NAME>	OpenPages database name.
<OP_DB_USER>	OpenPages user name for accessing the OpenPages database.
<OP_DB_PASSWORD>	OpenPages password for accessing the OpenPages database.
<UPDATE_FREQUENCE_WEEKDAY>	Weekday update frequency. Accepted values are between 0 and 6; multiple values can be separated with a comma. For all weekdays use * (asterisk).
<UPDATE_FREQUENCE_HOUR>	Hourly update frequency. Accepted values are between 0 and 23; multiple values can be separated with a comma. For all hours use * (asterisk).
<UPDATE_FREQUENCE_MINUTE>	Minute update frequency. Accepted values are between 0 and 59, multiple values can be separated with a comma. Typically, values are specified as top of the hour (0), or in multiples of 5 minute increments after the hour, for example, 0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50 or 55.
<MINIMUM_UPDATES>	Minimum number of updates in the base table before a scheduled index updates is run.

The following example shows a Windows script:

```
clpplus -nw @sql-wrapper CustomIndexing_Step2_IndexCreate.sql
   CustomIndexing_Step2_IndexCreate.log server1 50000 opx opuser
   password "*" "*" "0,5,10,15,20,25,30,35,40,45,50,55" 1
```

The following example shows the same script on UNIX:

```
clpplus -nw @sql-wrapper CustomIndexing_Step2_IndexCreate.sql
   CustomIndexing_Step2_IndexCreate.log server1 50000 opx opuser
   password "'*'" "'*'" "0,5,10,15,20,25,30,35,40,45,50,55" 1
```

These examples create an index with updates that start every 5 minutes of every hour of every weekday if there is a minimum of one update to the PROPERTYVALS_CLOB table.

Results

An index is created for long string fields.

Create a schedule job to synchronize a long string index in a DB2 database

Create a schedule to synchronize and refresh the long string index. Scripts are provided for Windows, AIX, and Linux.

Procedure

1. Log on to a system as a user with Administrator privileges. You can use any system with access to CLPPlus that can connect to the IBM OpenPages GRC Platform database server.

   Note: For SQL tool information, see "Database tool information" on page xxv.
2. Open a command or shell window, and navigate to the `bin` directory as follows:
   - For Microsoft Windows, type *<OP_Home>*`\aurora\bin`.
   - For AIX or Linux, type *<OP_Home>*`/aurora/bin`.

   Note: If the database server is not on the same machine as the IBM OpenPages GRC Platform server, you must copy the script and the SQL files that the script invokes to the database server.
3. Run the following script:

```
clpplus -nw @sql-wrapper CustomIndexing_Step3_IndexRefresh.sql
<LOG_FILE_NAME> <DB2_SERVER_NAME> <DB2_PORT_NUMBER> <DATABASE_NAME>
<OP_DB_USER> <OP_DB_PASSWORD> <UPDATE_FREQUENCE_WEEKDAY>
<UPDATE_FREQUENCE_HOUR> <UPDATE_FREQUENCE_MINUTE> <MINIMUM_UPDATES>
```

Table 123: Refresh DB2 index required script parameters

Required Parameter	Description
<LOG_FILE_NAME>	Name of the log file.
<DB2_SERVER_NAME>	Name of the DB2 server.
<DB2_PORT_NUMBER>	Port number of the DB2 database service
<DATABASE_NAME>	OpenPages database name.
<OP_DB_USER>	OpenPages user name for accessing the OpenPages database.
<OP_DB_PASSWORD>	OpenPages password for accessing the OpenPages database.
<UPDATE_FREQUENCE_WEEKDAY>	Weekday update frequency. Accepted values are 0 - 6; multiple values can be separated with a comma. For all weekdays, use * (asterisk).
<UPDATE_FREQUENCE_HOUR>	Hourly update frequency. Accepted values are 0 - 23; multiple values can be separated with a comma. For all hours, use * (asterisk).

Table 123: Refresh DB2 index required script parameters (continued)	
Required Parameter	**Description**
<UPDATE_FREQUENCE_MINUTE>	Minute update frequency. Accepted values are 0 - 59, multiple values can be separated with a comma. Typically, values are specified as top of the hour (0), or in multiples of 5-minute increments after the hour, for example, 0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50 or 55.
<MINIMUM_UPDATES>	Minimum number of updates in the base table before a scheduled index updates is run.

The following example shows a Windows script:

```
clpplus -nw @sql-wrapper CustomIndexing_Step3_IndexRefresh.sql
CustomIndexing_Step3_IndexRefresh.log server1 50000 op1 OPENPAGES
opxpassword "*" "*" "0,5,10,15,20,25,30,35,40,45,50,55" 1
```

The following example shows the same script on UNIX:

```
clpplus -nw @sql-wrapper CustomIndexing_Step3_IndexRefresh.sql
CustomIndexing_Step3_IndexRefresh.log server1 50000 op1 OPENPAGES
opxpassword "'*'" "'*'" "0,5,10,15,20,25,30,35,40,45,50,55" 1
```

This example schedules index synchronization to start every 5 minutes of every hour of every weekday if there is a minimum of one update to the PROPERTYVALS_CLOB table.

Results

Index synchronization jobs run at the interval specified.

Note: Changes to long string fields are not available for filtering until the next scheduled index job runs.

Drop a long string index

Remove the long string index. An index must be dropped before it can be re-created. Scripts are provided for Windows, AIX, and Linux.

For more information about working with long string indexes, see Text search index maintenance.

Procedure

1. Log on to a system as a user with Administrator privileges. You can use any system with access to CLPPlus that can connect to the IBM OpenPages GRC Platform database server.

   Note: For SQL tool information, see “Database tool information” on page xxv.
2. Open a command or shell window, and navigate to the text-indexing directory as follows:

   Windows
   <OP_HOME>\aurora\bin\full-text-index

   AIX and Linux
   <OP_HOME>/aurora/bin/full-text-index

   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 that the script invokes to the database server.
3. Run the following SQL script:

```
clpplus -nw @sql-wrapper CustomIndexing_Step5_IndexDrop.sql <LOG_FILE_NAME>
<DB2_SERVER_NAME> <DB2_PORT_NUMBER> <DATABASE_NAME> <OP_DB_USER>
<OP_DB_PASSWORD> <FORCE_DROP_INDEX>
```

Table 124: Enable DB2 drop index required script parameters

Parameter	Description
<LOG_FILE_NAME>	Name of the log file.
<DB2_SERVER_NAME>	Name of the DB2 server.
<DB2_PORT_NUMBER>	Port number of the DB2 database service
<DATABASE_NAME>	Name of the OpenPages database instance.
<OP_DB_USER>	OpenPages user name for accessing the OpenPages database.
<OP_DB_PASSWORD>	OpenPages password for accessing the OpenPages database.
<FORCE_DROP_INDEX>	Drops the index without regard to the status of any associated scheduled task. Values are Y (for Yes) or N (for No)

For example,

```
clpplus -nw @sql-wrapper CustomIndexing_Step5_IndexDrop.sql
CustomIndexing_Step5_IndexDrop.log server1 50000 op1 OPENPAGES opassword Y
```

Results

You must re-create the index before you filter on the content of long string fields again. For details on creating a long string index, see “Create a long string index for an Oracle database” on page 452.

Entity Move/Rename utility

The IBM OpenPages GRC Platform Entity Move/Rename utility allows batch processing of multiple Business Entities for overnight or weekend execution without running the risk of operations that time out. You can run the utility interactively or as a scheduled job.

Using the Entity Move/Rename utility, you can do the following:

- Rename a Business Entity hierarchy
- Simultaneously rename and move a Business Entity hierarchy

A single batch job can contain multiple independent operations, multiple dependent operations, or any combination thereof.

Each operation provides transactional consistency. If an operation fails, all the pending changes for this operation are rolled back. If an operation succeeds, all the changes are persisted.

Each rename, move, or combined operation runs in its own transactional context. So, failure in one operation does not result in the failure of the entire batch job.

CAUTION: Before running the utility, you must stop all application services to avoid data or security errors.

Entity Move/Rename utility prerequisites

Before you use the IBM OpenPages GRC Platform Entity Move/Rename utility, consider these prerequisites.

- A physical computer or VM that meets the OpenPages GRC Platform installation requirements. For detailed specifications, see the *IBM OpenPages GRC Installation and Deployment Guide*.
- An application that produces either CSV (comma-separated value) files or Unicode tab delimited files. This application can be installed on any computer in your environment and is used to prepare the input data for the utility.
- User name and password for the Oracle or DB2 account that owns the OpenPages application database schema (for example, OPENPAGES).

Configuring the Entity Move/Rename utility for a DB2 database

You must configure parameters in the OpenPages GRC Platform Entity Move/Rename utility before you use it in a DB2 database environment.

Procedure

1. Go to the Entity Move/Rename utility installation location as follows:

   OP_Home|aurora|bin|batch_entity_move_rename_relative
2. Open the batch-entity-move-rename.ini configuration file for editing.
3. Specify appropriate values for the following parameters for a DB2 database environment:

Table 125: Parameters for a DB2 database in the batch-entity-move-rename.ini file:

Parameter Name	Description
server_name	DB2 database server.
port_number	DB2 service port number.
db_Name	OpenPages database name on DB2.
user_name	OpenPages database user name.
password	OpenPages database user password.
data_format	Format of the input file to the utility. Example: csv or unicode-text.
input_file	Name of the input file (including extension). Example: 'Sample-batch-entity-move-rename.txt'
code_page	Code page that is used in the DB2 database. If the data_format parameter is set to the following value: • csv saved from Microsoft Excel, it is encoded in ANSI, then the code page must be set to 1252. • unicode-text and encoded in UTF-8 without BOM, then the code page must be set to 1208.

Table 125: Parameters for a DB2 database in the `batch-entity-move-rename.ini` file: (continued)	
Parameter Name	**Description**
skip_rows	The number of rows in the input files to skip on load. Example If the first row of the file: • Contains a list of column names, set the value to '1'. • Does not contain a list of column names, set this value to '0'.

4. Save and close the `batch-entity-move-rename.ini` configuration file.
5. Prepare the input file. See “Prepare the input file for the Entity Move/Rename utility” on page 414.

Prepare the input file for the Entity Move/Rename utility

The input file for the Entity Move/Rename utility can be in CSV or Unicode tab delimited format. You can use any editor to create the input files. Included in the utility installation folder is a sample Unicode text file (`.txt` format).

Important: On AIX and Linux, the text input file must be saved or converted to be encoded in UCS-2 Little Endian and have UNIX end of line (LF) characters.

Tip: If you are using Microsoft Excel, you must save the spreadsheet as a CSV or tab delimited file.

The input file must have the following five columns of data:

Table 126: Columns in the input file		
Column Name	**Description**	**Sample Value**
Source entity location	The entity on which the operation is run.	`/The Bank/USA/North East/Providence`
Target entity location	The new parent entity for "move" and "move and rename" operations only. **Note:** • For Oracle "rename" operations only (no move), the value must be "-" (dash). • For DB2 "rename" operations only (no move), the value must be blank.	For "move" and "move and rename" operations: `/Worldwide/ Americas/USA/NE`
Run as user	Application user name, whose identity is used to run the operation.	`OpenPagesAdministrator`
New entity name	The new name after the operation for "rename" and "move and rename" operations only. **Note:** • For Oracle "move" operations only (no rename), the value must be "-" (dash). • For DB2 "move" operations only (no rename), the value must be blank.	For "rename" and "move and rename" operations: `Boston`

Table 126: Columns in the input file (continued)		
Column Name	**Description**	**Sample Value**
Execution order	Establishes the operation execution order as follows: • Operations that specify the execution order are run before operations that do not. • Operations that have a numeric value in the execution order column are run in regular ascending ordering. If set, the value must to be a valid number; Otherwise, leave the field blank.	1

The following is a short description of the data in the sample `.txt` file that is included in the utility directory.

- The first line illustrates moving entity `/The Bank/USA/North East/Providence` to new location `/Worldwide/Americas/USA/NE`. Operation is to be run as the user `SOXAdministrator`. This operation is run first in the batch.
- The second line illustrates in place rename of the entity `/Worldwide/Americas/USA/NE/Providence`. Entity name changes to Boston. Target location does not apply and is set to "-". This entry has a dependency on the previous move operation and has higher number in the execution order column. Also, it references to the new entity location that will be in effect after the first operation completes.
- If the first operation fails for any reason, this operation fails as well and the entity location would be incorrect.
- The third line illustrates simultaneous move of the entity `/The Bank/USA/Midwest/Chicago` to new location `/Worldwide/Americas/USA/MW` and rename to Detroit. This operation has no dependencies and will be run after the first two complete.

If you have an Oracle database with the 32-bit SQL*Loader utility and an IBMAIXor Linux environment, see the topic: "Avoid error 0509-036 when you use the 32-bit Oracle SQL*Loader" on page 466. Otherwise, run the IBM OpenPages GRC Platform Entity Move/Rename utility.

Running the Entity Move/Rename utility interactively for a DB2 database

Use the following steps to run the IBM OpenPages GRC Platform Move/Rename utility interactively in a DB2 database environment.

Before you begin, make sure that you prepared the input file. See "Prepare the input file for the Entity Move/Rename utility" on page 414 for instructions.

Procedure

1. Move the input file into the utility installation directory, which is at:

   ```
   OP_Home|aurora|bin|batch_entity_move_rename_relative
   ```

2. Validate that the input_file parameter in the `batch-entity-move-rename.ini` configuration file is correctly set to the input file name. For more information, see "Configuring the Entity Move/Rename utility for a DB2 database" on page 413.
3. For Windows operating systems only: Start the DB2 command line processor first by opening a command window and entering the db2cmd command.
4. From the location where the utility is installed, run the batch command file and review the output on the screen.

Windows
`batch-entity-move-rename.cmd`

AIX or Linux
`batch-entity-move-rename.sh`

5. Upon completion, review the following log files for any errors:
   - `batch-entity-move-rename-load.log`
   - `batch-entity-move-rename-proc.log`

   If any errors are reported and you are unable to fix them, contact your IBM Support representative. Make sure you supply a copy of the screen that contains the error messages and all the log files that are generated by the tool.

Running the Entity Move/Rename utility as a scheduled task

You can set up a scheduled task to run the IBM OpenPages GRC Platform Entity Move/Rename utility.

Depending on your environment, you can run the `batch-entity-move-rename` batch command file by using any scheduling application. For example, in Windows, you might use the built-in Windows scheduler. In IBM AIX or Linux, you might set up a `cron` job.

Important: If you are using a DB2 database in a Windows environment, you must run the batch command file within the **DB2 Command Line Processor**.

If the job fails, the batch command returns a non-zero exit code. You can redirect the console output to a log file. For example, in Windows:

```
batch-entity-move-rename.cmd >> batch-entity-move-rename.log
```

The following files are overwritten on each run:

- `batch-entity-move-rename-load.log`
- `batch-entity-move-rename-proc.log`

These files can be saved, either manually or through a script, if log archives are needed.

Impact of the Entity Move/Rename utility on the OpenPages GRC Platform application

The Entity Move/Rename utility works directly against the IBM OpenPages GRC Platform database repository. As a result, the Java based OpenPages GRC application is unaware of the changes made to the entity hierarchy and folder structure.

As a result, internal application caches might become out of sync with the data in the repository and lead to discrepancies in the application user interface.

It is required that after you run the tool you restart application services, or run the tool when application services are stopped.

Also, ensure that the `OPBackup` command is not running during execution, and that all batch rename and move operations are completed before you run a backup.

Improve performance of OpenPages GRC Platform application functions on a DB2 server

You can improve the performance of IBM OpenPages GRC Platform application functions by collecting performance statistics for the IBM DB2 server, and by rebinding OpenPages GRC pl/sql packages.

Examples of application functions include importing instance data using FastMap, importing metadata using Object Manager, and updating OpenPages GRC repository using SCOR rules.

Up-to-date statistics are necessary for the proper performance of OpenPages GRC applications that use a DB2 server. You can use a script to force the DB2 server to collect statistics, and by default, rebind all OpenPages GRC pl/sql packages. The script requires all OpenPages GRC application services to stop before it runs. For details on stopping servers, see Chapter 20, “Starting and stopping servers,” on page 549.

You run the script from the primary OpenPages GRC application server. You do not need to run this script from all cluster member servers, but you must stop all cluster member services before running the script to rebind OpenPages GRC pl/sql packages.

If a database is still running, you see the error SQL1026N. If this happens, verify that OpenPages GRC services are not running, and disconnect all active connections to the database before continuing.

You can run the script on Microsoft Windows, AIX, and Linux.

1. For Windows users only, type the following command in a command prompt window to initialize the DB2 command line processor (CLP):

   ```
   db2cmd
   ```

2. Browse to the *<OP_HOME>* | `aurora` | `bin` | `db2stats` folder.
3. Run the following script:
   - On Windows: `CollectSchemaStatistics.bat [-n] [-i]`
   - On AIX and Linux: `CollectSchemaStatistics.sh [-n] [-i]`

Use these parameters as required:

- [-n] to skip rebinding of database packages.
- [-i] to run the script in interactive mode.

The script execution time varies depending on OpenPages GRC application usage.

You can schedule this script to run by using a task scheduler, cronjob, or similar utility. The suggested schedule to use is as follows:

- Schedule the script to run daily without rebinding of OpenPages GRC pl/sql packages.
- Schedule the script to run once a week with rebinding of OpenPages GRC pl/sql packages.

Chapter 18. Using IBM OpenPages GRC Platform utilities with Oracle databases

You can use these utilities with your Oracle database for backing up and restoring OpenPages GRC Platform and Cognos files and databases, and setting up a test environment.

Oracle databases and the backup and restore utilities

The backup and restore utilities are installed during the IBM OpenPages GRC Platform installation.

Use these utilities to back up and restore the OpenPages GRC Platform environment:

- OpenPages GRC Platform backup (OPBackup) and restore (OPRestore) are used to backup and restore the OpenPages GRC Platform application and database
- Cognos backup (OPCCBackup) and restore (OPCCRestore) are used to backup and restore OpenPages GRC Platform Cognos files and the content store.
- Users can choose to execute a live OPBackup. When running live OPBackup, OpenPages GRC Platform services are not restarted on the application server, allowing for maximum uptime of the application. By default, the services will be restarted.

Prerequisite: Oracle Admin Client

To use the backup and restore utilities that are included with IBM OpenPages GRC Platform, the Oracle Admin Client software must be installed on both the OpenPages GRC Platform application server and OpenPages GRC Platform Cognos server machines.

Note: For the currently supported version of the Oracle Admin Client, see the *IBM OpenPages GRC Release Notes* or the *IBM OpenPages GRC Installation and Deployment Guide Installation Guide* .

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 GRC Platform application and Cognos backup and restore utilities and was automatically configured during the OpenPages GRC Platform 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) after the OPBackup or OPCCBackup tool has completed.
- Before you use the Cognos 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 431.

  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.

Email notification for backup jobs

You can configure email notification when you complete an IBM OpenPages GRC Platform application backup or Cognos backup job.

Note:

- Log files for email notification are stored in the `logs` folder in the following location:
  - For OPBackup (OpenPages GRC Platform application backup):

    ```
    <OP_Home>|aurora|bin|logs with the timestamp on the log files.
    ```

  - For OPCCBackup (Cognos backup):

    ```
    <CC_Home>|tools|bin|logs with the timestamp on the log files.
    ```

- Make sure to set rules in your email client to never send emails from the OpenPages GRC Platform application server to the Spam or Junk mail folders.

Configuring backup job notification

Use this procedure to configure email parameters for IBM OpenPages GRC Platform and Cognos backup jobs.

Procedure

1. Open a command or shell window and do one of the following.
   a) For an OPBackup (OpenPages GRC Platform application backup,

      navigate to the `op-backup-restore.env` file in the `bin` directory as follows:

      - For Microsoft Windows, the bin directory is *<OP_Home>*`\aurora\bin`
      - For AIX and Linux, the bin directory is *<OP_Home>*`/aurora/bin`

   b) For a OPCCBackup (Cognos backup), navigate to the `op-cc-backup-restore.env` file in the `bin` directory where *<cc_home>* represents the installation of Cognos.

      - For Microsoft Windows, the back up path is `OPBackup <path-to-back-up-location>`
      - For AIX and Linux, the back up path is `OpBackup.sh <path-to-back-up-location>`

      where `<path-to-backup-location>` is the full path of the directory where the backed up files are located on the 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.
2. Open the selected `.env` file in a text editor.
3. Specify a value after the equal sign (=) for the parameters described in the following table and save the `.env` file.

Table 127: Backup email parameters

Parameter name	Description
BACKUP_EMAIL_NOTIFICATION_SERVER=	The host name of the outgoing mail server.

Table 127: Backup email parameters (continued)	
Parameter name	**Description**
BACKUP_EMAIL_NOTIFICATION _TO_EMAIL_ID=	The name of recipients that will receive the email notification. Separate email addresses with a comma (,). **Note:** Do not type a comma after the last email 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 email in the `From:` field of the email. The email address is also used as the personal name.
BACKUP_EMAIL_NOTIFICATION _SUCCESS_MSG_ FILE=BACKUP_SUCCESS_MSG.txt	The `BACKUP_SUCCESS_MSG.txt` file 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. The first line of the file is used as the email's subject.
BACKUP_EMAIL_NOTIFICATION _FAIL_MSG_FILE= BACKUP_FAIL_MSG.txt	The `BACKUP_FAIL_MSG.txt` file is the default file that contains the message text that is 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 email's subject.

Asynchronous background jobs and administrative functions

IBM OpenPages GRC Platform supports asynchronous execution of processes in the background.

The most common examples of these type jobs are FastMap web-based data import jobs, object resets, and reporting schema generation.

For example, after a user submits a data import file, that file is queued for loading and the import process occurs in the background. Because it is important for asynchronous background jobs to run to completion, certain administrative operations are suspended until all background jobs complete.

By default, the following administrative functions will not start until background jobs are complete:

- OPBackup command
- OPRestore command
- System Administrative Mode (SAM)

Note: To disable the default setting that checks for background jobs before you start `OPBackup` or `OPRestore`, see “Enabling and disabling asynchronous background processes checking” on page 386.

If asynchronous processes are found, error messages are written to the OPBACKUP restore log.

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 and Linux

```
/opt/OpenPages/openpages-backup-restore/op_backup_2010_07_26_09_35_42.log
```

Sample error log messages follow.

- For Oracle database environments, a sample error log message might look similar to this text:

```
– can-proceed:
  [exec] declare
  [exec] *
  [exec] ERROR at line 1:
  [exec] ORA-20001: There are existing processes running.
  [exec] Please let them finish or terminate them before proceeding.
  [exec] ORA-06512: at line 7
  [exec]
```

```
– can-proceed:
  [exec] declare
  [exec] *
  [exec] ERROR at line 1:
  [exec] ORA-20001: There are existing object reset operations running.
  [exec] Please let them finish or terminate them before proceeding.
  [exec] ORA-06512: at line 7
  [exec]
```

- For IBM DB2 environments, a sample error log message might look similar to this text:

```
– can-proceed:
  [exec] ERROR near line 26:
  [exec] SQL0438N Application raised error or warning with diagnostic
  [exec] text: "There are existing processes running. Please let them
  [exec] finish or termi".
```

```
– can-proceed:
  [exec] ERROR near line 26:
  [exec] SQL0438N Application raised error or warning with diagnostic
  [exec] text: "There are existing object reset operations running.
  [exec] Please let them finish or termi".
```

Enabling and disabling asynchronous background processes checking

By default, IBM OpenPages GRC Platform does not allow a backup (OPBackup) or restore (OPRestore) operation to start until all asynchronous background jobs are complete.

It is best to run all jobs to completion before you start a backup or restore operation. However, this check can be enabled or disabled as follows.

Procedure

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

2. Navigate to the `op-backup-restore.env` file in the `bin` directory.
   - For Microsoft Windows, the bin directory is *<OP_Home>*`\aurora\bin`
   - For AIX and Linux, the bin directory is *<OP_Home>*`/aurora/bin`
3. Open the `op-backup-restore.env` file in a text editor.
4. Set the `CHECK_BACKGROUND_PROCESSES` parameter in the file to true or false.
   Setting the value to true enables the asynchronous background job. If background processes are running, this value prevents OPBackup or OPRestore from starting. True is the default value. false disables the validation check for asynchronous background jobs. OPBack or OPRestore start even if background processes are running.

Encrypting database passwords in the backup-restore utility environment files

Passwords that are used by the IBM OpenPages GRC Platform, and Cognos 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 value is in plain text until it is encrypted. `op-backup-restore.env` database password parameters (file are stored on the application server):

- `DB_SYSTEM_PWD=`
- `DB_SYS_PWD=`
- `DB_OP_PWD=`

`op-cc-backup-restore.env` database password parameters (file are stored on the reporting server):

- `DB_SYSTEM_PWD=`
- `DB_CC_PWD=`

For security purposes, it is best to encrypt the changed passwords by completing the following procedure.

Important: In a horizontal clustered environment, you must complete this procedure on each OpenPages GRC Platform application server in the horizontal cluster.

Procedure

1. Open a command or shell window on the OpenPages GRC Platform server.
2. Go to the `bin` directory:
   - For Microsoft Windows, the directory is *<OP_HOME>*\aurora\bin
   - For AIX or Linux, the directory is *<OP_HOME>*/aurora/bin
3. To encrypt changed database password parameters in the `op-backup-restore.env` environment file, run the following command:
   - On Windows operating systems: `OPBackup.cmd secure`
   - On AIX and Linux operating systems: `./OPBackup.sh secure`
4. To encrypt changed database password parameters in the `op-cc-backup-restore.env` environment file, do the following steps:
   a) Open a command or shell window on the reporting server.
   b) Go to the *<CC_Home>*`/tools/bin` directory.
      <CC_Home> is the installation location of Cognos.
      - For Microsoft Windows, *<CC_Home>* is `C:\OpenPages\CommandCenter`.
      - For AIX or Linux, *<CC_Home>* is `opt/OpenPages/CommandCenter`.
   c) Type the following backup command:

- On Windows: `OPCCBackup.cmd secure`
- On AIX or Linux: `./OPCCBackup.sh secure`

The OPBackup utility

OPBackup is the IBM OpenPages GRC Platform backup utility that backs up the necessary product 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 GRC restore utility (OPRestore).

When you use the OPBackup utility, the following OpenPages GRC Platform resources are backed up:

- The OpenPages GRC Platform application
- The OpenPages GRC Platform storage folder and its content
- The OpenPages GRC Platform application environment files

In a horizontal clustered environment, if the Backup Utility is run on a non-administrative server, the application database will not be included in the backup. To include this database in a backup file, run the Backup Utility on an administrative server.

OPBackup does not back up standard OpenPages tools by default. If you want to include additional files or directories, you must add them to a manifest file before you run the backup. For more information, see "Backing up custom OpenPages GRC Platform files" on page 387.

If you use IBM Business Process Manager, OPBackup does not back up the BPM database. BPM backups and restores are handled outside of the OpenPages OPBackup and OPRestore utilities. For more information, see the BPM documentation in the following topic: (http://www.ibm.com/support/knowledgecenter/SSFPJS_8.5.7/com.ibm.wbpm.admin.doc/topics/cadm_recovery_backup.html).

Depending on your configuration, if any asynchronous background jobs are detected, an OPBackup job will exit and possibly display errors (see "Asynchronous background jobs and administrative functions" on page 385).

You can also configure email notification upon completion of an OPBackup. For details, see "Email notification for backup jobs" on page 383.

Attention: If you have global search enabled, global search must be disabled before running the OPBackup and OPRestore utilities. For more information, see "Using OPBackup and OPRestore when global search is enabled" on page 360.

Modifying the backup-restore environment file

The IBM OpenPages GRC Platform 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`.

- For Microsoft Windows: *<OP_Home>* is `C:\OpenPages`.
- For AIX and Linux: *<OP_Home>* is `/opt/OpenPages`.

Scenario 1: The root installation path of the OpenPages GRC Platform storage location changed after installation

If you modify the root path of the IBM OpenPages GRC Platform 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 (OpenPages GRC Platform 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 you 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 GRC Platform files

Custom IBM OpenPages GRC Platform files, such as SiteSync or scheduled job files that are specific 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.

For example, you could add the following file to the manifest file:

- *OP_HOME*\aurora\lib\openpages-ext.jar

Before you begin

- 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 GRC Platform Customer Support.
- In a horizontal clustered environment, you must perform this procedure on each OpenPages GRC Platform Application Server in the horizontal cluster.

Procedure

1. Log on to the current OpenPages GRC Platform application server.
2. Navigate to the *OP_HOME* | aurora | bin directory and open the op_backup.manifest file in a text editor.
3. Type the full path name to all custom directory names or to 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 GRC Platform application backup utility, run the OPBackup command in a command or shell window.

The OPBackup command does the following:

- Stops all OpenPages GRC Platform services before performing any backup operation
- Backs up OpenPages GRC Platform application and environment files
- Restarts the services when the backup activities are complete

See "Running a live OpenPages GRC Platform backup" on page 388 if you want to perform a backup without stopping services.

Procedure

1. If global search is enabled, disable it:
   a) Log in to OpenPages as an administrator.
   b) Click **Administration** > **Global Search** > **Disable**.

2. Open a command or shell window on the OpenPages GRC Platform application server.
3. Navigate to the bin directory as follows:
   - For Microsoft Windows, the bin directory is *<OP_Home>*\aurora\bin
   - For AIX and Linux, the bin directory is *<OP_Home>*/aurora/bin
4. Execute the following backup command:

   ```
   OPBackup <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 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.

Backing up the OpenPages database (Oracle)

You can use the OPBackup utility to back up the IBM OpenPages GRC Platform databases.

About this task

Note: You can back up the databases by using other methods. Some examples of alternative methods include:

- Doing a full physical backup by using RMAN
- Doing a combination of full and incremental backup by using RMAN
- Doing an Oracle data pump export.

If you want to use an alternative method, it is critical that you have the necessary skills available within your organization to complete all aspects of the backup and restore activity.

Procedure

1. Make sure that no OpenPages GRC Platform processes are running, such as object reset jobs.
2. Shut down all OpenPages components: application servers (admin and non-admin), reporting servers (active and standby), and the search server.

   For more information, see Chapter 20, “Starting and stopping servers,” on page 549.
3. Open a command or shell window on the admin application server.
4. Go to the *<OP_HOME>*/aurora/bin directory.
5. Do a full database backup of the OpenPages schema by using OPBackup.

   Windows:

   ```
   OPBackup.cmd <backup_directory> dbonly
   ```

   Linux or AIX:

   ```
   ./OPBackup.sh <backup_directory> dbonly
   ```

   The *<backup_directory>* is the full path to a directory on the database server. This directory is where the log files are saved. If the file path is not specified, the OPBackup command uses the location that is specified by the BACKUP_LOCATION parameter in the *<OP_HOME>*/aurora/bin/op-backup-restore.env file.

   A dump file is created in the OP_DATAPUMP_DIRECTORY directory.
6. Examine the backup log and make note of the dump file name. The naming convention is openpage_*<timestamp>*.dmp.

Running a live OpenPages GRC Platform backup

A live IBM OpenPages GRC Platform backup means that the application can continue running while the backup is in progress. The services are not stopped during the backup.

Note: Run live OpenPages GRC Platform backups during off-peak hours because the backup consumes processing resources.

You might encounter 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 may be 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 OpenPages GRC Platform application backup utility live, you run the `OPBackup` command with the `nosrvrst` option. This does the following:

- Backs up OpenPages GRC Platform application and environment files
- Exports the OpenPages GRC Platform application database

Procedure

1. Open a command or shell window on the OpenPages GRC Platform server.
2. Navigate to the `bin` directory as follows:
   - For Microsoft Windows, the bin directory is `\<OP_Home>\aurora\bin`
   - For AIX or Linux, the bin directory is `/<OP_Home>/aurora/bin`
3. Type the following backup command:

   Windows

   ```
   OPBackup <path-to-backup-location> nosrvrst
   ```

   AIX and Linux

   ```
   OPBackup.sh <path-to-backup-location> nosrvrst
   ```

   where:

   Windows
   <path-to-backup-location> is `<oracle_base>\admin\<SID>\dpdump`

   AIX and Linux
   <path-to-backup-location> is `<oracle_base>/admin/<SID>/dpdump`

OpenPages GRC Platform backed-up content

The backup process creates a ZIP file (`.zip`) in the `<backup-directory-name>` directory.

The ZIP file contains the following necessary backed up databases and data files:

- IBM OpenPages GRC Platform application database
- IBM OpenPages GRC Platform properties files (such as `aurora.properties` and `sosa.properties`).

- Application server configuration files for IBM WebSphere.
- The openpages-storage directory.
- Pointers to the database schema dump extracts.
- Manifest-defined content (such as solutions-sosa-files.zip or services-sosa-files.zip).

Note:

- If a backup file is 4 GB or larger, 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 GRC Platform 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.

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.

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). After 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.
   - For Windows, the installation directory is c:*<OP_Home>*\aurora\bin
   - For AIX or Linux, the installation directory is *<OP_Home>*/aurora/bin
2. Open the op-backup-restore.env file in a text editor of your choice.
3. Change the USE_GZIP_COMPRESSION= setting from false to true.

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 OpenPages GRC Platform server.
2. Navigate to the op-backup-restore.env file in the bin directory as follows.

Table 128: Installation locations

Operating system	Installation location
Windows	*<OP_Home>*\aurora\bin
AIX and Linux	*<OP_Home>*/aurora/bin

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:

Table 129: BACKUP_OP_STORAGE parameter values and their meanings	
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.

The OpenPages GRC Platform restore utility on the Oracle database

OPRestore is the IBM OpenPages GRC Platform restore utility that restores the OpenPages files and database content on the server from which it was originally run. The OPRestore utility uses a backup file created by the OpenPages GRC Platform backup utility (OPBackup).

Important: To refresh a "test" environment, see “Refreshing a test environment from backup files” on page 441.

As part of the restoration process, the following OpenPages GRC Platform resources are restored:

- The OpenPages GRC Platform application
- The OpenPages GRC Platform storage folder and its content
- The OpenPages GRC Platform application environment files

Important: In a horizontal environment, if OpenPages GRC Platform backup is run on a non-administrative server, the application database is 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 “Asynchronous background jobs and administrative functions” on page 385).

Running the OPRestore command

You can restore a backup using the OPRestore command.

Before you begin

If you used OPBackup, the zip file should contain the database dump files (`.dmp`). If the dump files are not in the zip file, copy them to the backup location before you start the restore.

Procedure

1. If you enabled the global search component during backup, recreate your search index so that your search results are synchronised.
   a) Click **Administration** > **Global Search**.
   b) Click **Disable** to disable the global search component.
   c) Click **Drop** to drop the search indexes.
   d) Click **Create** to recreate the search indexes.
2. Stop the `IBM Cognos` service.
3. From a command or shell window, navigate to the `bin` directory as follows:
   - For Microsoft Windows, the bin directory is *<OP_Home>*`\aurora\bin`
   - For AIX and Linux, the bin directory is *<OP_Home>*`/aurora/bin`
4. Execute the following command:

   Windows

   ```
   OPRestore <backup-file-name> <path-to-backup-location>
   ```

AIX and Linux

```
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)

What to do next

Preferences related to the long string text index won't be exported by "Running the OPBackup command" on page 425, and therefore are not restored. You must "Create a long string index for an Oracle database" on page 452 pointing to the database server you are restoring to.

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 Cognos backup utility

OPCCBackup is the Cognos utility that backs up the necessary Cognos files. The OPCCBackup utility creates a backup file that can be used by the Cognos restore utility (OPCCRestore).

To back up or restore the IBM DB2 databases for IBM OpenPages GRC Platform, you must use the utilities that are provided with DB2. For more information about the databases in IBM OpenPages GRC Platform and backing up or restoring them, see Backing up and restoring DB2 database.

When you use the OPCCBackup utility, the following Cognos resources are backed up.

- Cognos reports
- Branding and environment files

You can configure e-mail notification (with an attached log file) upon the completion of an OPCCBackup. For details, see "Email notification for backup jobs" on page 383.

Oracle Data Pump configuration on a first time use

Before you use the Cognos backup utility for the first time, you must configure Oracle Data Pump by running an SQL script.

This task is required.

For details on running the script, see "Configuring or updating the Oracle Data Pump directory" on page 431.

The script configures a data pump 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.

The OpenPages GRC Platform file storage directory

By default, OP_DATAPUMP_DIRECTORY is the name of the directory used for storing Cognos 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

The script used in this procedure requires access to the content of the installation kit: OP_*<version>*_Non_Embedded.

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) Navigate to the OP_*<version>*_Non_Embedded directory on your network drive or in the installation kit.
   b) Navigate to the following folder:

   /OP_*<version>*_Non_Embedded/OP_*<version>*_Configuration/Database/ORACLE/UPGRADE_SCRIPTS
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.

Table 130: Parameters for Oracle Data Pump SQL script

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 and Linux `/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.

Table 130: Parameters for Oracle Data Pump SQL script (continued)	
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 Cognos 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 Cognos application.
   - For Microsoft Windows, navigate to *<CC_Home>*\tools\bin. By default, *<CC_Home>* is C:\OpenPages\CommandCenter.
   - For AIX or Linux, navigate to *<CC_Home>*/tools/bin.
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 Cognos 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).

   The default Content Store database export locations are:

   Windows: <oracle_base>\admin\<SID>\dpdump

   AIX: <oracle_base>/admin/<SID>/dpdump

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.

Cognos backed-up content

The Cognos backup process creates a ZIP file (.zip) in the <backup-directory-name> directory. This ZIP file contains the necessary report and environment files that can be used by the Cognos restore utility (OPCCRestore).

Note:

- If a backup file is very large (4 GB or larger), 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 IBM OpenPages GRC Platform 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 Cognos application
   - For Microsoft Windows, the directory is: *<CC_Home>*`\tools\bin`. By default, *<CC_Home>* is `C:\OpenPages\CommandCenter`
   - For AIX or Linux, the directory is: *<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.
3. Change the `USE_GZIP_COMPRESSION=` setting in the file from `false` to `true`:

Using the Cognos restore utility

OPCCRestore is the IBM OpenPages GRC Platform Cognos utility that restores the necessary Cognos files and Content Store on the server from which it was originally run. The OPCCRestore utility uses a backup file created by the OpenPages GRC Platform Cognos backup utility (OPCCBackup).

Note: To refresh a "test" environment, see “Refreshing a test environment from backup files” on page 441.

As part of the restoration process, the following Cognos resources are restored:

- Cognos reports
- Content Store
- Branding and environment files

Running the OPCCRestore command

You can restore backed up Cognos data using the OPCCRestore utility as follows.

Procedure

1. Stop the `IBM Cognos` service on the administrative server and any non-administrative servers in the cluster. For details, see “Starting and stopping the Cognos services” on page 560.
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 where the *<CC_Home>* represents the installation location of the Cognos application.
   - For Microsoft Windows, the installation location is *<CC_Home>*\tools\bin. By default, *<CC_Home>* is C:\OpenPages\CommandCenter.
   - For Aix or Linux, the installation location is *<CC_Home>*/tools/bin. By `default, <CC_Home> is /opt/OpenPages/CommandCenter`

4. On the administrative Cognos server, run 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 Cognos server. The file path is optional.

   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 `IBM Cognos` service on the administrative server and on any non-administrative servers in the cluster. For details, see "Starting and stopping the Cognos services" on page 560.

The OPCCRestore log file

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

To perform an online backup of the IBM OpenPages GRC Platform database, using custom OpenPages scripts that utilize Oracle's Recovery Manager (RMAN) facility.

Knowledge of basic Oracle database backup and recovery operations is necessary, as well as use of RMAN. For more information on the use of RMAN for online database backup and recovery, see the Oracle documentation.

Oracle online database backups

Unlike the IBM OpenPages GRC Platform 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 OpenPages GRC Platform database and OpenPages GRC Platform services. It also allows "point in time" recovery of the OpenPages GRC Platform 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 OpenPages GRC Platform 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 OpenPages GRC Platform storage directory and application environment files.

Running Oracle online database backups (RMAN)

Setting up and running Oracle online database backups has several steps.

Complete the following steps to set up and run Oracle online database backups:

"Plan the size of the Oracle backup area" on page 435

"Copying the online Oracle backup scripts to a local directory" on page 435

"Modifying the environment variables in the Oracle RMAN-ENV script" on page 436

"Configure the Oracle database for online backup" on page 438

"Run the Oracle rman-daily script" on page 438

Plan the size of the Oracle 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. Estimate the maximum size of the backup area in order to set the appropriate environment variable. For more information, see "Modifying the environment variables in the Oracle RMAN-ENV script" on page 436.

As a guideline, use a backup area that is 3x the size of the database. It includes the sum of the database, database copy, and archived log files.

The size of the backup area must be large enough to store all of the following information:

- 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

The backup area should be able to store at least 24 hours of archived redo logs that have not been backed up.

Copying the online Oracle backup scripts to a local directory

To access the scripts for online database backup, copy them from the installation media: `OP_<version>_Non_Embedded` to any local directory on the database server. You can run the scripts from the local directory.

Procedure

1. Log on to the IBM OpenPages GRC Platform database server as a user with administrative privileges.
2. Open a command or shell window and complete the following action:
   a) Go to the `OP_<version>_Non_Embedded` directory on your network drive or in the installation kit.
   b) Go to the `INSTALL_SCRIPTS` directory at the following location:

```
OP_<version>_Configuration|Database|ORACLE|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

     `rman-env.cmd`

     `rman-init.cmd`

     `rman-daily.cmd`

recover-db.cmd

AIX and Linux

rman-env.sh

rman-init.sh

rman-daily.sh

recover-db.sh

- More online backup scripts:

```
enable-archivelog-mode.sql
disable-archivelog-mode.sql
check-fra-size.sql
load_OP_APP_DATA.sql
no-op.sql
op-app-global-env.sql
sql-wrapper.sql
update-fra-size.sql
init_recovery_env.sql
```

Note:

- The name of the local directory where you are copying the scripts must not contain any space characters.
- You can run the scripts described in the following topics from the local directory. You can add the directory to your PATH environment variable so that you can run them from any directory.

Modifying the environment variables in the Oracle RMAN-ENV script

After you determine the size of the backup area, edit the environment variable values in the `rman-env` script.

Before you begin

Complete the following steps to modify the Oracle RMAN-ENV script:

Procedure

1. Open the `rman-env.cmd` (Windows) or `rman-env.sh` (AIX and Linux) script in a text editor on the database server. Edit the following environment variables for your Oracle database environment as shown in Table 131 on page 436.

Table 131: Environment Variables in RMAN-ENV Script

Environment Variable	Description
ORACLE_HOST_NAME=	Fully qualified network identifier for the database server computer. The host name can be found in the HOST parameter in the `tnsnames.ora` file. Example: `mydbhost.openpages.com`
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: op

Table 131: Environment Variables in RMAN-ENV Script (continued)

Environment Variable	Description

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 and Linux
	`/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 and Linux
	`/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 and Linux** `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)
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

Table 131: Environment Variables in RMAN-ENV Script (continued)	
Environment Variable	**Description**
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>*\Inventory\ ContentsXML directory. Example: OPServer

2. Save the script file.

Results

After 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" for more information. Never modify the `rman-env` script to adjust the size of the backup area after 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 Oracle 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 and Linux

```
rman-init.sh <tns_name_alias> SYS <sysdba_password>
```

Where:

<tns_name_alias> is the TNS alias of the IBM OpenPages GRC Platform 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.

Windows example

```
rman-init.sh op 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 the Oracle 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`).

After you configure 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 GRC Platform 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.

AIX example

```
rman-daily.sh op SYS SYSPWD
```

Review Oracle 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

Monitoring the size of the Oracle backup area

You can use a script to monitor 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 IBM OpenPages GRC Platform 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 op SYSTEM SYSTEMPWD
```

Displays the used, allocated, and free space for database instance op.

Adjusting the size of the Oracle backup area

You can adjust the size of the backup area if necessary.

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
```

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 one of the scripts described in the following section.

Important: Do not delete files manually from the backup area to free up space. Doing so causes the following error: `RMAN-06059: expected archived log not found`.

Reclaiming used space by running the Oracle 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 Oracle UPDATE-FRA-SIZE script

You can adjust the size of the backup using a 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 IBM OpenPages GRC Platform 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> op SYS SYSPWD 15G
```

Adjusts the backup area for database instance op to 15 gigabytes.

Important: The script restarts the database. Users are unable access the database while the script is running.

Disabling online backup of the Oracle 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 IBM OpenPages GRC Platform 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> op SYS SYSPWD
```

Important:

- The script restarts the database. Users are unable access the database while the script is 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

To refresh an existing test (target) environment, you can replicate it from a production (source) environment. By using backup files from a production environment, you can update a test environment that closely matches your production environment.

Note: Oracle Data Pump backup files are created on the database server.

Prerequisites

Ensure you have access to the production server and test server.

Ensure the production server and test server have the same installed version of the IBM OpenPages GRC Platform application, including patches.

Ensure you have access to the installation media:

- OP_*version*_Non_Embedded

Backing up and copying the OpenPages GRC Platform application production files for an Oracle database

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 GRC Platform server as a user with administrative permissions.
2. Run the OpenPages GRC Platform backup utility (`OPBackup`) to back up the OpenPages application database.

   For more information, see "The OPBackup utility" on page 387.
3. Copy the backup `.zip` or `.tar.gz` file to your test server.

Backing up the OpenPages GRC Platform application test files on your Oracle test data

You can back up IBM OpenPages GRC Platform application test data.

Procedure

1. Log on to your test OpenPages GRC Platform server as a user with administrative permissions.
2. Run the backup utility (`OPBackup`) as described in "The OPBackup utility" on page 387 to backup the OpenPages GRC Platform application database.

Deleting data on the test database system

You can delete data on the test database system.

Procedure

1. If necessary, log on to your IBM OpenPages GRC Platform test server as a user with administrative permissions.
2. Open a command or shell window and do the following:
   a) Navigate to `OP_<version>_Non_Embedded` on your network drive or in the installation kit.
   b) Navigate to the `INSTALL_SCRIPTS` directory at the following location:

   ```
   OP_<version>_Configuration|Database|ORACLE|INSTALL_SCRIPTS
   ```
3. From the `INSTALL_SCRIPTS` directory, run the `AuroraDbDelete.sql` script as follows:
   a) Log on to SQL*Plus as the OpenPages GRC Platform database user (for example: `sqlplus openpages/openpages@test`).
   b) Run the following script to drop the objects in the schema on the test server:

   ```
   @AuroraDbDelete.sql
   ```
   c) When finished, log out of SQL*Plus.

Copy the production database dump (.dmp) file to the test database server

You can copy the production database 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 the IBM OpenPages GRC Platform database dump (`.dmp`) file from the Oracle `datapump` directory on the production database server to the `datapump` directory on the test database server.

Table 132: Default file name for .dmp file	
For this .dmp file...	**The default file name will be similar to this...**
OpenPages GRC Platform	`OPENPAGES_<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

You must import the IBM OpenPages GRC Platform 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 and Linux

   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 OpenPages GRC Platform database on the test database server from the backup files in “Backing up and copying the OpenPages GRC Platform application production files for an Oracle database” on page 442 as follows.

   Note: The Oracle Data Pump command IMPDP is used as the IMP command is not supported.

   For more information on Oracle Data Pump, see “Oracle Data Pump” on page 419.

   From the same command or shell window, run the following command to import the OpenPages GRC Platform database:

   ```
   impdp <op_db_user>/<op_db_password>@<SID>
    DIRECTORY=OP_DATAPUMP_DIRECTORY
    DUMPFILE=<openpages_dump_file>
    LOGFILE=openpages_import.log
   ```

Table 133: Parameters and their descriptions	
Parameter	**Description**
<op_db_user>	The OpenPages GRC Platform user name for accessing the OpenPages database.

Table 133: Parameters and their descriptions (continued)	
Parameter	**Description**
<op_db_password>	The OpenPages GRC Platform password for accessing the OpenPages database.
<SID>	The Oracle System Identifier (for example, OP or OP).
<openpages_dump_file>	The `.dmp` file name of the backed up OpenPages GRC Platform application database. **Important:** Do not enter an explicit path when specifying the `.dmp` file name. Enter only the file name.
DIRECTORY	The directory on the database server where the backed up files will be placed. This is set when "Configuring or updating the Oracle Data Pump directory" on page 431. **Important:** Do not enter an explicit path when specifying the DIRECTORY parameter. Use `OP_DATAPUMP_DIRECTORY` only.

Example

```
impdp openpages/openpages@OP
 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 this `impdp` command to remap the schema:

```
Remap_schema=<source_schema>:<target_schema>
```

Example

```
impdp openpages/openpages@OP
 DIRECTORY=OP_DATAPUMP_DIRECTORY
 DUMPFILE=openpages_backup_YYYY_MM_DD_HH_MI_SS.dmp
 LOGFILE=openpages_import.log remap_schema=opuser:openpages
```

Update the OpenPages GRC Platform storage location in the Oracle database

After you restore the `openpage-storage` file from the product backup, you must update the IBM OpenPages GRC Platform storage location in the database.

Procedure

1. Log on to a system with administrative permissions. You can use any system with access to CLPPlus that can connect to the OpenPages database server.
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`

Table 134: Installation location of the OpenPages GRC Platform application	
Operating system	**Installation location**
Windows	By default, *<OP_Home>* is `C:\OpenPages`

Table 134: Installation location of the OpenPages GRC Platform application (continued)	
Operating system	**Installation location**
AIX and Linux	By default, *<OP_Home>* is `/opt/OpenPages`

3. Open a command or shell window and do the following:
   a) Navigate to the `OP_<version>_Non_Embedded` on your network drive or in the installation kit.
   b) Navigate to the `INSTALL_SCRIPTS` directory at the following location:

```
OP_<version>_Configuration|Database|ORACLE|INSTALL_SCRIPTS
```

4. From the `INSTALL_SCRIPTS` directory, run the `update-storage` SQL wrapper script with the following parameters (see Table 135 on page 445 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 135: 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 GRC Platform database instance, as set during the Oracle database installation.
`<op_db_user>`	The OpenPages GRC Platform user name for accessing the OpenPages GRC Platform database.
`<op_db_password>`	The OpenPages GRC Platform password for accessing the OpenPages GRC Platform database.
`<storage-type>`	The type of file storage to be used. Valid values are: • LFS (local file system) • UNC (Universal Naming Convention) **Note:** After you move from LFS to UNC, you cannot go back to using LFS.
`<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-wrapper.sql
```

```
 update-storage c:\temp\upd-storage-output.log
 op openpages openpages LFS eng11 eng11
 Windows c:\OpenPages\openpages-storage
```

AIX

```
sqlplus /nolog @sql-wrapper.sql
 update-storage /home/op/upd-storage-output.log
 op 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
 op openpages openpages UNC eng11
 eng11 Windows openpages-storage
```

  AIX

```
sqlplus /nolog @sql-wrapper.sql
 update-storage /home/op/upd-storage-output.log
 op openpages openpages UNC aix11 aix11
 Unix /usr/opdata/openpages-storage
```

Update the global search settings

After you import data from a production environment (the source environment) into a test or development environment (the target environment), you need to update the global search settings.

About this task

When you import data from the source environment, the settings for the search server are imported. You need to update the target environment so that it uses the search server in your target environment.

Procedure

1. Log in to the OpenPages application in the target environment as a user with administrative privileges.
2. If the global search component is enabled, disable it.
   a) Click **Administration** > **Global Search**.
   b) Click **Disable**.
3. Stop the global search services.

   For more information, see “Start or stop the global search services” on page 553.
4. Update the global search settings.
   a) Click **Administration** > **Settings** > **Applications** > **Common** > **Configuration** > **Show Hidden Settings** and set the value to `true`.
   b) Click **Administration** > **Settings** > **Platform** > **Search** > **Admin** and update the **Search Server Administration URL**with the URL of the search server in your target environment.
   c) Click **Administration** > **Settings** > **Platform** > **Search** > **Index** and update the **Search Server URL** with the URL of the search server in your target environment.
   d) Click **Administration** > **Settings** > **Platform** > **Search** > **Request** and update the **Search Server URL** with the URL of the search server in your target environment.
5. If the source environment is using IBM OpenPages GRC Platform version 7.3 or later, do the following steps.
   a) Copy the *<SEARCH_HOME>*`/openpages-solr-index` directory to the search server in the target environment.

      The *<SEARCH_HOME>*`/openpages-solr-index` contains the global search index.

b) Start the global search services.

For more information, see “Start or stop the global search services” on page 553.

c) Enable global search. Click **Administration** > **Global Search** > **Enable**.

6. If the source environment is using IBM OpenPages GRC Platform version 7.2.x, drop and then re-create the global search index.

a) Start the global search services.

For more information, see “Start or stop the global search services” on page 553.

b) Click **Administration** > **Global Search** > **Drop**. Wait for the process to complete.

c) Click **Create**.

Results

Global search is enabled in the target environment.

Update Cognos data in the test environment

You can update Cognos data in the test environment by using the Cognos backup utility.

Before you begin

Before you run the Cognos 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 Cognos server.

Backup Cognos production Oracle 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 Cognos server as a user with administrative permissions.
2. Run the Cognos backup utility (`OPCCBackup`) to back up the Cognos database and configuration files.

   For more information, see “Using the Cognos backup utility” on page 430.

   Tip: If the mail server for notification e-mails has not been set up for running Cognos 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 this step says `BUILD SUCCESSFUL`.
3. Copy the production Cognos server backup `.zip` or `.tar.gz` file to the Cognos 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`

Backing up the Cognos Oracle test data and files
You can back up test data and files.

Procedure

1. If necessary, log on to your test IBM OpenPages GRC Platform server as a user with administrative permissions.
2. Run the Cognos backup utility (OPCCBackup) as described in "Using the Cognos backup utility" on page 430 to back up the Cognos database and configuration files.

Restoring the Cognos data and files to the Oracle test environment
You can restore data and files to the test environment.

Procedure

1. Log on to your test IBM OpenPages GRC Platform 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 the objects in the schema on the test server:

      `@AuroraDbDelete.sql`

   c) When finished, log out of SQL*Plus.
3. Import the Cognos 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 Cognos database:

   ```
   impdp <cognos_db_user>/<cognos_db_password>@<SID>
    DIRECTORY=OP_DATAPUMP_DIRECTORY
    DUMPFILE=<cc_dump_file> LOGFILE=cc_import.log
   ```

   Where:

Table 136: Parameters and their descriptions

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).

Table 136: Parameters and their descriptions (continued)	
Parameter	**Description**
<cc_dump_file>	The .dmp file name of the backed up Cognos database.

```
Example
impdp cognos/cognos@OP 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 this impdp command to remap the schema:

```
Remap_schema=<source_schema>:<target_schema>
```

Example

```
impdp cognos/cognos@OP 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 Oracle data sources

The following procedure describes how to manually update the signon password for the user account to access data sources.

Depending on the type of installation, one or both of the following Oracle data source links are displayed in the IBM Cognos Administration tool for the reporting framework:

- The **OpenPages DataSource** is used for the Reporting Framework V6. V6 refers to the latest framework version, not to any specific OpenPages release number.
- For Oracle Database environments only, the **Oracle Native Driver** is used for the Legacy Reporting Framework (upgraded systems only).

Note: For Oracle Database environments only, 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. From a browser, log on to the Cognos Analytics portal as a user with administrative privileges, for example, OpenPagesAdministrator.

   By default, the URL is http://<hostname>/ibmcognos/bi

   Where <hostname> is the name of the Cognos server.
2. Click **Manage** > **Administration Console** to launch the **IBM Cognos Administration** page.
3. On the **Configuration** tab, click **Data Source Connections** (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.

Updating Oracle database connection references for reports
You can update the database connection references for reports.

Procedure

1. From a browser, log on to the Cognos Analytics portal as a user with administrative privileges, for example, OpenPagesAdministrator.

   By default, the URL is:

   `http://<hostname>/ibmcognos/bi` (if you are using port 80 for Cognos)

   Where <hostname> is the name of the Cognos server.
2. Click **Manage** > **Administration Console** to launch the **IBM Cognos Administration** page.
3. On the **Configuration** tab, click **Data Source Connections** (if not already selected).
4. On the **Directory > Cognos** page, click the link for the IBM OpenPages GRC Platform data source.
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) On the **OCI** tab, 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) On the **JDBC** tab, in the **Server name**, **Port number**, and **Oracle Service ID** boxes, change the values to valid values for the IBM OpenPages GRC Platform database on the target environment.
8. 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 triggers

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 GRC Platform 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 "Backing up and copying the OpenPages GRC Platform application production files for an Oracle database" on page 442, 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.

Table 137: Installation location of the OpenPages GRC Platform application	
Operating system	**Installation location**
Windows	*<OP_Home>*\aurora\lib\openpages-ext.jar By default *<OP_Home>* is C:\OpenPages
AIX and Linux	*<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.

Copy other custom deliverables to the test environment

If you have other custom deliverables, such as UI helpers and JSP reports, copy these custom deliverables to their respective folders on the test or target machine.

If you have any questions about the location of your custom data, contact your IBM representative.

Procedure

1. From your application production backup .zip files, extract all custom files such as JAR files, JSP files, JavaScript files, and Image files.
2. Copy these files into their respective folders on the target machine. The target folders should match the folders on the source installation.

Starting the OpenPages GRC Platform in the test environment

When finished, start IBM OpenPages GRC Platform services on the servers in your test environment.

For details, see Chapter 20, "Starting and stopping servers," on page 549.

Update URL host pointers for Cognos reports

Modify the URL host pointer settings and then propagate these changes to the reporting schema on the application server (does not require services to be restarted).

For more information, see "Updating URL host pointers for reports" on page 478.

Utilities for filtering on long string field content in an Oracle database

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.

Warning: Do not include long string fields that are encrypted using field level encryption in the search criteria because they can return unexpected results.

Long string fields allow users to enter values over 4KB in length. To apply filters on the content of these long string fields, first "Enabling Oracle Text" on page 453 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 "Long string fields" on page 174.

There are five utilities provided to help manage full text searching:

- "Enabling Oracle Text" on page 453
- "Create a long string index for an Oracle database" on page 452

- “Create a schedule job to synchronize a long string index” on page 454
- “Drop a long string index” on page 455
- “Modifying the list of stop words” on page 456

To apply filters with long string fields, you must change the **OpenPages** > **Platform** > **Database** > **Text Indexes** setting to **true**.

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Table 138: Values and what they mean

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 Chapter 15, “Viewing the Configuration and Settings page,” on page 307.

Create a long string index for an Oracle database

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, AIX, and Linux.

Before you begin

Oracle Text must be enabled. See “Enabling Oracle Text” on page 453.

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 IBM OpenPages GRC Platform database server.
2. Open a command or shell window, navigate to the `full-text-index` directory as follows.

   The following table identifies the installation location of the application on the Microsoft Windows, AIX, and Linux operating systems.

   Table 139: Installation location of the full-text-index directory

Operating system	Installation location
Windows	*<OP_Home>*`\aurora\bin\full-text-index`
AIX and Linux	*<OP_Home>*`/aurora/bin/full-text-index`

   Note: If the database server is not on the same computer as the OpenPages server, you must copy the script, and the SQL files it starts, 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 and Linux

   ```
   CreateOpenPagesTextIndex.sh <SID> <OPX_USER_NAME> <OPX_USER_PASSWORD>
   <MEMORY_LIMIT> <PARALLEL_INDEXING_DEGREE>
   ```

Table 140: Parameters	
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 runtime 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.

Enabling Oracle Text

Enable the Oracle Text feature to filter based on the contents of fields with long string data types. Scripts are provided for Windows, AIX, and Linux.

Procedure

1. Log on to the Oracle database server as a user with database administrator privileges.

   Note: You can enable only Oracle Text from the database server.
2. Open a command or shell window, navigate to the `full-text-index` directory as follows.

   The following table identifies the installation location of the application on the Microsoft Windows, AIX, and Linux operating systems.

Table 141: Installation location of the full-text-index directory	
Operating system	**Installation location**
Windows	*<OP_Home>*`\aurora\bin\full-text-index`
AIX and Linux	*<OP_Home>*`/aurora/bin/full-text-index`

   Note: If the database server is not on the same computer as the IBM OpenPages GRC Platform server, copy the script and the SQL files to the database server.
3. Run the following batch command:

   Windows

   ```
   EnableOpenPagesTextIndexing.bat <SID> <SYSDBA_USER_NAME>
   <SYSDBA_PASSWORD> <OPX_USER_NAME>
   ```

   AIX and Linux

   ```
   EnableOpenPagesTextIndexing.sh <SID> <SYSDBA_USER_NAME> <SYSDBA_PASSWORD>
   <OPX_USER_NAME>
   ```

   Note: All parameters are required.

Table 142: Parameters in the batch command	
Parameter name	**Description**
<SID>	The system ID or TNS alias for the OpenPages GRC Platform database instance.
<SYSDBA_USER_NAME>	Database SYSDBA account. Usually 'SYS' user.

Table 142: Parameters in the batch command (continued)	
Parameter name	**Description**
<SYSDBA_PASSWORD>	Password for SYSDBA user account.
<OPX_USER_NAME>	OpenPages GRC Platform application schema owner name.

Results

The database is now enabled for indexing. Use "Create a long string index for an Oracle database" on page 452 script to create the index.

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, AIX and Linux.

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 IBM OpenPages GRC Platform database server.
2. Open a command or shell window, then navigate to the `full-text-index` directory as follows.

   The following table identifies the installation location of the application on the Microsoft Windows, AIX, and Linux operating systems.

Table 143: Installation location of the full-text-index directory	
Operating system	**Installation location**
Windows	*<OP_Home>*\aurora\bin\full-text-index
AIX and Linux	*<OP_Home>*/aurora/bin/full-text-index

   Note: If the database server is not on the same machine as the 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 and Linux

   ```
   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>
   ```

Table 144: Parameters	
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.

Table 144: Parameters (continued)	
Parameter name	**Description**
<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 runtime 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 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 repeats every day 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, AIX and Linux.

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 IBM OpenPages GRC Platform database server.
2. Open a command or shell window, then navigate to the `full-text-index` directory as follows.

   The following table identifies the installation location of the application on the Microsoft Windows, AIX, and Linux operating systems.

Table 145: Installation location of the full-text-index directory	
Operating system	**Installation location**
Windows	*<OP_Home>*`\aurora\bin\full-text-index`
AIX and Linux	*<OP_Home>*`/aurora/bin/full-text-index`

Note: If the database server is not on the same machine as the 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 and Linux

   ```
   DropOpenPagesTextIndex.sh <SID> <OPX_USER_NAME> <OPX_USER_PASSWORD>
   ```

Table 146: Parameters

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.

What to do next

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 for an Oracle database” on page 452.

Modifying the list of stop words

You can change the default list of stop words used by the Oracle Text feature. A stop word is 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 for an Oracle database” on page 452 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 following, commented out sections:

```
/*
    ADD_STOPWORD_TO_ARRAY
    (
    p_name                => 'me'
    );
    */
```

For example, if you want to add the stop word "the", copy the preceding section, remove the comment sign, and replace "me" with "the" as follows. 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 concatenation 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.

To concatenate simple strings, the fields must be unencrypted. After you use the concatenation utility, you can encrypt the new long text field.

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 IBM OpenPages GRC Platform database server.

String concatenation is a database operation. A SQL template file is provided to specify parameters for the action. For more information, see "Running string concatenation" on page 457.

For more information on long text fields, see "Long string fields" on page 174 .

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.
- When you concatenate multiple strings, if field level security is applied to any of the strings, then after concatenation into a single, large long text field, some hidden values can be visible. To prevent unauthorized users from viewing the values for a concatenated string, apply the same field level security rule to the large long text field.

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 IBM OpenPages GRC Platform database server.
2. Stop all services (see Chapter 20, "Starting and stopping servers," on page 549).
3. Navigate to the `field-concat-utility` folder located in the `bin` directory:

Table 147: Installation locations

Operating system	Installation location
Windows	*<OP_Home>*`\aurora\bin`
AIX and Linux	*<OP_Home>*`/aurora/bin`

4. Copy the contents of the SQL template `field_concat_template.sql` into a new file.
5. 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 "The string concatenation SQL file" on page 458.

   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.

6. 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>
   ```

Table 148: Parameters	
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;
   ```

7. Start all services (see Chapter 20, “Starting and stopping servers,” on page 549).
8. Optional: Apply a field level security rule to the large long text field. For more information, see “Field level security” on page 69.

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 “The string concatenation SQL file” on page 458.

The string concatenation SQL file

IBM OpenPages GRC Platform 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 457 .

Parameters

Table 149: 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.
l_field_group_name_src<#>	The name of the field group containing the simple string field. Where: <#> is a value from 01 to 08. • 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. • 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 149: 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.
	• 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. 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. • 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. • 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.
l_property_desc	The description of the destination long text field.

Table 149: field_concat_template.sql parameters (continued)	
Parameter	**Description**
l_large_text_length	The length property of the destination field. The default is OP_OBJ_MODEL_MGR.g_dl_longtext_medium. 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 479
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 149: 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;
```

Entity Move/Rename utility

The IBM OpenPages GRC Platform Entity Move/Rename utility allows batch processing of multiple Business Entities for overnight or weekend execution without running the risk of operations that time out. You can run the utility interactively or as a scheduled job.

Using the Entity Move/Rename utility, you can do the following:

- Rename a Business Entity hierarchy
- Simultaneously rename and move a Business Entity hierarchy

A single batch job can contain multiple independent operations, multiple dependent operations, or any combination thereof.

Each operation provides transactional consistency. If an operation fails, all the pending changes for this operation are rolled back. If an operation succeeds, all the changes are persisted.

Each rename, move, or combined operation runs in its own transactional context. So, failure in one operation does not result in the failure of the entire batch job.

CAUTION: Before running the utility, you must stop all application services to avoid data or security errors.

Entity Move/Rename utility prerequisites

Before you use the IBM OpenPages GRC Platform Entity Move/Rename utility, consider these prerequisites.

- A physical computer or VM that meets the OpenPages GRC Platform installation requirements. For detailed specifications, see the *IBM OpenPages GRC Installation and Deployment Guide*.
- An application that produces either CSV (comma-separated value) files or Unicode tab delimited files. This application can be installed on any computer in your environment and is used to prepare the input data for the utility.
- User name and password for the Oracle or DB2 account that owns the OpenPages application database schema (for example, OPENPAGES).

Configuring the Entity Move/Rename utility for an Oracle database

You must configure parameters in the OpenPages GRC Platform Entity Move/Rename utility before you use it in an Oracle database environment.

Procedure

1. Go to the Entity Move/Rename utility installation location as follows:

   OP_Home|`aurora`|`bin`|`batch_entity_move_rename_relative`
2. Open the `batch-entity-move-rename.ini` configuration file for editing.
3. Specify appropriate values in the following parameters for an Oracle database environment:

Table 150: Parameters for an Oracle database in the `batch-entity-move-rename.ini` file:

Parameter Name	Description

connect_string	Oracle database connection details. Use either the TNS alias or EZCONNECT format.
	TNS:
	`<user>/<password>@<TNS alias>`
	EZCONNECT:
	`<user>/<password>@//<host>:<port>/<sid>`

Table 150: Parameters for an Oracle database in the batch-entity-move-rename.ini file: (continued)	
Parameter Name	**Description**
data_format	Format of the input file to the utility. Example: csv or unicode-text Use the csv file format as follows: • Only if the data is known to contain ASCII characters exclusively. • All the national characters in the data input file are produced from the same Windows or ISO code page that is configured on the computer. You must specify the correct Oracle character set name that matches the code page in the character_set parameter.
input_file	Name of the input file (including extension). Example: 'Sample-batch-entity-move-rename.txt'
character_set	ANSI/ISO character set that is used by the utility. If the data_format parameter is set to csv, you must use a correct Oracle character set name that corresponds to the ANSI/ISO code page used by the OS (such as, WE8MSWIN1252). If the data_format parameter is set to unicode-text, this parameter is ignored.
skip_rows	The number of rows in the input files to skip on load. Example If the first row of the file: • Contains a list of column names, set the value to '1'. • Does not contain a list of column names, set this value to '0'.

4. Save and close the batch-entity-move-rename.ini configuration file.
5. Prepare the input file. See "Prepare the input file for the Entity Move/Rename utility" on page 414.

Prepare the input file for the Entity Move/Rename utility

The input file for the Entity Move/Rename utility can be in CSV or Unicode tab delimited format. You can use any editor to create the input files. Included in the utility installation folder is a sample Unicode text file (.txt format).

Important: On AIX and Linux, the text input file must be saved or converted to be encoded in UCS-2 Little Endian and have UNIX end of line (LF) characters.

Tip: If you are using Microsoft Excel, you must save the spreadsheet as a CSV or tab delimited file.

The input file must have the following five columns of data:

Table 151: Columns in the input file		
Column Name	**Description**	**Sample Value**
Source entity location	The entity on which the operation is run.	/The Bank/USA/North East/Providence

Table 151: Columns in the input file (continued)

Column Name	Description	Sample Value
Target entity location	The new parent entity for "move" and "move and rename" operations only. **Note:** • For Oracle "rename" operations only (no move), the value must be "-" (dash). • For DB2 "rename" operations only (no move), the value must be blank.	For "move" and "move and rename" operations: `/Worldwide/Americas/USA/NE`
Run as user	Application user name, whose identity is used to run the operation.	`OpenPagesAdministrator`
New entity name	The new name after the operation for "rename" and "move and rename" operations only. **Note:** • For Oracle "move" operations only (no rename), the value must be "-" (dash). • For DB2 "move" operations only (no rename), the value must be blank.	For "rename" and "move and rename" operations: `Boston`
Execution order	Establishes the operation execution order as follows: • Operations that specify the execution order are run before operations that do not. • Operations that have a numeric value in the execution order column are run in regular ascending ordering. If set, the value must to be a valid number; Otherwise, leave the field blank.	1

The following is a short description of the data in the sample `.txt` file that is included in the utility directory.

- The first line illustrates moving entity `/The Bank/USA/North East/Providence` to new location `/Worldwide/Americas/USA/NE`. Operation is to be run as the user `SOXAdministrator`. This operation is run first in the batch.
- The second line illustrates in place rename of the entity `/Worldwide/Americas/USA/NE/Providence`. Entity name changes to Boston. Target location does not apply and is set to "-". This entry has a dependency on the previous move operation and has higher number in the execution order column. Also, it references to the new entity location that will be in effect after the first operation completes.
- If the first operation fails for any reason, this operation fails as well and the entity location would be incorrect.
- The third line illustrates simultaneous move of the entity `/The Bank/USA/Midwest/Chicago` to new location `/Worldwide/Americas/USA/MW` and rename to Detroit. This operation has no dependencies and will be run after the first two complete.

If you have an Oracle database with the 32-bit SQL*Loader utility and an IBMAIXor Linux environment, see the topic: "Avoid error 0509-036 when you use the 32-bit Oracle SQL*Loader" on page 466. Otherwise, run the IBM OpenPages GRC Platform Entity Move/Rename utility.

Avoid error 0509-036 when you use the 32-bit Oracle SQL*Loader

This task applies only to the Entity Move/Rename operation if you use the 32-bit SQL*Loader utility with Oracle databases in IBM AIX or Linux environments. Skip this task if you are using the 64-bit SQL*Loader utility.

If you use the 32-bit SQL*Loader (`sqlldr`) utility, the following system error might be displayed:

```
exec(): 0509-036 Cannot load program sqlldr because of the following errors:
        0509-026 System error: There is not enough memory available now.
Failure while executing the Oracle SQL*Loader. Exit code is 255
```

If the `0509-036` system error is displayed, you can set the Loader Control environment variable by opening a shell window and running the following command:

```
export LDR_CNTRL=MAXDATA=0x80000000 at LARGE_PAGE_DATA=Y
```

Tip: If you are running the IBM OpenPages GRC Platform Entity Move/Rename utility as a scheduled `cron` job, make sure to set the Loader Control environment variable in the `cron` environment.

When finished, run the IBM OpenPages Entity Move/Rename utility. See "Running the entity move/rename utility interactively" on page 466 or "Running the Entity Move/Rename utility as a scheduled task" on page 416.

Running the entity move/rename utility interactively

Use the following steps to run the IBM OpenPages GRC Platform Entity Move/Rename utility interactively in an Oracle database environment.

Before you begin, make sure that you prepared the input file. See "Prepare the input file for the Entity Move/Rename utility" on page 414 for instructions.

Procedure

1. Move the input file into the utility installation directory, which is at:

   ```
   OP_Home|aurora|bin|batch_entity_move_rename_relative
   ```

2. Validate that the input_file parameter in the `batch-entity-move-rename.ini` configuration file is correctly set to the input file name. For more information, see "Configuring the Entity Move/Rename utility for an Oracle database" on page 463.
3. From the location where the utility is installed, run the batch command file and review the output on the screen.

   Windows
   `batch-entity-move-rename.cmd`

   AIX or Linux
   `batch-entity-move-rename.sh`
4. Upon completion, review the following log files for any errors:

   - `batch-entity-move-rename-load.log`
   - `batch-entity-move-rename-proc.log`

   If any errors are reported and you are unable to fix them, contact your IBM Support representative. Make sure you supply a copy of the screen that contains the error messages and all the log files that are generated by the tool.

Running the Entity Move/Rename utility as a scheduled task

You can set up a scheduled task to run the IBM OpenPages GRC Platform Entity Move/Rename utility.

Depending on your environment, you can run the `batch-entity-move-rename` batch command file by using any scheduling application. For example, in Windows, you might use the built-in Windows scheduler. In IBM AIX or Linux, you might set up a `cron` job.

Important: If you are using a DB2 database in a Windows environment, you must run the batch command file within the **DB2 Command Line Processor**.

If the job fails, the batch command returns a non-zero exit code. You can redirect the console output to a log file. For example, in Windows:

```
batch-entity-move-rename.cmd >> batch-entity-move-rename.log
```

The following files are overwritten on each run:

- `batch-entity-move-rename-load.log`
- `batch-entity-move-rename-proc.log`

These files can be saved, either manually or through a script, if log archives are needed.

Impact of the Entity Move/Rename utility on the OpenPages GRC Platform application

The Entity Move/Rename utility works directly against the IBM OpenPages GRC Platform database repository. As a result, the Java based OpenPages GRC application is unaware of the changes made to the entity hierarchy and folder structure.

As a result, internal application caches might become out of sync with the data in the repository and lead to discrepancies in the application user interface.

It is required that after you run the tool you restart application services, or run the tool when application services are stopped.

Also, ensure that the `OPBackup` command is not running during execution, and that all batch rename and move operations are completed before you run a backup.

Chapter 19. System Maintenance

You can perform system maintenance tasks such as changing the default port numbers, changing password references, updating values in property files, and so on.

Application server restrictions

When you are performing system maintenance, be aware of the restrictions for IBM OpenPages GRC Platform application servers.

- Do not rename application servers. The OpenPages property files contain hard-coded references to the application servers.
- Do not rename IBM WebSphere Application Server nodes. The WebSphere nodes for OpenPages use a specific naming convention, and the OpenPages Administrative Console is dependent on the naming convention.

Port assignments

Both dedicated ports and ports that are dynamically assigned for each installation are used for the IBM OpenPages GRC Platform installation. These default ports can be changed after installation.

Default ports

The following table lists the default ports.

Table 152: Default fixed port assignments

Description	Ports
OpenPages installation server	8443
OpenPages installation agent	8443
OpenPages database instance (Oracle)	1521
OpenPages database instance (IBM DB2)	50000
OpenPages deployment manager	9060
OpenPages deployment manager (SSL)	9043
OpenPages application URL	10108
OpenPages application URL (SSL)	10111
OpenPages deployment manager SOAP port	8879
Cognos Analytics gateway (as configured for your web server)	80
Framework Generator port	8080
Cognos Analytics dispatcher URI	9300

Table 152: Default fixed port assignments (continued)	
Description	**Ports**
Search server (used for indexing and searching OpenPages data)	8983
Search server (used to administer global search)	8985

On Windows computers, additional OpenPages installations increment the port numbers by two.

Files containing port numbers

After installation, you can view the OpenPages port assignments by using the IBM WebSphere Administrative Console.

The following tables list property files on the OpenPages admin application server that contain port numbers for other components.

Table 153: Files that contain port numbers		
Port	**File name**	**Parameter Name**
Oracle database instance port	`<ORACLE_HOME>/NETWORK/ADMIN/tnsnames.ora`	N/A
Framework Generator port	`<OP_HOME>/aurora/conf/aurora.properties`	cognos.framework.refresh.servlet
Cognos Analytics server port	`<OP_HOME>/aurora/conf/aurora.properties`	cognos.server
Cognos Analytics Dispatcher URI	`<OP_HOME>/aurora/conf/aurora.properties`	cognos.computation.server

Dynamically assigned ports

Port numbers for IBM OpenPages GRC Platform servers that are not listed, such as OpenPages non-admin application servers, are assigned dynamically during the installation.

OpenPages application non-admin server port numbers start at 9080 and increment by 1 for each additional server in the installation.

After installation, you can view all port assignments by using the IBM WebSphere Administrative Console.

Change default port numbers

You can change the default IBM OpenPages GRC Platform port numbers after installation.

Important: Only ports 80, 443, or an open port in the range 1024 - 65535 can be used as the IBM OpenPages GRC Platform application port number.

The OpenPages GRC Platform installer sets several default ports during installation, such as the ports for the OpenPages server.

After installing the application, you can change the OpenPages ports to 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.

For a port conflict, change all of the OpenPages application server ports to a new range. Follow the instructions in the following section.

Important:

- Do not change the port number for the OpenPages GRC Platform administrative server.
- To modify port numbers on other application servers in a cluster, repeat the following tasks on each cluster member.

Checking 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 GRC Platform application ports for an IBM WebSphere Application Server environment

Because the IBM OpenPages GRC Platform application on the IBM WebSphere Application Server uses port ranges, if you need to change one of the OpenPages environment port numbers, you should change all of the OpenPages application server ports to a new range.

Important: This information applies only to IBM WebSphere environments.

By default, the OpenPages GRC Platform application on the IBM WebSphere Application Server uses the port range 10101-10120.

Stopping the OpenPages GRC Platform application servers

Before changing the ports, make sure that all managed IBM OpenPages GRC Platform application 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 or Linux 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 for which you want to change the port numbers:

      ```
      ./stopServer.sh <host_name>-OPNode1Server<#>
      ```

      Where *<#>* is the number of the OpenPages application server.

Updating the port numbers in the Admin Console

Use the following steps to change the default port numbers on an IBM OpenPages GRC Platform application server.

Procedure

1. Open a browser window and navigate to the following address to launch IBM WebSphere Integrated Solutions Console for the OpenPages GRC Platform application, by default:

   `http://<server_name>:<port>/ibm/console` where `<server_name>` is the name of the server where the IBM WebSphere Application Server is installed and `<port>` is the OpenPages GRC Platform application port. For more information see "Port assignments" on page 469.
2. Log on to the IBM WebSphere Integrated Solutions Console as a user with administrative privileges.
3. Expand **Servers** then **Server Types** 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, it is best to 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, 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 GRC Platform application port (by default, `10108`) and/or OpenPages application SSL port (by default, `10111`), update the port numbers in the default OpenPages GRC Platform application virtual hosts created by the IBM WebSphere Application Server as follows:
   a) In 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 GRC Platform application (`WC_defaulthost`) port you changed. The port numbers listed are the previous port numbers for each port.

      For example, if the application port for the OpenPages GRC Platform 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, click **Save** to commit the changes to the master configuration.
   h) On the **Host Aliases** page, click ***** to select the OpenPages GRC Platform 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, click **Save** to commit the changes to the master configuration.

Updating Ports to the Java Messaging Service

If you changed the IBM WebSphere Service Integration Bus (SIB) messaging service endpoint port for the IBM OpenPages GRC Platform application server (by default, 10115), you need to change other settings within the OpenPages application server.

If you did not change the SIB Endpoint Address, skip to the task "Updating port values in IBM OpenPages property files" on page 474.

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

"Updating the Java Messaging ports on the OpenPages GRC Platform server" on page 473

Updating the Java Messaging ports on the OpenPages GRC Platform server

Launch the IBM WebSphere Integrated Solutions Console for the IBM OpenPages GRC Platform application and update the OpenPages ports used by the Java Messaging Service.

Procedure

1. On the IBM WebSphere Integrated Solutions Console for the OpenPages GRC Platform application (`http://<server_name>:<port>/ibm/console`), update the OpenPages topic connection factories with the new port number(s) set previously.

   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** 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, click **Save** to commit the changes to the master configuration.

2. Update the OpenPages server activation specifications with the new port number(s) set previously.

   a) In the **Resources** > **JMS** tree, 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, 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 previous steps to change the OpenPages SIB endpoint address:
`<server_name>:<SIB_ENDPOINT_ADDRESS>:BootstrapBasicMessaging`

i) In the **Messages** box that appears, click **Save** to commit the changes to the master configuration.

3. Log out of the IBM WebSphere Integrated Solutions Console for the OpenPages server.

Updating port values in IBM OpenPages property files
If you changed the IBM OpenPages GRC Platform 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`, `<server_name>-OPNode1Server<#>-sosa.properties`, and `<server_name>-OPNode1Server<#>-server.properties`.

Updating port values in the aurora property file
You can update port values in the `aurora.properties` file.

Procedure

1. Log on to the IBM OpenPages GRC Platform admin server associated with the application server for which you changed ports as a user with administrator privileges.
2. Open an AIX or Linux 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 and Linux
   `/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=
   ```

Updating port values in the OpenPages GRC Platform Sosa property file
You can update port values in the -sosa.properties file.

Procedure

1. In the AIX or Linux shell window, remain in the *<OP_Home>* | `aurora` | `conf` directory.
2. Locate the `<server_name>-OPNode1Server<#>-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 IBM OpenPages GRC Platform 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 GRC Platform application port number (by default, `10108`) update the port in the following property:

   ```
   application.url.path=
   ```

b) If you changed the OpenPages GRC Platform bootstrap port number (by default, 10101) update the port in the following property:

```
openpages.service.port=
```

Updating ObjectManager properties file
If you changed the IBM OpenPages GRC Platform 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 or Linux 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=
```

Updating the IBM WebSphere Application Server global security details

If you changed the default IBM WebSphere Application Server user name after you enabled REST API security or IBM WebSphere Application Server global security, you must update the op-backup-restore-env.sh file to use the new value.

Do this procedure on Linux and AIX application servers where you use OPBackup.sh and OPRestore.sh.

Procedure

1. Go to the *<OP_HOME>*/bin directory.
2. Open the op-backup-restore-env.sh file in a text editor.
3. Update the following variables:

```
WAS_ADMIN_USERNAME=admin
WAS_ADMIN_PASSWORD=$admin
```

For example:

```
WAS_ADMIN_USERNAME=IBMWASAdmin
WAS_ADMIN_PASSWORD=$IBMWASAdmin
```

Updating port values in RunTool.sh script

If you changed the IBM OpenPages GRC Platform 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.

Important: This information applies only to IBM WebSphere environments.

Procedure

1. In the AIX or Linux 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:

   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-$TOOL_NAME.jar "$@"
```

Updating port values in the database

If you updated any of the default IBM OpenPages GRC Platform ports, you must update the port value(s) in the REGISTRY_ENTRIES table in the IBM 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.

Updating port values on the Reporting server

If you changed the IBM OpenPages GRC Platform application port number, 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 or Linux shell window and navigate to the <Cognos_Home>|configuration directory where <Cognos_Home> represents the installation location of the Cognos application.
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 GRC Platform 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.

Changing the OpenPages GRC Platform Framework Generation port

You can change the port number that the IBM OpenPages GRC Platform Framework Model Generator Service runs on.

Procedure

1. Log on to the IBM Cognos Reporting Server as the owner of the OpenPages CommandCenter installation.

2. Stop the OpenPages Framework Model Generator Service.

   Windows:
   Right-click the IBMOpenPagesFrameworkModelGenerator service and select **Stop**.

   AIX and Linux:

   a. Open an AIX or Linux shell as a user with administrative privileges and navigate to the following directory:

   ```
   <CommandCenter_Home>/wlp/bin
   ```

   Where *<CommandCenter_Home>* is the installation location of OpenPages GRC Platform CommandCenter. By default, this location is: /opt/OpenPages/CommandCenter.

   b. Run the following command:

   ```
   server stop IBMOpenPagesFrameworkModelGenerator
   ```

3. In the server.xml file, update the HTTP and HTTPS port and allow a connection to the host from the remote system. For example:

```
<op_home>\CommandCenter\wlp\usr\servers\defaultServer
```

4. In the server.xml file, search for the following block of text:

```
<!-- A "Connector" represents an endpoint by which requests are received
    and responses are returned. Documentation at :
    Java HTTP Connector: /docs/config/http.html (blocking & non-blocking)
    Java AJP Connector: /docs/config/ajp.html
    APR (HTTP/AJP) Connector: /docs/apr.html
    Define a non-SSL HTTP/1.1 Connector on port 8080
    -->
    <Connector port="8080" protocol="HTTP/1.1"
    connectionTimeout="20000"
    redirectPort="8443" />
```

5. Change port="8080" to the port number you want the services to run on.
6. Start the OpenPages Framework Model Generator Service.

   Windows:
   Right-click the IBMOpenPagesFrameworkModelGenerator service and select **Start**.

   AIX and Linux:

   a. Open an AIX or Linux shell as a user with administrative privileges and navigate to the following directory:

   ```
   <CommandCenter_Home>/wlp/bin
   ```

   Where *<CommandCenter_Home>* is the installation location of OpenPages GRC Platform CommandCenter. By default, this location is: /opt/OpenPages/CommandCenter.

   b. Run the following command:

   ```
   server start IBMOpenPagesFrameworkModelGenerator
   ```

7. Log on to the OpenPages server as the OS owner of the OpenPages software and stop the services by using stopAllServers.
8. Go to the *<OPENPAGES_HOME>* | aurora | conf, where *<OPENPAGES_HOME>* is the installation location of the OpenPages software. Typically, the location is C:\OpenPages for Microsoft Windows servers and /opt/OpenPages for AIX and Linux systems.
9. In the aurora.properties file, change the port number for the following entry to the value that you set it to in step 5:

```
cognos.framework.refresh.servlet=http\://reporting-server\:8080/crf-refresher/
```

   In this case, you would change 8080 to the new port number.

10. Restart the OpenPages services.
11. Log on to OpenPages as the OpenPagesAdministrator.
12. Update the reporting schema and framework. For more information, see "Creating or recreating the reporting schema" on page 91.

What to do next

- Application server names - After OpenPages is installed, the application server name cannot be changed. Many configuration files, such as `aurora.properties`, include the application server names as an embedded string. The name cannot be changed after installation.
- Restart services - After you complete the port changes, restart OpenPages. For details, see Chapter 20, "Starting and stopping servers," on page 549.
- Update the reporting schema and Framework - After services are restarted, you must re-create the reporting schema and regenerate the Reporting Framework. Doing so allows the port change to be reflected in any redirects of reports. For more information, see "Creating or recreating the reporting schema" on page 91.

Updating URL host pointers for reports

After you migrate, change port settings in a production environment, or if you want to refresh a test environment from a production database, you must update the URL host pointers on the application server so that links in 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).

  Note: For SQL tool information, see the topic "Database tool information" in the *IBM OpenPages GRC Administrator's Guide*.
- Use the IBM OpenPages GRC Platform application user interface to re-create the entire reporting schema.

Procedure

1. Start the IBM OpenPages GRC Platform services on the admin application server.
2. Log on to the OpenPages GRC Platform application user interface as a user with administrator privileges.
3. Change the **Object URL Generator** settings.
   a) From the menu bar, click **Administration** > **Settings**.
   b) Expand **Platform** > **Reporting Schema** > **Object URL Generator**.
   c) Update the **Object Generator URL** settings, as required, to point to the application server (such as a test application server). Make sure to click **Save** after you modify each setting.

Table 154: Object Generator URL settings

Setting Name	Description
Host	The changed name of the application server. Example : `test-eng1`
Port	The changed port number of the application server. Example : 10108 (IBM WebSphere)

Table 154: Object Generator URL settings (continued)	
Setting Name	**Description**
Protocol	The changed protocol for accessing the application server. Valid values are either `http` or `https`.

4. To update the changed URL setting on the 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 a SQL tool and access to the database server, log on to SQL as the OpenPages GRC Platform 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;
/
```

   - Method 2: Re-create the entire reporting schema by using the application user interface. For details, see the topic "Creating or recreating the reporting schema" in the *IBM OpenPages GRC Administrator's Guide*.

Auditing configuration changes

The IBM OpenPages GRC Platform provides you with the capability of tracking configuration changes made to your system through the Configuration Audit Report.

Accessing the Configuration Audit Report

To view and generate the Configuration Audit Report, you must have the 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 IBM OpenPages GRC Platform V6 folder (if necessary, click the plus sign to expand the folder tree). In the folder tree, expand the **Audit Reports, Configuration** folders.

     Important: In reference to Reporting Framework V6, V6 refers to the latest framework version, not to any specific OpenPages release number.
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 Configuration Audit Report

The Configuration Audit Report tracks any metadata changes made to field groups, object types, application text, object text, profiles, and settings.

- 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.
- Profiles - such as modifying object views and showing or hiding object types and fields.
- Registry settings

Table 155 on page 480 describes the various audited configuration changes contained in the report under the following column headings:

Table 155: 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 might have to update or change the database or application server system password, or a server IP address. When you do, you must update the password in various places inside the OpenPages GRC Platform configuration files and property files.

Changing password references

There are several steps to changing password references.

Before you begin

Before you change password references for data sources in IBM OpenPages GRC Platform, make sure that you have the following:

- Administrative access to the following machines and application:
  - OpenPages application server
  - OpenPages Cognos server
  - Cognos Analytics portal
- The current and new password for the following database users:
  - OpenPages database user

About this task

To change a password reference, you must do the following tasks:

"Change password references on the OpenPages GRC Platform Application server" on page 481).

"Changing Reporting Framework password references" on page 482.

"Changing the password for OpenPages GRC Platform Administrator account" on page 483).

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 423.

Change password references on the OpenPages GRC Platform Application server

The process for changing the database password on the IBM OpenPages GRC Platform application server requires two tasks.

"IBM WebSphere: Modifying the JDBC data source password" on page 481

"Updating the application server database password in the Aurora properties file" on page 482

Important: Make a backup copy of each file before modifying it.

IBM WebSphere: Modifying the JDBC data source password

This task includes instructions for modifying the JDBC data source password.

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 admin server where IBM WebSphere is installed.

   `<port>` is the admin server port number. By default, the installation port numbers are:

   - `9060` for the IBM OpenPages GRC Platform server (`OpenPagesCell`)
2. Expand **Resources** then **JDBC** and click the **Data sources** link.
3. In the **Data sources** pane, depending on your server selection, do the following:

Table 156: Links in the Data Sources pane	
For updating this server...	**Click this link in the Data Sources table...**
application	`CWTxDataSourceXA`

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:

Table 157: Links in the JAAS - J2C authentication data pane	
For updating this server	**Click this link in the JAAS-J2C authentication data table**
application	`OpenPages JDBC authentication entry`

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**.

Updating the application server database password in the Aurora properties file

To change the database password on the IBM OpenPages GRC Platform application servers, one task that you must do is to edit the Aurora properties file.

Note: This information applies to Windows, AIX and Linux environments.

Procedure

1. Open a command or shell window and navigate to the *<OP_Home>* | `aurora` | `conf` directory.

Table 158: Installation location of the OpenPages GRC Platform application	
Operating system	**Installation location**
Windows	By default, *<OP_Home>* is `C:\OpenPages`
AIX and Linux	By default, *<OP_Home>* is `/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.

Changing Reporting Framework password references

If you change the password of the user account that is used by Cognos for updating the reporting framework, you must manually modify the password value in the `framework.properties` file on the Cognos server, and then restart services to re-encrypt the password.

Note: This information applies to Windows, AIX and Linux environments.

Procedure

1. Log on to the Cognos 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 and Linux: `/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 686).
7. When finished, update the data source password for the reporting framework (see "Change password references for Oracle data sources" on page 449).

Changing the password for OpenPages GRC Platform Administrator account

If IBM WebSphere Application Server global security is enabled on the IBM OpenPages GRC Platform application servers, you can change the password for the administrative user account.

For more information about configuring global security and changing the IBM WebSphere administrator user account password, see Configuring global administration security in IBM WebSphere.

Updating the Oracle Enterprise Manager 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 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.

Create the OpenPages GRC Platform application managed server instances

When working with cluster members, to create the new IBM OpenPages GRC Platform application managed server instances, use the following steps.

See "Parameters for cluster members" on page 529 for descriptions of the common parameters used in this procedure.

Procedure

1. Make sure that the following services are running:
   - **OpenPagesDmgr**
   - **OPNode1**
2. Navigate to the *<OP_Home>*|temp|perlinstall directory.

   <OP_Home> in the file path represents the installation location of the OpenPages GRC Platform application. The default path for a Windows installation is c:\OpenPages. The default path for an AIX and Linux installation is /opt/OpenPages.
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 "Masking passwords in the Install property file and Restart Services" on page 493.

   - 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>*

b) For Windows only, update the path separator in the WASCONFIG_PATH parameter from backslash to forward slash, except the escape character for the colon. For example, the value should look like this WASCONFIG_PATH=C\:/OpenPages/temp/wasconfig

c) When finished, save the file.

4. At an AIX or Linux shell prompt, or Windows command prompt, run the following Perl script:

a) perl addOPServer.pl <server_name>-OPNode1 *<server_name>*- OPNode1Server*<server#>*

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 and Linux
cd $ORACLE_HOME/bin

3. Type the following command to deconfigure the Oracle Enterprise Manager tool:

```
emca -deconfig dbcontrol db -repos drop
```

4. Type the following command to reconfigure the Oracle Enterprise Manager tool:

```
emca -config dbcontrol db -repos create
```

IBM WebSphere: Modifying the JDBC data source password

This task includes instructions for modifying the JDBC data source password.

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 admin server where IBM WebSphere is installed.

   <port> is the admin server port number. By default, the installation port numbers are:

   - 9060 for the IBM OpenPages GRC Platform server (OpenPagesCell)
2. Expand **Resources** then **JDBC** and click the **Data sources** link.
3. In the **Data sources** pane, depending on your server selection, do the following:

Table 159: Links in the Data Sources pane

For updating this server...	**Click this link in the Data Sources table...**
application	CWTxDataSourceXA

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:

Table 160: Links in the JAAS - J2C authentication data pane	
For updating this server	**Click this link in the JAAS-J2C authentication data table**
application	`OpenPages JDBC authentication entry`

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**.

Change password references on the OpenPages GRC Platform Application server

The process for changing the database password on the IBM OpenPages GRC Platform application server requires two tasks.

"IBM WebSphere: Modifying the JDBC data source password" on page 481

"Updating the application server database password in the Aurora properties file" on page 482

Important: Make a backup copy of each file before modifying it.

Changing database references

If you have 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 stand-alone 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 take the following actions:

"Modify the Connection URL for the JDBC Data Source" on page 485

"Modify Database References in the Application Configuration Files" on page 488

"Modify Database Connection References for the Reporting Server" on page 489

Before you begin

Make sure that you have the following information:

- Administrative access to the following machines and application:
  - OpenPages application server
  - OpenPages Cognos server
  - Cognos Analytics portal
  - OpenPages (if global security is enabled) system account user and password
- For Oracle database environments, the Oracle System Identifier (SID) of the new database instance.
- For IBM DB2 database environments, the database name.

Modify the Connection URL for the JDBC Data Source

This task includes instructions for modifying the JDBC data source in the IBM WebSphere Integrated Solutions Console for the application server. Select the instructions that correspond to your particular environment.

Oracle WebLogic - Modifying the Data Source Connection URL

This information applies only to Oracle WebLogic environments.

Procedure

1. Stop all IBM OpenPages application services except for the following administrative service:

Table 161: Administrative services to keep running	
If changing the reference on this server...	**Then only this service should be running...**
application	`OpenPagesAdminServer`

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 admin server port number. By default, the installation port numbers are:

   - `7001` for the IBM OpenPages server (`OpenPagesDomain`)
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 activity:

Table 162: Servers and data source links for Oracle WebLogic	
For updating this server...	**Click this link in the Data Sources table...**
application	`OpenPages Data Source`

6. On the **Settings for <data-source-name>Data Source** page, do the following tasks:
   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.
      - For Oracle database environments, the URL format might look similar to the following example.

        ```
        jdbc:oracle:thin:@//<host-name>:<port>/<SID>
        ```

        Where:
        – *host-name* is the name of the database server, such as `eng11`.
        – *port* is the database port number, such as `1521`.
        – *SID* is the Oracle System Identifier, such as `0P`.
      - For IBM DB2 environments, the URL format might look similar to the following example.

        ```
        jdbc:db2://<host-name>:<port>/<DATABASE_NAME>
        ```

        Where:
        – *host-name* is the name of the database server, such as `eng11`.

– *port* is the database port number, such as 50000.
– *DATABASE_NAME* is the name of the DB2 database, such as OP.

d) Click **Save**.

e) In the **Change Center** pane, click **Activate Changes** and log out.

Note: The password becomes encrypted when you save your change.

IBM WebSphere - Modifying the Data Source Connection URL

Note: This information applies only to IBM WebSphere Application Server 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 admin server where IBM WebSphere is installed.

   <port> is the admin server port number. By default, the installation port numbers are:

   • 9060 for the IBM OpenPages GRC Platform server (OpenPagesCell)
2. Expand **Resources** then **JDBC** and click the **Data sources** link.
3. In the **Data sources** pane, depending on your server selection, do the following:

Table 163: Servers and data source links for IBM WebSphere

For updating this server...	**Click this link in the Data Sources table...**
application	CWTxDataSourceXA

4. On the **Configuration** tab in the **Data sources** > **<Data-source-name>**, 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.
   • For Oracle database environments, the URL format might look similar to the following example.

   ```
   jdbc:oracle:thin:@//<host-name>:<port>/<SID>
   ```

   Where:
   – *host-name* is the name of the database server, such as eng11.
   – *port* is the database port number, such as 1521.
   – *SID* is the Oracle System Identifier, such as OP.
   • For IBM DB2 environments, the URL format might look similar to the following example.

   ```
   jdbc:db2://<host-name>:<port>/<DATABASE_NAME>
   ```

   Where:
   – *host-name* is the name of the database server, such as eng11.
   – *port* is the database port number, such as 50000.
   – *DATABASE_NAME* is the name of the DB2 database, such as OP.
   c) For IBM DB2 environments, in the **Database name** box, type the new database name.
   d) Click **Apply**.

5. In the **Messages** box, click **Save**.
6. Click **OK**.

Modify Database References in the Application Configuration Files

Use the following instructions to update database references in these files: `aurora.properties` and `op-backup-restore.env`. Once the values are updated, you will need to restart all administrative and managed servers to effect the changes.

Note: This information applies to Windows, AIX and Linux environments.

Modify the Database Reference in the Aurora Properties File

You can update the database references in the `aurora.properties` file.

Procedure

1. Open a command or shell window and go to the *<OP_Home>* | `aurora` | `conf` directory.
2. Locate the `aurora.properties` file in the `conf` directory and do the following tasks:
   a) Make a backup copy of the file before you modify 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 that follows the equal sign to the new database connection URL.
   - For Oracle database environments, the URL format might look similar to the following example.

     ```
     database.URL=jdbc\:oracle\:thin\:@//<host-name>\:<port>/<SID>
     ```

     Where:
     – *host-name* is the name of the database server, such as `eng11`.
     – *port* is the database port number, such as `1521`.
     – *SID* is the Oracle System Identifier, such as `OP`.
   - For IBM DB2 environments, the URL format might look similar to the following example.

     ```
     database.URL=jdbc\:db2\://<host-name>\:<port>/<DATABASE_NAME>
     ```

     Where:
     – *host-name* is the name of the database server, such as `eng11`.
     – *port* is the database port number, such as `50000`.
     – *DATABASE_NAME* is the name of the DB2 database, such as `OP`.

   e) Save your changes and exit the editor.

Oracle only - Modify Database References in the IBM OpenPages Backup and Restore Environment File

This task applies only to Oracle database environments. You must modify Oracle database references in the `op-backup-restore.env` file.

Procedure

1. Open a command or shell window and navigate to the *<OP_Home>* | `aurora` | `bin` directory.

   For information about *OP_Home*, see "Installation locations" on page xxvi.
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=<Database alias>`

Where:

- *-host-name* is the name of the database server, such as `eng11`.
- *-port* is the database port number, such as `1521`.
- *-SID* is the system ID of the database, such as `OP`.
- *-Database alias* is the alias of the database, such as `OP`.

d) Change the value following the equal sign to the new database connection URL and SID.

e) Save your changes and exit the editor.

Oracle only - Restart All Application Servers
This task applies only to Oracle database environments. When finished modifying the database reference values in the files, restart all administrative and managed servers to effect the changes.

See "Starting application servers" on page 549 for details.

Modify Database Connection References for the Reporting Server

Use the following instructions to update database references in the Cognos Analytics portal. If you have an Oracle database environment, you must also update the `op-cc-backup-restore.env` file.

Note: This information applies to Windows, AIX and Linux environments.

Once the values are updated, you will need to restart all administrative and managed servers to effect the changes.

Modifying database connection references in Cognos
You must change the database connection reference values in Cognos Analytics portal for the `OpenPages DataSource`. If you have an Oracle database environment, you must also update the `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 OpenPages GRC Platform application user interface as a user with administrative permissions.
3. From the navigation bar, select **Reporting** > **Cognos Analytics**.
4. Click **Manage** > **Administration Console** to launch the **IBM Cognos Administration** page.
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 **OCI** tab, on the **Edit the connection string - Oracle** page, edit the SID value in the **SQL*Net connect string** field.
   c) On the **JDBC** tab, edit the values in the **Server name**, **Port number**, and **Oracle Service ID** boxes.

9. For the Oracle Database environments, 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. Restart all administrative and managed servers.

Modifying the Oracle database reference in the Cognos backup and restore environment file
You must modify Oracle database references in the Cognos backup and restore environment file. This task applies only to Oracle database environments.

Procedure

1. Open a command or shell window and go to the *<CC_Home>* | `tools` | `bin` directory.
2. Locate the `op-cc-backup-restore.env` file in the `bin` directory and do the following tasks:
   a) Make a backup copy of the file before you modify 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 that follows the equal sign to the new Cognos database alias. The format might look similar to the following example:

   ```
   DB_ALIAS=<CommandCenter Database Alias>
   ```

   Example

   ```
   DB_ALIAS=OP
   ```

   e) Save your changes and exit the editor.

What to do next

After the values are updated, you will need to restart all administrative and managed servers to effect the changes.

Modifying database connection references in Cognos Configuration
You can modify database connection references in IBM Cognos Configuration.

Procedure

1. Log on to the reporting server as a user with administrative privileges.

   Note: For AIX and Linux 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 or Linux shell and navigate to the *<Cognos_Home>* | `bin64` directory.
   b) Execute one of the following commands to open the tool:

   Windows:
   `cogconfig.bat`

   AIX and Linux:
   `./cogconfig.sh`
3. In the **Explorer** pane, do the following:
   a) Expand **Data Access** (if not already expanded).
   b) Under **Content Manager**, click **Content store**.
4. In the properties 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, OP).

5. When finished, exit from Cognos Configuration.

What to do next

When finished modifying the database reference values in the files, restart the Cognos server to effect the changes.

See "Starting and stopping the Cognos services" on page 560 for details.

Update values in property files

Use the following instructions to modify and update values in property files.

- "Modifying values in the Sosa property file" on page 491
- "Running patch scripts to update server configuration" on page 493

Modifying values in the Sosa property file

When working with cluster members, modify values in the `-sosa.properties` file.

See "Parameters for cluster members" on page 529 for descriptions of the common parameters used in this procedure.

Procedure

1. In the *<OP_Home>* | `aurora` | `conf` directory, do the following:

   <OP_Home> in the file path represents the installation location of the IBM OpenPages GRC Platform application. The default path for a Windows installation is `c:\OpenPages`. The default path for an AIX and Linux installation is `/opt/OpenPages`.

   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.

Modifying the Stop Server script

To add information about the new managed server instance to the stop server scripts, follow this procedure.

Procedure

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

   <OP_Home> in the file path represents the installation location of the IBM OpenPages GRC Platform application. The default path for a Windows installation is `c:\OpenPages`. The default path for an AIX and Linux installation is `/opt/OpenPages`.

AIX and Linux only: do steps "2" on page 491-"4" on page 492.

2. Open the `stopAllServers.sh` script in a text editor.

3. 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.
4. When finished, save the file.

Windows only: do steps "5" on page 492-"8" on page 492.

5. Open the `stopAllServers.cmd` script in a text editor.
6. Locate the code to stop the `<server_name>-OPNode1Server1` server.
   For example:

```
if "%IS_SECURED_MODE%" == "true" (
    call %WAS_HOME%\bin\stopServer.bat OP-OPNode1Server1
     -user %ADMIN_USERNAME% -password %ADMIN_PASSWORD%
) else (
    call %WAS_HOME%\bin\stopServer.bat OP-OPNode1Server1
)
```

7. Copy that code after the existing and change the value to match the server number.
   For example:

```
if "%IS_SECURED_MODE%" == "true" (
    call %WAS_HOME%\bin\stopServer.bat OP-OPNode1Server2
     -user %ADMIN_USERNAME% -password %ADMIN_PASSWORD%
) else (
    call %WAS_HOME%\bin\stopServer.bat OP-OPNode1Server2
)
```

8. When finished, save the file.

Modifying the Start Server script

To add information about the new managed server instance to the start server scripts, follow this procedure.

Procedure

1. Navigate to the *<OP_Home>* | `bin` directory.
   <OP_Home> in the file path represents the installation location of the IBM OpenPages GRC Platform application. The default path for a Windows installation is `c:\OpenPages`. The default path for an AIX and Linux installation is `/opt/OpenPages`.

AIX and Linux only: do steps "2" on page 492-"4" on page 492.

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. When finished, save the file.

Windows only: do steps "5" on page 492-"8" on page 493.

5. Open the `startAllServers.cmd` script in a text editor.
6. Locate the code to start the `<server_name>-OPNode1Server1` server.
   For example:

```
if "%IS_SECURED_MODE%" == "true" (
    call %WAS_HOME%\bin\startServer.bat OP-OPNode1Server1
     -user %ADMIN_USERNAME% -password %ADMIN_PASSWORD%
) else (
```

```
    call %WAS_HOME%\bin\startServer.bat OP-OPNode1Server1
)
```

7. Copy that code after the existing and change the value to match the server number.

   For example:

```
if "%IS_SECURED_MODE%" == "true" (
    call %WAS_HOME%\bin\startServer.bat OP-OPNode1Server2
     -user %ADMIN_USERNAME% -password %ADMIN_PASSWORD%
) else (
    call %WAS_HOME%\bin\startServer.bat OP-OPNode1Server2
)
```

8. When finished, save the file.

Running patch scripts to update server configuration

To update the new cluster member with the updated configuration on the IBM OpenPages GRC Platform server and run the `updateOPPatch.pl` perl script.

Important: This task applies to AIX and Linux environments where the OpenPages GRC Platform 6.0.1 fresh installer was used to install the product. If you use the IBM OpenPages 6.1 installer, or a newer version, to install the product, then you do not need to perform this task.

Procedure

1. Navigate to the following directory:

   <OP_Home>|`temp`|`perlinstall`

   <OP_Home> in the file path represents the installation location of the OpenPages GRC Platform application. The default path for a Windows installation is `c:\OpenPages`. The default path for an AIX and Linux installation is `/opt/OpenPages`.
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 GRC Platform server as follows:

```
perl updateOPPatch.pl <server_name>-OPNode1
<server_name>-OPNode1Server<server#>
```

Masking passwords in the Install property file and Restart Services

For security purposes, use this procedure to manually mask the plain text passwords that you entered in the `install.properties` files.

For more information about entering passwords in the in the `install.properties` files, see “Create the OpenPages GRC Platform application managed server instances” on page 483.

Procedure

1. Navigate to the *<OP_Home>*|`temp`|`perlinstall` directory.

   <OP_Home> in the file path represents the installation location of the IBM OpenPages GRC Platform application. The default path for a Windows installation is `c:\OpenPages`. The default path for an AIX and Linux installation is `/opt/OpenPages`.
2. Open the `install.properties` file in a text editor.
3. 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= *****

4. When finished, save the file.
5. 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
6. Restart all services.

   For details on starting services, see Chapter 20, “Starting and stopping servers,” on page 549

SSL for OpenPages GRC Platform environments

You can configure your OpenPages GRC Platform to use Secure Sockets Layer (SSL).

SSL establishes an encrypted link between the OpenPages GRC Platform application server and the user through a browser. The encryption ensures that all data that is passed between the application server and a browser remains private.

Tip: For more information about how to set up SSL for OpenPages GRC Platform, see the GRC Power Plant community (http://www.ibm.com/developerworks/community/groups/service/html/communityoverview?communityUuid=d89a3ddf-2acf-4cc8-b11b-14f33b5c653e). The GRC Power Plant community provides technical information and articles about OpenPages GRC Platform.

Accessing the OpenPages GRC Platform application using SSL

You can access the IBM OpenPages GRC Platform application using a secure SSL connection. This procedure assumes that the default settings were not changed during installation.

Note: You must have an SSL digital certificate to use SSL with the OpenPages application.

Procedure

Open a browser window, and enter the following URL:

```
https://<server_name>:<ssl_port>/openpages
```

Where <server_name> is the name of the server machine hosting the OpenPages GRC Platform application, and <ssl_port> is the SSL port number that is associated with the application server.

For example:

```
https://server01.com:10111/openpages
```

Verifying WebSphere Application Server configuration for SSL

IBM WebSphere application server uses the concept of multiple transport channels to handle web traffic. Use the IBM WebSphere Integrated Solutions Console to make sure the Web Container Transport Chains are configured for SSL.

Procedure

1. Log on to cluster administrator server as a user with administrative privileges.
2. Go to the IBM WebSphere Integrated Solutions Console:

   For example, http://*<server_name>*:*<port>*/ibm/console .
3. Log on to the IBM WebSphere Integrated Solutions Console with an administrator account.
4. Expand the tree for **Servers | Server Types | WebSphere Application servers**.
5. In the **Application servers** list, click on the name of the server to be configured.
6. Under **Container Settings**, click **Web Container Settings | Web Container Transport Chains.**

7. For the **WCInboundDefaultSecure** chain, ensure that the **Enabled** field is set to **Enabled** and the **SSL Enabled** field is set to **Enabled**.

   If the fields are not set, click the **WCInboundDefaultSecure** resource and on the **General Properties** tab, and select **Enable** to enable the resource.
8. Click **Save** to save your changes.

Verifying SSL ports on virtual hosts

The IBM OpenPages GRC Platform Installer added the OpenPages SSL ports to the list of host aliases in the IBM WebSphere Integrated Solutions Console. You must verify that all ports for each OpenPages node pairing are added.

Procedure

1. Log on to the cluster administration server.
2. In the IBM WebSphere Integrated Solutions Console, expand the tree for **Environment | Virtual Hosts**.
3. Select **default_host**.
4. On the **Host Aliases** page, check that the SSL ports are added by the OpenPages GRC Platform Installer.

   For example, if the OpenPages application SSL ports are not listed, add port 10111 for the OpenPages application.

   Note: The OpenPages default port is 9060.
5. If any SSL ports are missing, click **New**.
6. On the **Configuration** page, enter the port number in the **Port** field. Optionally, enter a name in the **Host Name** field.
7. Click **OK**.
8. On the **Host Aliases** page, click **Save**.

Verifying the SSL protocol before you deploy a new non-administrative server

Before you can deploy a new non-administrative application server to a horizontal cluster, you must ensure that the SSL protocol is set correctly. You must verify the SSL protocol for the OpenPages application server.

For example, if you are using either the TLSv1.1 or TLSv1.2 protocols, the deployment will fail.

After you complete the configuration, you can change the SSL protocol back to your original selection. But, you cannot use TLSv1.1 or TLSv1.2 during the deployment of the new server.

Procedure

1. Go to the IBM WebSphere Integrated Solutions Console for the OpenPages Deployment Manager server:

   For example, `http://<server_name>:<port>/ibm/console`

   Where <server_name> is the name of the application server and <port> is the WebSphere port that is assigned during the WebSphere installation. The default port value is 9060.
2. Log on to the IBM WebSphere Integrated Solutions Console with an administrator account.
3. Expand **Security**, and select **SSL certificate and key management**.
4. In the **Related Items** list, click **SSL configurations**.
5. Click **CellDefaultSSLSettings**.
6. In the **Additional Properties** list, click **Quality of protection (QoP) settings**.
7. In the **Protocol** box, ensure that you have an option other than **TLSv1.1** or **TLSv1.2** selected.

Attention: If **TLSv1.1** or **TLSv1.2** are selected, deploying a new non-administrative server to your environment will fail.

a) If either **TLSv1.1** or **TLSv1.2** are selected, change the value to **SSL_TLSv2**.

b) Click **Apply**, and then click **Save**.

c) In the main menu, expand **System administration**, and click **Nodes**.

d) Select the check box for ***<host>*-OPNode1**.

e) Click **Full Resynchronize**.

Creating the keystore in the IBM WebSphere Integrated Solutions Console

Use the IBM WebSphere Integrated Solutions Console to create the public and private key pairs and store both keys in a file that is called a keystore.

About this task

You must perform the following step to create the opkeystore.

Use the appropriate URL to log on to the cluster administrator server.

Logon URL to create the opkeystore

`http://<server_name>:<port>/ibm/console`.

Where `<server_name>` is the name of the application server and `<port>` is the WebSphere port that is assigned during the WebSphere installation. The default port value is 9060.

Procedure

1. Log on to the cluster administrator server by using the appropriate port value in the URL: `http://<server_name>:<port>/ibm/console`.
2. In the IBM WebSphere Integrated Solutions Console, expand the tree for **Security | SSL certificate and key management.**
3. On the **SSL certificate and key management** page, in the **Related Items** list, click **Key stores and certificates**.
4. On the **SSL Certificates and key management** page, click **New**.
5. On the **Key store and certificates** page, use the following table to select or enter the appropriate values:

Table 164: Keystore and certificates values for OpenPagesCell

Value	**OpenPagesCell values**
Name	Enter `opkeystore`
Management scope	Select **(cell):OpenPagesCell**
Path	Enter a path in *<OP_Home>* where the keystore is to be created. For example, `/opt/OpenPages/Keystore`
Password	Enter a password for the keystore, by default `Spassword`
Type	Select **JKS**

6. Click **Apply**.

Generating a Certificate Signing Request file the IBM WebSphere Integrated Solutions Console

If you require an authorized certificate from a third-party certificate authority, you can use the IBM WebSphere Integrated Solutions Console to generate the required certificate signing request.

Procedure

1. Log on to the cluster administrator server.
2. In the IBM WebSphere Integrated Solutions Console, open the **Key store and certificates** page.
3. Select the **opkeystore**.
4. In the **Additional Properties** list, click **Personal certificate requests** to create a certificate request. The list becomes active after clicking **Apply**.
5. On the **Personal certificates requests** page, click **New**.

   Enter the following values:

   - Name - Enter a name for the certificate request, such as `ServerCertificateRequest.csr`
   - Key label - Enter a label for the certificate, such as the server name.
   - Common name - Enter a name for the certificate and any other identifying information.

     Note: The common name is the fully qualified domain name.
6. Click **Apply** and **OK**.
7. Click **Save**.
8. Repeat steps 5 to 7 for each secondary application server.

Submitting a CSR for Certificate Authority approval in a WebSphere Application Server environment

The Certificate Signing Request file must be submitted to an appropriate Certification Authority (CA) for approval.

Procedure

1. In the IBM WebSphere Integrated Solutions Console, open the **SSL certificate and key management** page.
2. Select the Certificate Signing Request you created and click **Extract**.
3. Enter a name for the file where the extracted certificate request is to be placed.

   On UNIX, the file is created in *<OP_Home>*`/profiles/OpenPagesDmgr/etc/` unless you enter a specific path.

   On Windows, the file is create in *<OP_Home>*`\profiles\OpenPagesDmgr\etc\` unless you enter a specific path.
4. Follow the instructions to submit your Certificate Signing Request file to an appropriate Certification Authority.
5. Download the approved root and Certificate Authority certificates to a local directory.
6. Check that the certificates are named to distinguish the root from the Certificate Authority certificate.
7. Repeat steps 2 to 6 for each secondary application server.

Importing signed CA certificates in the IBM WebSphere Integrated Solutions Console

You must install a root certificate and a server certificate from a trusted third-party certificate authority on each application server. You might also need to install an intermediate certificate on each application server. You can use the IBM WebSphere Integrated Solutions Console to import these certificates on the cluster administrator server and all cluster member systems.

About this task

You must perform the following steps to import the OpenPagesCell keystore.

To import the OpenPagesCell keystore

In step 2, log on to the IBM WebSphere Integrated Solutions Console by using the following URL `http://<server_name>:<port>/ibm/console`.

Where *<server_name>* is the name of the application server and *<port>* is the WebSphere port assigned during the WebSphere installation. The default port value is 9060.

Procedure

1. Log on to each IBM OpenPages GRC Platform server as a user with administrative privilege.
2. Start a web browser and go to the IBM WebSphere Integrated Solutions Console.

   For example: `http://<server_name>:<port>/ibm/console`.
3. Log on to the IBM WebSphere Integrated Solutions Console with an administrator account.
4. Expand the tree for **Security | SSL certificate and key management.**
5. On the **SSL certificate and key management** page, in the **Related Items** list, click **Key stores and certificates.**
6. In the list of keystores and certificates, click the keystore you want to configure.
7. Under **Additional Properties**, select **Signer certificates**.
8. On the **Signer Certificate** page, click **Add**.
9. On the **General Properties** page, enter the following values:
   - **Alias**. Enter the name used to identify the Root CA certificate in the keystore.
   - **File name**. Enter the full path to the Root CA certificate.
   - **Data type**. Select **Base64-encoded ASCII data** from the list.
10. Click **Apply** and **OK**.
11. Click **Save**.
12. To import server certificates to the keystore, under **Additional Properties**, select **Personal Certificates**.
13. Click **[Receive Certificate from CA]**.
14. On the **General Properties** page, enter the following values:
    a) **File name**. Enter the full path to the server certificate.
    b) **Data type**. Select **Base64-encoded ASCII data** from the list.
15. Click **Apply** and **OK**.
16. Click **Save**.
17. Repeat steps 13 to 16 for each secondary application server.

Importing the Certificate Authority certificate for Java Runtime Environment

Use the Keytool command to import the Certificate Authority certificate into the Java JRE environment on the cluster administrator server and all cluster member systems.

Procedure

1. Log on to each IBM OpenPages GRC Platform server as a user with administrative privileges.
2. Start an AIX or Linux shell or Windows command prompt.
3. Go to the *<WebSphere_Home>*`|java|jre|lib|security` directory.
4. Type the following Keytool command to import the root certificate.

```
keytool -import -alias certificate_name -trustcacerts -file
     file_name -keystore keystore_name
```

For example, the following Keytool command imports the `rootca` certificate into the `trustedcafilename.cer` file:

```
keytool -import -alias rootca -trustcacerts -file trustedcafilename.cer
     -keystore cacerts
```

5. Enter the password for the certificate.

   The default password is `changeit`.
6. Enter `Yes` to trust the certificate.

What to do next

If you are using self-signed certificates for OpenPages and Cognos that are not issued by a known CA, you must import the self-signed root certificate from any Cognos server connected to the current OpenPages server. Use the following Java keytool command to import the certificates into the *<OP_Home>*|`jre`|`lib`|`security` directory.

`keytool -import -alias` *`certificate_name`* `-trustcacerts -file` *`file_name`* `-keystore` *`keystore_name`*

Installing certificate authority certificates

After you configure the web server for SSL, you must configure any web browsers that access the web server. You must import the root certificate into the browser keystore on the cluster administrator, on all cluster member systems, and on client systems that access IBM OpenPages GRC Platform.

About this task

The following steps provide an example for configuring a Microsoft Internet Explorer web browser.

Procedure

1. On any system that accesses the OpenPages environment, open a web browser.
2. Click **Tools**, then **Internet Options**.
3. Click the **Content** tab, and then click **Certificates**.
4. To start the **Certificate Import Wizard**, click the **Trusted Root Certification Authority** tab, and then click **Import**.
5. On the **Certificate Import Wizard Welcome** page, click **Next**.
6. On the File to Import page, enter the path to the root certificate. For example, `C:\`*`OP_Home`*`\profiles\OpenPagesDmgr\etc\root-certificate.cer`.
7. On the **Certificates Store** page, select **Place all certificates in the following store**. Ensure that **Trusted Root Certification Authorities** is selected.
8. On the **Completing the Certificate Import Wizard** page, review the settings, and click **Finish**.
9. If you are required to install an authenticated certification authority certificate, follow these steps:
   a) Click the Intermediate **Certification Authority** tab.
   b) Click **Import to start the Certification Import Wizard**.
   c) Repeat steps 5 - 8 to ensure that **Intermediate Certification Authorities** is selected on the **Certificate Store** page.
10. After you receive the certification authority certificate, follow these steps:
    a) Click the **Trusted Publishers** tab.
    b) To start the **Certification Import Wizard**, click **Import**.
    c) Repeat steps 5 - 8 to ensure that **Trusted Publishers** is selected on the **Certificate Store** page.

Updating properties files so web browsers use HTTPS protocol and SSL ports

After you configure the web server for SSL, edit the properties files to ensure web browsers use HTTPS protocol and SSL ports on the cluster administrator server and all cluster member systems.

About this task

In a load balanced environment, the values are the fully qualified domain name of the load balancer and port.

Procedure

1. Log on to each IBM OpenPages GRC Platform server as a user with administrative privileges.
2. Open a command prompt window by using the **Run as Administrator** option.
3. Go to the *<OP_Home>*\aurora\conf directory.
4. Open the aurora.properties properties file in a text editor.
   a) Edit the following lines to change http to https and update the port number.

   ```
   application.url.path=http\://<server_name>\:<port>/openpages
   cognos.server=http\://<server_name>\:<port>/ibmcognos/cgi-bin/cognos.cgi
   ```

   logout.url.cognos=http\://*<server_name>*\:*<port>*/ibmcognos/cgi-bin cognos.cgi?b_action\=xts.run&m\=portal/logoff.xts&h_CAM_action\=logoff

   For example, in a load balanced environment, the application.url.path value is the fully qualified domain name of the load balancer and port.
   b) Save and close the file.
5. Open each *server_name*-OPNode1Server#-sosa.properties file in a text editor.
   a) Edit the following lines to change http to https and update the port number.

   ```
   application.url.path= http://<server>:\<port>/openpages
   ```

   Note: In a load-balanced environment, this value is the fully qualified domain name of the load balancer and port.
   b) Save and close the file.
6. Open each *server_name*-OPNode#Server#-server.properties in a text editor.
   a) Edit the following lines to change the http to https and update the port number.

   ```
   url.path.openpages=http\://<server>:<port>/openpages
   webclient.http.server.protocol=http
   webclient.http.server.port=<port>
   ```

   b) Save and close the file.

Configuring SSL by using IBM Console web application

The WebSphere Application Server must be configured to use the opkeystore.jks keystore. You can use the IBM Console Web Application to configure WebSphere application server to use only the opkeystore.jks keystore.

About this task

You must perform the following steps to configure the opkeystore. Use the appropriate logon URL when you perform the steps.

Logon URL to configure the opkeystore

http://*<server_name>*:*<port>*/ibm/console.

Where <server_name> is the name of the application server and <port> is the WebSphere port that is assigned during the WebSphere installation. The default port value is 9060.

Procedure

1. Log on to the cluster administration server as a user with administrative privileges.
2. In the IBM WebSphere Integrated Solutions Console, click **Security** > **SSL certificate and key management**.
3. On the **SSL certificate and key management** page, in the **Related Items** list, click **SSL Configurations**.
4. On the **SSL Configurations** page, click **CellDefaultSSLSettings**.
5. On the **General Properties** page, use the following table to set the appropriate values:

*Table 165: **CellDefaultSSLSettings** keystore property values*	
Setting	**opkeystore value**
Truststore name	**opkeystore**
Keystore name	**opkeystore**
Management scope	`(cell):OpenPagesCell`

6. Click **Get certificate aliases**.
7. Click **Apply**.
8. On the **SSL configurations** page, click **NodeDefaultSSLSettings**.
9. On the **General Properties** page, use the following table to set the appropriate values:

*Table 166: **NodeDefaultSSLSettings** keystore properties values*	
Setting	**opkeystore value**
Truststore name	**opkeystore**
Keystore name	**opkeystore**

10. Click **Get certificate aliases**.
11. Click **Apply**.
12. Repeat steps 8 to 11 for each node.

Enabling secure session cookies on IBM WebSphere Application Server

Enable or disable the Restrict cookies to HTTPS sessions setting on all application servers in your environment.

A secure session cookie informs the browser to only send the session cookie back over an encrypted HTTP connection. This ensures that the cookie identifier is secure and is only used with IBM OpenPages GRC Platform when using HTTPS connections. When this feature is enabled, session cookies over an HTTP connection no longer work.

Procedure

1. Open a browser window and log on to the IBM WebSphere Integrated Solutions Console as a server administrator.

   The default URL is `http://<server_name>:<port>/ibm/console`.
2. In the Integrated Solutions Console:
   a) Expand **Servers | Server Types**
   b) Click the **WebSphere Application Server** 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. On the **Configuration** tab, under the **Container Settings** heading, click **Session Management**.
6. On the **Application servers | OpenPages-server-name | Session Management** page:
   a) Verify that **Enable cookies** setting is selected.
   b) On the **Application servers | OpenPages-server-name | Session Management Cookies** page, configure the **Restrict cookies to HTTPS sessions**.
      - To enable secure session cookies, select the Restrict cookies to HTTPS sessions check box.
      - To disable secure session cookies, clear the Restrict cookies to HTTPS sessions check box.
   c) When finished, click **Apply**.
7. Repeat steps 3-7 for all available application servers.

Updating the SSL socket factory providers

Cognos Analytics and IBM OpenPages GRC Platform can be installed on the same application server. If so, and if Cognos Analytics uses WebSphere Java, then in an SSL environment you must update the SSL socket factory providers in the `java.security` file. If you do not update the `java.security` file, you get a `ClassNotFoundException` error message.

Procedure

1. Log on to each IBM OpenPages GRC Platform server as a user with administrative privileges.
2. Open the *<WebSphere_Java_Home>*`/jre/lib/security/java.security` file in a text editor.
3. Locate ssl.SocketFactory.provider and ssl.ServerSocketFactory.provider properties.
4. Comment out WebSphere socket factories, and uncomment the default JSSE socket factories as follows:

```
# Default JSSE socket factories
ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl
ssl.ServerSocketFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
# WebSphere socket factories (in cryptosf.jar)
#ssl.SocketFactory.provider=com.ibm.websphere.ssl.protocol.SSLSocketFactory
#ssl.ServerSocketFactory.provider=com.ibm.websphere.ssl.protocol.SSLServerSocketFa
ctory
```

5. Save the file.
6. Restart the OpenPages and Cognos servers.

SSL configuration for Microsoft Internet Information Services

In most environments, traffic to and from Cognos Analytics passes through a web server. You can configure the Microsoft Internet Information Services web server for SSL. Microsoft Internet Information Services requires a certificates snap-in.

Procedure

1. Log on to each Cognos Analytics server as a user with administrative privileges.
2. Start the Microsoft Management Console.
   a) Click the Windows **Start** menu.
   b) Type `mmc` in the **Search Programs and Files** field and press **Enter**.
3. In the **MMC** dialog box, click **File** > **Add/Remove Snap-Ins.**
4. In the **Available snap-ins** list, double-click **Certificates**.
5. In the **Certificates Snap-ins** dialog box, select **Computer account**, and then click **Next**.
6. In the **Select Computer** dialog box, select **Local Computer**, and then click **Finish**.
7. Click **OK** to close the dialog box.

Generating a key pair and request using Microsoft Internet Information Services

Use the reporting server to generate the key pair and specify the keystore in Microsoft Internet Information Services

Procedure

1. Log on to the primary reporting server as a user with administrative privileges.
2. In the Microsoft Management Console dialog box on the reporting server, expand the **Certificates** and select **Personal**.
3. In the **Actions** panel, right-click the **Certificates** icon and select **All Tasks** > **Advanced Options** > **Create Custom Request**.
4. In the **Certificate Enrollment** dialog box, click **Next**.
5. On the **Select Certificate Enrollment Policy** pane, select **Proceed without enrollment policy**, and click **Next**
6. On the **Custom request** pane, accept the default values of **CNG key** and **PKCS#10**, and click **Next**.
7. In the **Certificate Information** pane, click the **Details** icon, and click **Properties**.
8. In the **Certificate Properties** dialog box, click the **Subject** tab to supply details for the certificate's Distinguished Name.
9. To specify at a common name and organization value.
   a) In the **Type** list, select **Common Name**, and enter a value for the certificate common name, and click **Add**.
   b) Select **Organization** in the **Type** list and enter a value for the certificate common name, and click **Add**.
10. Click the **Private Key** tab and then:
    a) Click the arrow next to **Key Options**, and select **Make private key exportable**.
    b) Click the arrow next to **Select Hash Algorithm**, select **sha1** from the **Hash Algorithm** list, and click **OK**.
11. In the **Certificate Information** pane, click **Next**.
12. In the **Certificate Enrollment** pane:
    a) Click **Browse** and in the **Save as** dialog box, enter a name for the certificate request file in the **File name** field. Use a `.csr` extension.
    b) From the **Save as type** list, select **All Files**, and then click **Save**.
13. Click **Finish**.
14. Close the Microsoft Management Console.

Submitting a Certificate Signing Request for your web server

Submit the Certificate Signing Request to a Certificate Authority for approval.

Procedure

1. Download the approved root and server certificates to a local directory, such as the `OpenPagesDomain` directory.
2. Check that the certificates are named to distinguish the root from the server certificate.
3. Follow the instructions provided by the Certificate Authority.

Importing the root certificate into Microsoft Internet Information Services

You must import the root certificate into Microsoft Internet Information Services on the primary Cognos system and all secondary Cognos systems.

Procedure

1. Log on to each Cognos server as a user with administrative privileges.
2. Start the Microsoft Management Console (MMC).

a) Click the Windows **Start** menu.

b) Type `mmc` in the **Search Programs and Files** field and press **Enter**.

3. In the **MMC** dialog box, click **File** > **Add/Remove Snap-Ins**.
4. In the **Available snap-ins** list, double-click **Certificates**.
5. In the **Certificates Snap-ins** dialog box, select **Computer account**, and click **Next**.
6. In the **Select Computer** dialog box, select **Local Computer**, and click **Finish**.
7. In the **MMC** dialog box, expand **Certificates** and select **Trusted Root Certification Authorities**.
8. In the **Actions** panel, right-click the **Certificates** icon and select **All Tasks** > **Import**.
9. In the Certificate Import wizard, click **Next**.
10. On the **File to Import** pane, click **Browse** to locate the CA certificate, and then click **Next**.
11. On the **Certificate Store** pane, select **Place all certificates in the following store** > **Trusted Root Certification Authorities**, and click **Next**.
12. On the **Completing the Certificate Import** wizard screen, click **Finish**.
13. Repeat these steps to import any intermediate certificates required by your Certificate Authority.

What to do next

If you are using self-signed certificates for OpenPages GRC Platform and Cognos, that are not issued by a known Certificate Authority, you must import the OpenPages GRC Platform signed root certificate from any OpenPages server connected to the current Cognos server. Use the following Java keytool command to import the certificates into the *<Cognos_Home>*`\analytics\jre\8.0\lib\security` directory.

```
keytool -import -alias certificate_name -trustcacerts -file file_name
     -keystore keystore_name
```

Adding the SSL binding for Microsoft Internet Information Services

To bind the root certificate to the web server use Cognos on the primary Cognos system and all secondary Cognos systems.

Procedure

1. On the Cognos server, open the Windows Internet Information Services Manager, by clicking the **Start** menu, then selecting **Administrative Tools** > **Internet Information Services Manager**.
2. Expand the folder structure for the server you want to configure and select **Sites**.
3. In the **Sites** pane, select the website to configure.
4. In the **Action** panel, select **Bindings**.
5. In the **Site Bindings** dialog box, select **HTTPS** and click **Edit**.

SSL configuration for Apache Web Server

To use SSL between IBM OpenPages GRC Platform applications and Apache Web Server, some configuration is required. For example, you must generate a keystore and a keypair, generate a certificate signing request, and establish the root of trust.

Generating a key pair and request using Cognos

Use Cognos to generate the key pair and specify the keystore for Apache web server on the primary Cognos system.

Procedure

1. Log on to the reporting server as a user with administrative privileges.

   Note: For AIX and Linux installs, log in as a non-root user, such as the opuser user that you created for the IBM OpenPages GRC Platform installation.
2. Open an AIX or Linux shell, or Windows command prompt.

3. Go to the `bin` directory in the web server home directory.
4. Enter the following commands to generate a certificate request:

   Windows:

   ```
   openssl req -new -sha1 -newkey rsa:1024 -config %APACHE_HOME%\conf\
   openssl.cnf -nodes -keyout server_pkey.key
   -out certreq.csr
   ```

   AIX and Linux:

   ```
   openssl req -new -sha1 -newkey rsa:1024 -config $APACHE_HOME/conf/
   openssl.cnf -nodes -keyout server_pkey.key
   -out certreq.csr
   ```
5. Open the `httpd.conf` file using a text editor.
   a) Uncomment the following line.

   ```
   LoadModule ssl_module modules/mod_ssl.so
    Secure (SSL/TLS) connections
    Include conf/extra/httpd-ssl.conf
   ```
6. Save and close the file.

Submitting a Certificate Signing Request for your web server
Submit the Certificate Signing Request to a Certificate Authority for approval.

Procedure

1. Download the approved root and server certificates to a local directory, such as the `OpenPagesDomain` directory.
2. Check that the certificates are named to distinguish the root from the server certificate.
3. Follow the instructions provided by the Certificate Authority.

Importing the root certificate into Apache web server
You must import the root certificate into Apache web server on the primary Cognos system and all secondary Cognos systems.

Procedure

1. Log on to the reporting server as a user with administrative privileges.

   Note: Log on as a non-root user, such as the `opuser` user you created for the IBM OpenPages GRC Platform installation.
2. Go to the *<Apache_Home>*`/conf/extra` directory.
3. Open the `httpd-ssl.conf` file in a text editor.
4. Under **Server Certificate**, uncomment the SSLCertificateFile parameter, and enter the path to the PEM encoded certificate.
5. Under **Server Private Key**, uncomment the SSLCertificateKeyFile parameter, and enter the path to the keyfile on this server.
6. Under **Certificate Authority (CA)**, uncomment the SSLCACertificateFile parameter, and enter the path to the root certificate.
7. Save and close the file.

What to do next

If you are using self-signed certificates for OpenPages and Cognos that are not issued by a known Certificate Authority, you must import the OpenPages self-signed root certificate from any OpenPages

server connected to the current Cognos server. Use the Java `keytool` command to import the certificates into the following directories.

```
<Cognos_Home>\analytics\jre\8.0\lib\security
      keytool
       -import -alias certificate_name -trustcacerts -file file_name
       -keystore keystore_name
```

Importing the server certificate into Apache web server
You must import the server certificate from the Certificate Authority into Apache web server on the primary Cognos system and all secondary Cognos systems.

Procedure

1. Log on to the reporting server as a user with administrative privileges.

   Note: Log on as a non-root user, such as the opuser user you created for the IBM OpenPages GRC Platform installation.
2. Go to the *<Apache_Home>*`/conf/extra` directory.
3. Open the `httpd-ssl.conf` file in a text editor.
4. Under **Server Certificate**, uncomment the SSLCertificateFile parameter, and enter the path to the PEM encoded certificate.
5. Under **Server Private Key**, uncomment the SSLCertificateKeyFile parameter, and enter the path to the keyfile on this server.
6. Under **Certificate Authority (CA)**, uncomment the SSLCACertificateFile parameter, and enter the path to the root certificate.

Configuring SSL in the OpenPages GRC Platform properties files

If IBM OpenPages GRC Platform is configured for SSL, you must configure the properties file to use the OpenPages GRC Platform HTTPS address and SSL port. Modify the OpenPages GRC Platform properties file, to use HTTPS and the SSL port, on the primary Cognos system and secondary Cognos systems.

Procedure

1. Log on to the Cognos server as a user with administrative privileges.

   Note: For AIX and Linux, you log on as a non-root user, such as the opuser user you created for the OpenPages GRC Platform installation.
2. On Windows computers, start a Command Prompt using the Run as Administrator option, or on a AIX or Linux computer open an AIX or Linux shell.
3. Go to the following directory.
   - Windows: *<Cognos_Home>*`\configuration`
   - AIX and Linux:*<Cognos_Home>*`/configuration`
4. Open the `OpenPagesSecurityProvider_OpenPagesSecurityRealm.properties` in a text editor.
5. Edit the openpages.application.url value, replacing `http` with `https` and changing the *<port>* to the SSL port.

SSL configuration on AIX and Linux load balancer server

To use SSL on an AIX-based and Linux-based load-balancing server running IBM HTTP Server (IHS) in IBM OpenPages GRC Platform, some configuration is required. For example, you must generate a keystore and a keypair, and generate a certificate signing request, and establish the root of trust.

Generating a keystore and key pair using the iKeyman tool

If you are using IBM HTTP Server as your web server, generate a key pair using the iKeyman tool on the load balance server.

Procedure

1. Log on to the load balance server as a user with administrative privileges.
2. Start iKeyman by running the following command:

   IHS_root/bin/ikeyman

   Where *IHS_root* is the location of the IHS.

   The default location is *IHS_root* is /usr/IBM/HTTPServer/.
3. Create the keystore file to store the key pair.
   a) Select **Key Database File** > **New**.
   b) In the dialog box that displays, select **CMS** from the **Key database type** list.
   c) In the **File Name** field, enter a file name for the new key database file.
   d) In the **Location** field, enter the location where you want to store the keystore file, and click **OK**

      For example: usr/IBM/HTTPServer/bin.
   e) In the **Password Prompt** dialog box that displays, enter a password for the keystore. Re-enter the password.
   f) In iKeyman, select **Stash password to file** to create a .sth file. This file encrypts and stores the keystore password which is assigned an expiration time. You must change the password periodically.
   g) Click **OK**.

Generating a certificate signing request file using the iKeyman tool

If you require an authorized certificate from a trusted third-party certificate authority, you can use the iKeyman tool to generate the required certificate signing request.

Procedure

1. Log on to the load balance server as a user with administrative privileges.
2. Start iKeyman by running the following command: *IHS_root*/bin/ikeyman

   Where *IHS_root* is the location of the IBM HTTP Server installation. The default location is /usr/IBM/HTTPServer/.
3. In the iKeyman tool, open the keystore created in Step 2.
   a) Select **Key Database File** > **Open**.
   b) Specify the type of keystore. The default type is **CMS**.
   c) In the **File Name** and **Location** fields, enter the name and path to the keystore. You can also click **Browse** to locate the keystore, and click **OK**.
   d) In the **Password Prompt** dialog box, enter the password for the keystore, and click **OK**.
4. Generate the certificate request for the open keystore.
   a) Select **Create** > **New Certificate Request**.
   b) In the **Create New Key and Certificate Request** dialog box, in the **Key Label** field, provide an identifier for the certificate.

c) In the **Key Size** list, select a key length for the certificate. The key size determines the strength of the encryption.

d) From the **Signature Algorithm** list, select an algorithm to apply to the certificate.

e) Provide the dname information to identify the certificate. Enter the values as appropriate.
`commonName`
`organization`
`organizationUnit`
`localityName`
`stateName`
`country`

f) Click **OK** to generate the request. A certificate request in the `.arm` format is created and saved to the specified location.

Submitting a Certificate Signing Request to a Certificate Authority running IBM HTTP
To submit the Certificate Signing Request, follow the instructions that are provided by the Certificate Authority. Depending on the instructions, you need to either copy and paste the content of the CSR to the text area or attach the CSR file.

Importing the Root and Signed Server Certificates using the iKeyman tool
You must install a signed certificate from a third-party certificate authority or self-signed certificates in both the keystore created and the keystore used by IBM HTTP Server. You must install a server certificate into the keystore created.

Procedure

1. Log on to the load balance server as a user with administrative privileges.
2. Start iKeyman by running the following command: *IHS_root*`/bin/ikeyman`

   Where *IHS_root* is the location of the IHS. The default location is`/usr/IBM/HTTPServer/`.
3. In the iKeyman tool, open the keystore you created in Step 2.
   a) Select **Key Database File** > **Open**.
   b) Specify the type of keystore, by default **CMS**.
   c) In the **File Name** and **Location** fields, enter the name and path to the keystore.
   d) In the **Password Prompt** dialog box, enter the password for the keystore.
4. Import the signed CA certificate.
   a) In the **Key database content** list, select **Signer Certificates**, and click **Add**.
   b) In the **Open** window, in the **File Name** and **Location** fields, enter the name and path to the keystore.
   c) In the **Enter a Label** dialog box that displays, in the **Enter a label for the certificate** field, enter a name for the certificate.
5. Select **Key Database File** > **Close**.
6. In the iKeyman tool, open the `plugin-key.kdb` keystore.
   a) Select **Key Database File** > **Open**.
   b) Specify the type of keystore. The default type is `CMS`.
   c) In the **File Name** and **Location** fields, enter the name and path to the keystore.

      The default directory for the `plugin-key.kdb` keystore is `<IHS root>/Plugins/config/`*server_name*`/plugin-key.kdb`, and click **OK**.
   d) In the `Password Prompt` dialog box, enter the password for the keystore. The default password is **WebAS**, and click **OK**.
7. Select **Signer Certificates** in the **Key database content** list, and click **Add**.
8. In the **Add CA's Certificate from a file** window, enter the following information.

9. In the **Data type** list, select `Base64-encoded ASCII data`.
10. In the **File Name** and **Location** fields, enter the name and path to the keystore.
11. In the **Enter a Label** dialog box and the **Enter a label for the certificate** field, enter a name for the certificate.

Editing the Apache configuration file on IBM HTTP server
You must edit the `httpd.conf` file on the load balancer server for the IBM HTTP server.

Procedure

1. On Windows computers, start a Command Prompt window by using the **Run as Administrator** option, or on AIX or Linux computers, open an AIX or Linux shell.
2. Go to the *IHS root*`/conf` directory.
3. Open the `httpd.conf` file using a text editor.
   a) Uncomment the following in the file.

   ```
   LoadModule was_app22_module modules/mod_was_ap22_http.so
   LoadModule negotiation_module module8s/mod_negotiation.so
   ```

   b) Uncomment the following lines in the file and add any missing lines.

   ```
   Listen 443
   <VirtualHost *:443>
   ServerName <server_name>
   SSLEnable
   SSLProtocolDisable SSLv2
   SSLClientAuth None
   <Directory />
   Options FollowSymLinks
   AllowOverride None
   Order allow,deny
   Allow from all
   </Directory>
   </VirtualHost>
   SSLDisable
   KeyFile <IHS_root>/<keystore_name>.kdb
   ```

   c) Add the following line to point to the WebSphere plug-in Configuration.

   ```
   WebSpherePluginConfig
   <IHS root>/Plugins/config/<server_name>/plugin-cfg.xml
   ```

   d) Save and close the file.
4. To apply the changes, restart the IBM HTTP Server.

SSL configuration for an Apache load balancer server in Windows environments

There are four procedures for the web server on any reporting server that handles external IBM OpenPages GRC Platform CommandCenter requests.

Generating a key pair and request with an Apache load balancer server
If you are using Apache as your load balancer server, you must generate a key pair and specify the keystore.

Procedure

1. Log on to the load-balancing server as a non-root user with administrative privileges.
2. Start a Command Prompt window by using the **Run as Administrator** option.
3. Go to the `\bin` directory in the web server home directory to use as the keystore.
4. To generate a certificate request, enter the following command :

- For Windows operating systems or computers:

  ```
  openssl req -new -sha1 -newkey rsa:1024 -config %APACHE_HOME%\conf
  \openssl.cnf
  -nodes -keyout server_pkey.key -out certreq.csr
  ```

- For AIX and Linux operating systems or computers:

  ```
  openssl req -new -sha1 -newkey rsa:1024 -config $APACHE_HOME\conf
  \openssl.cnf
  -nodes -keyout server_pkey.key -out certreq.csr
  ```

5. Open the `httpd.conf` file in a text editor and uncomment following line:

   ```
   LoadModule ssl_module modules/mod_ssl.so
   Secure (SSL/TLS) connections
   Include conf/extra/httpd-ssl.conf
   ```

   a)

Submitting a Certificate Signing Request to a Certificate Authority for an Apache load balancer server

Submit the Certificate Signing Request file for an Apache load balancer server to an appropriate Certification Authority (CA) for approval.

Procedure

1. Download the approved root and server certificates to a local directory, such as the `OpenPagesDomain` directory.
2. Check that the certificates are named to distinguish the root from the server certificate.
3. Follow the instructions provided by the Certificate Authority.

Importing the root certificates for an Apache load balancer server

You must import the root certificates into an Apache load balancer server.

Procedure

1. Log on to the load-balancing server as a non-root user with administrative privileges.
2. Start a Command Prompt window by using the Run as Administrator option.
3. Go to the *<Apache_Home>*`/conf/extra` directory.
4. Open the `httpd-ssl.conf` file in a text editor.
5. Under **Server Certificate**, uncomment the SSLCertificateFile parameter, and enter the path to the PEM encoded certificate.
6. Under **Server Private Key**, uncomment the SSLCertificateKeyFile parameter, and enter the path to the key file on this server.
7. Under **Certificate Authority (CA)**, uncomment the SSLCACertificateFile parameter, and enter the path to the root certificate.
8. Save and close the file.

Editing the Apache configuration file on Apache load balancer server

To add SSL parameters for the Apache load balancer server, you must edit the `httpd.conf` file.

Procedure

1. Log on to load-balancing web server as a user with administrative privileges.
2. Stop the Apache web Server.
3. Start a Command Prompt window by using the **Run as Administrator** option.
4. Copy the *WL_Home*`\server\plugin\win\32\mod_wl_22.so` file to the *Apache_Home*`\modules` directory.

Copy `C:\Oracle\Middleware\wlserver_10.3\server\plugin\win\32\mod_wl_22.so` to `C:\Program Files\Apache Software Foundation\Apache2.2\conf`

5. Go to the *Apache_Home*`\conf\` directory.
6. Open the `httpd.conf` file and locate the parameters added to the end of the file for SSL. See the following example of these parameters.
   a) Before the first <Location /> parameter, add the following parameter.

   ```
   <IfModule ssl_module>
   SSLRandomSeed startup builtin
   SSLRandomSeed connect builtin
   </IfModule>
   ```

   b) In the <Location /> parameter, add the location of the trusted CA certificate file.

SSL configuration for IBM HTTP server

If you use IBM HTTP Server (IHS) as a web server for Cognos, some configuration is required. For example, you must generate a keystore and key pair, and generate a certificate signing request, and submit a Certificate Signing Request (CSR).

Generating a keystore and key pair using the iKeyman tool

If you are using IBM HTTP Server as your web server, generate a key pair using the iKeyman tool on the reporting server.

Procedure

1. Log on to the reporting server as a user with administrative privileges.
2. Start iKeyman by running the following command:

   IHS_root`/bin/ikeyman`

   Where *IHS_root* is the location of the IHS.

   The default location is *IHS_root* is `/usr/IBM/HTTPServer/`.
3. Create the keystore file to store the key pair.
   a) Select **Key Database File** > **New**.
   b) In the dialog box that displays, select **CMS** from the **Key database type** list.
   c) In the **File Name** field, enter a file name for the new key database file.
   d) In the **Location** field, enter the location where you want to store the keystore file, and click **OK**

      For example: `usr/IBM/HTTPServer/bin`.
   e) In the **Password Prompt** dialog box that displays, enter a password for the keystore. Re-enter the password.
   f) In iKeyman, select **Stash password to file** to create a `.sth` file. This file encrypts and stores the keystore password which is assigned an expiration time. You must change the password periodically.
   g) Click **OK**.

Generating a certificate signing request file using the iKeyman tool

If you require an authorized certificate from a trusted third-party certificate authority, you can use the iKeyman tool to generate the required Certificate Signing Request.

Procedure

1. Log on to the reporting server as a user with administrative privileges.
2. Start iKeyman by running the following command: *IHS_root*`/bin/ikeyman`

   Where *IHS_root* is the location of the IBM HTTP Server installation. The default location is `/usr/IBM/HTTPServer/`.

3. In the iKeyman tool, open the keystore created in Step 2.
   a) Select **Key Database File** > **Open**.
   b) Specify the type of keystore. The default type is **CMS**.
   c) In the **File Name** and **Location** fields, enter the name and path to the keystore. You can also click **Browse** to locate the keystore, and click **OK**.
   d) In the **Password Prompt** dialog box, enter the password for the keystore, and click **OK**.
4. Generate the certificate request for the open keystore.
   a) Select **Create** > **New Certificate Request**.
   b) In the **Create New Key and Certificate Request** dialog box, in the **Key Label** field, provide an identifier for the certificate.
   c) In the **Key Size** list, select a key length for the certificate. The key size determines the strength of the encryption.
   d) From the **Signature Algorithm** list, select an algorithm to apply to the certificate.
   e) Provide the `dname` information to identify the certificate. Enter the values as appropriate.
   `commonName`
   `organization`
   `organizationUnit`
   `localityName`
   `stateName`
   `country`
   f) Click **OK** to generate the request. A certificate request in the `.arm` format is created and saved to the specified location.

Submitting a Certificate Signing Request to a Certificate Authority
To submit the Certificate Signing Request, follow the instructions that are provided by the Certificate Authority. Depending on the instructions, you need to either copy and paste the content of the CSR to the text area or attach the CSR file.

Downloading and importing the root and signed server certificates using the iKeyman tool
You must install a signed certificate from a third-party Certificate Authority or self-signed certificates in both the keystore created and the keystore used by IBM HTTP Server. You must install a server certificate into the keystore created.

Procedure

1. Follow the instructions provided by the Certificate Authority to download the root and signed server certificates.
2. Download the approved root and Certificate Authority certificates to a local directory.
3. Check that the certificates are named to distinguish the root from the Certificate Authority certificate.
4. Log on to the reporting server as a user with administrative privileges.
5. Start iKeyman by running the following command: *IHS_root*`/bin/ikeyman`

   Where *IHS_root* is the location of the IHS. The default location is`/usr/IBM/HTTPServer/`.
6. In the iKeyman tool, open the keystore you created for Cognos.
   a) Select **Key Database File** > **Open**.
   b) Specify the type of keystore, by default **CMS**.
   c) In the **File Name** and **Location** fields, enter the name and path to the keystore.
   d) In the **Password Prompt** dialog box, enter the password for the keystore.
7. Import the root certificate.
   a) In the **Key database content** list, select **Signer Certificates**, and click **Add**.
   b) In the **Open** window, in the **File Name** and **Location** fields, enter the name and path to the root certificate file.

c) In the **Enter a Label** dialog box that displays, in the **Enter a label for the certificate** field, enter a name for the root certificate.

8. Import CA signed certificate.
   a) In the **Key database content** list, select **Personal Certificates**, and click **Receive**.
   b) In the **Open** window, in the **File Name** and **Location** fields, enter the name and path to the CA signed certificate file.
   c) In the **Enter a Label** dialog box that displays, in the **Enter a label for the certificate** field, enter a name for the CA signed certificate.

Updating the Apache configuration file on IBM HTTP server
You must update the `httpd.conf` file and restart the server.

Procedure

1. On Windows computers, start a Command Prompt window by using the Run as Administrator option, or on AIX® or Linux computers, open an AIX or Linux shell.
2. Go to the *IHS root*`/conf` directory.
3. Open the `httpd.conf` file using a text editor.
   a) Uncomment the following in the file.

```
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
Listen 443
<VirtualHost *:443>
SSLEnable
</VirtualHost>
KeyFile /home/opuser/IBM/HTTPServer/<yourkeystore.kdb>
SSLDisable
```

   b) Save and close the file.

   Note: You must also replace *<yourkeystore.kdb>* with your keystore file and replace port 443 with your SSL port for IBM HTTP Server.
4. To apply the changes, restart the IBM HTTP Server.

Importing root and signer certificates to the local trust store

You must install a root certificate and a signed server certificate from a trusted third-party certificate authority on each application server. The signer might need to be added to the local trust store. You can use the **Retrieve from port** option in the IBM WebSphere administrative console to retrieve the certificate and resolve the problem. Complete this task if you determine that the request is trusted.

Before you begin

- Determine the host name and port of the target secure server. The target secure server is the server that OpenPages GRC Platform connects to in order to retrieve the certificates.
- The target secure server application from which you are going to retrieve the certificate must be running and listening on the port.

About this task

The root certificate contains the public key and has been verified by the certificate authority (CA). Your web server sends the root certificate to browsers trying to access that web server.

The server certificate is returned from the CA and is based on the certificate request that you generated.

Import the certificates on the administrative application server and on all non-administrative application servers.

Procedure

1. Log on to the IBM WebSphere administrative console.
2. Expand **Security** and click **SSL certificate and key management**.
3. Under **Configuration settings**, click **Manage endpoint security configurations**.
4. Select the appropriate outbound configuration to get to the **(cell):OpenPagesCell** management scope.
5. Under **Related Items**, click **Key stores and certificates** and click the **CellDefaultTrustStore** keystore.
6. Under **Additional Properties**, click **Signer certificates** and **Retrieve From Port**.
7. Enter the host and port information.
   - **Host**: Enter the host name of the secure target server.
   - **Port**: Enter the port number of the secure target server application.
   - **Alias**: Enter a descriptive name for the certificate.
8. Click **Retrieve Signer Information**.
9. Verify that the certificate information is for a certificate that you trust.
10. Click **Apply** and then click **Save**.
11. Synchronize the OpenPages nodes.
    - On Microsoft Windows operating systems, go to the *<OP_HOME>*\profiles*<host_name>*-OPNode1\bin directory and run syncNode.bat *<admin_host_name> <OP_SOAP_port>*.
    - On UNIX operating systems, go to the *<OP_HOME>*/profiles/*<host_name>*-OPNode1/bin directory and run syncNode.sh *<admin_host_name> <OP_SOAP_port>*.

    If WebSphere Application Server security is enabled, include the user name and password in the command.

    For example, on Microsoft Windows operating systems, run the following command:

    ```
    syncNode.bat <admin_host_name> <OP_SOAP_port>
    -user <admin_username> -password <admin_password>
    ```
12. Restart the OpenPages GRC Platform services.

Modifying the LDAP configuration file for LDAP over SSL

You must modify the authentication configuration file to enable the LDAP Directory Server that you are using.

The aurora_auth.config file contains three authentication modules:

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

The only module that the IBM OpenPages GRC Platform system pays attention to is the module that is named Openpages. Therefore, you need to make a backup of the Openpages module, rename the OpenpagesIP or OpenpagesAD to Openpages, and then change the settings to reflect the settings of your LDAP server.

Procedure

1. Stop all OpenPages GRC Platform 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 GRC Platform application.
3. Find the Openpages module and change its name to OpenpagesDefault.

4. Modify either the OpenpagesIP or OpenpagesAD module name to Openpages.
   - If you are using a Microsoft Active Directory server, change the name of the OpenpagesAD module to Openpages.
   - If you are using a Sun One Directory Server, change the name of the OpenpagesIP module to Openpages.
   - If you are using a different LDAP server, you can use either of these modules. Choose a module to use as a template and change its name to Openpages.
5. Specify the correct values for the following properties in the module that you named Openpages:

   provider.url
   Change the value to the hostname and port number for the LDAP authentication server. For LDAP over SSL (LDAPS), the protocol is ldaps and the port is the LDAPS port number (by default, 636).

   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, 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
   You can add additional custom parameters that are supported by the Java Naming and Directory Interface (JNDI). Precede a JNDI property with the ctx.env. prefix.

   For example, if you want to use the JNDI property com.sun.jndi.ldap.connect.timeout, use ctx.env.com.sun.jndi.ldap.connect.timeout="*<value>*" in the aurora_auth.config file.

   For information about JNDI properties, see the Java SE documentation (http://docs.oracle.com/javase/7/docs/technotes/guides/jndi/jndi-ldap.html#JNDIPROPS).

   For example:

   ```
   Openpages
   {
      com.openpages.aurora.service.security.namespace.LDAPLoginModule
             required debug=false
         provider.url="ldaps://myserver.company.com:636"
         security.authentication="simple"
         security.search.user.dn="cn=Directory Manager"
         security.search.user.credentials="openpages"
         base.dn="ou=people,o=IBM,c=US"
         user.attr.id="uid"
         ;
   };
   ```

6. When you are finished editing the file, save your changes and exit.
7. Import the root certificate and any intermediate signer certificates for your LDAP server to the trust store on the IBM WebSphere Application Server that you are using for OpenPages.

   For more information, see “Importing root and signer certificates to the local trust store ” on page 513.
8. Restart all services.

Results
You have configured the OpenPages GRC Platform system to use an external LDAP user authentication server over SSL.

Renewing SSL Certificates for OpenPages GRC Platform

Periodically, SSL certificates need to be renewed and re-imported into your IBM OpenPages GRC Platform environment.

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 GRC Platform, 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 "Renewing SSL certificates in a IBM WebSphere Application Server environment" on page 517

Renewing SSL Certificates for Cognos Environments on an IIS Web Server

Renew SSL certificates for Cognos environments for the web server on any reporting server that will handle external Cognos traffic.

This information 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 **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:

Table 167: .	
In this text box	**Do this**

   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** icon 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 **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** icon 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 Cognos to use the IBM OpenPages GRC Platform HTTPS address and SSL port.

Renewing certificates for Cognos environments on an Apache Web Server
Perform these steps for the web server on any reporting server that will handle external Cognos traffic.

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 GRC Platform 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) Apache uses OpenSSL which requires the server keys and certificate locations be updated in `extras/httpd-ssl.conf`.

   For more information, see “SSL configuration for Apache Web Server” on page 504.

Renewing SSL certificates in a IBM WebSphere Application Server environment
To renew an SSL certificate 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**.

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 OpenPages GRC Platform 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.csr.

i) Click **OK**.

Note: To avoid additional configuration steps, ensure the alias matches the previous alias.

The certificate request file is created in *<OP_Home>* | profiles | OpenPagesDmgr | etc

where *<OP_Home>* is the installation location of the OpenPages GRC Platform application. By default, this is c:\OpenPages on Windows, and /opt/OpenPages on AIX and Linux.

.

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 server and CA certificates to the *<OP_Home>* | profiles | OpenPagesDmgr | etc directory. Make sure the certificates are named to distinguish the server 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**.

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 GRC Platform 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 GRC Platform admin server using the IBM WebSphere Integrated Solutions Console. For details on these tasks, see "SSL for OpenPages GRC Platform environments" on page 494.

Setting up SSL for the global search service

You can configure IBM OpenPages GRC Platform global search service (Apache Solr) to use Secure Sockets Layer (SSL). SSL ensures that all data that is passed between the application server and the Solr service remains private.

About this task

If you are setting up the global search component in a test environment, do not enable Secure Sockets Layer (SSL) until you resolve all installation and configuration issues.

For more information about the commands that are used in this task, see the Apache Solr documentation https://cwiki.apache.org/confluence/display/solr/Enabling+SSL#EnablingSSL-BasicSSLSetup.

Important: IBM is not responsible for third-party content. At the time of publication, the information is correct.

Procedure

1. If the global search component is enabled, you must disable it.
   a) Log on to OpenPages as a user with administrative privileges.
   b) Click **Administration** > **Global Search**.
   c) Click **Disable**.
2. Stop the global search services.

   For more information, see “Start or stop the global search services” on page 553.
3. Create a certificate for the secure connection.
   a) Go to the *<SEARCH_HOME>*`/solr/server/etc` folder and run the following command.

```
keytool -genkeypair -alias alias -keyalg key_algorithm
  -keysize keysize -keypass key_pass -storepass keystore_passwd
  -validity validity -keystore jks_keystore -ext ip_address
  -dname "CN=localhost, OU=Organizational Unit, O=Organization, L=Location,
   ST=State, C=Country"
```

   In the following example, the command creates a self-signed certificate in a key store named `solr-ssl.keystore.jks`. The key store contains a key with an alias of `solr-ssl`, a key store password of `secret`, a trust store password of `secret`. It specifies Subject Alternative Name (SAN) values of `DNS:host1.companya.com` and `IP:127.0.0.1,192.168.7.1` to include in the certificate. (SAN values are not mandatory, and might not be specified in your environment).

```
keytool -genkeypair -alias solr-ssl -keyalg RSA
  -keysize 2048 -keypass secret -storepass secret
  -validity 9999 -keystore solr-ssl.keystore.jks
  -ext SAN=DNS:host1.companya.com,IP:127.0.0.1,IP:192.168.7.1
  -dname "CN=localhost, OU=Organizational Unit, O=Organization, L=Location,
   ST=State, C=Country"
```

   b) Convert the JKS key store into PKCS12 format.

```
keytool -importkeystore -srckeystore jks_keystore
 -destkeystore jks_keystore.p12 -srcstoretype source_keystore_type
 -deststoretype destination_keystore_type
```

   When prompted, type a destination key store password, and the source key store password that you specified in the step 3a.

   c) Convert the PKCS12 format key store, including the certificate and the key, into PEM format.

   To run this command, `openssl` must be installed, and added to the PATH environment variable.

```
openssl pkcs12 -in <jks_keystore.p12> -out <jks_keystore.pem>
```

   When you are prompted for the import password and PEM pass phrase, you can use the same password that you specified for the *<key_pass>* value in step 3a.

4. Export the certificate.

```
keytool -export -keystore <jks_keystore> -alias <alias> -file <solr_certificate>
```

When you are prompted for the key store password, type the password that you specified for the *<key_pass>* value in step 3a.

5. Update the `solr.in` file.
   a) Edit the following file in a text editor:

   <SEARCH_HOME>`\solr\bin\solr.in.cmd` (on Windows)

   <SEARCH_HOME>`/solr/bin/solr.in.sh` (on UNIX)

   b) Uncomment and set the following SSL properties.

```
SOLR_SSL_KEY_STORE=etc/jks_keystore
SOLR_SSL_KEY_STORE_PASSWORD=keystore_passwd
SOLR_SSL_TRUST_STORE=etc/jks_keystore
SOLR_SSL_TRUST_STORE_PASSWORD=keystore_passwd
SOLR_SSL_NEED_CLIENT_AUTH=false
SOLR_SSL_WANT_CLIENT_AUTH=true
```

On Windows, you might need to use `server/etc` as the path name for the SOLR_SSL_KEY_STORE and SOLR_SSL_TRUST_STORE properties.

6. Log in to the OpenPages application as a user with administrative privileges. Update the following settings to use `https` instead of `http`.

Administration > **Settings** > **Platform** > **Search** > **Admin** > **Search Server Administration URL**

Administration > **Settings** > **Platform** > **Search** > **Index** > **Search Server URL**

Administration > **Settings** > **Platform** > **Search** > **Request** > **Search Server URL**

7. Copy the certificate file that you exported to the following folder on the application server.

<WAS_HOME>`/AppServer/Java/8.0/jre/lib/security`

8. Add the certificate to the IBM JRE key store file.
   a) Open a Windows command prompt by using the **Run as Administrator** option, or open a UNIX shell with administrative privileges.
   b) Back up the *<WAS_HOME>*`/WebSphere/AppServer/Java/8.0/jre/lib/security/cacerts` file.
   c) Go to *<WAS_HOME>*`/WebSphere/AppServer/Java/8.0/jre/lib/security` folder and run the following command.

```
keytool -import -alias <alias> -keystore cacerts -file
   solr_certificate
```

When prompted, type the key store password of the `cacerts` key store. The default password is typically `changeit`.

   d) Confirm that you want to trust the certificate.
   e) Restart all OpenPages services.

9. Import the certificate to the IBM WebSphere trust store.
   a) Log on to the WebSphere Integrated Solutions Console.

   `http://`*<server_name>*`:`*<port>*`/ibm/console`

   The default port is 9060.

   b) Click **Security** > **SSL certificate and key management** > **Key stores and certificates** > **CellDefaultTrustStore** > **Signer certificates**.
   c) Click **Add**.
   d) Update the following fields:

- **Alias**: Type the value that you specified for the *alias* in step 9.
- **File name**: Type the full path of the *solr_certificate* file that you imported into the cacerts file in step 9.

  Ensure that the data type is set to **Base64-encoded ASCII data**.

e) Click **OK**.

f) Click **Save** to update the master configuration.

g) Restart all OpenPages services.

10. Start the global search services.

    For more information, see "Start or stop the global search services" on page 553.

11. If the search server is installed on a different computer than the application server, add the certificate to the IBM JRE key store on the search server.

    a) Open a Windows command prompt by using the **Run as Administrator** option, or open a UNIX shell with administrative privileges.

    b) Go to the *<JAVA_HOME>*/lib/security directory and run the following command:

    ```
    keytool -import -alias <alias> -keystore cacerts
       -file <SEARCH_HOME>/solr/server/etc/solr_certificate
    ```

    c) When prompted, type the key store password of the cacerts key store. The default password is typically changeit.

12. Continue with the post installation or post upgrade steps for global search.

Enabling SSL database connection between the search server and the database server

When you install the global search server, it uses a plain connection to communicate with the database server. If your organization requires that you use a SSL connection, you must complete these steps.

Procedure

1. Disable global search.

   a) Log in to IBM OpenPages GRC Platform with administrative privileges.

   b) Navigate to **Administration** > **Global Search** and select **Disable**.

2. Configure SSL on the database server and exchange the certificate between the database server and the global search server.

3. On the search server, follow these steps to enable SSL:

   a) If you are using Windows, open a command prompt with the **Run As Administrator** option.

   b) Go to the *<SEARCH_HOME>*/OPSearch/opsearchtools/ directory.

   c) Enable SSL by running the following command.

   ```
   opsearchtool.cmd|.sh enableSSLDbConn -ssltruststorefile <path_to_client_keystore.jks>
   -ssltruststorepassword <your_JKS_password>
   ```

   For example:

   ```
   opsearchtool.cmd enableSSLDbConn -ssltruststorefile c:\keystore\client_keystore.jks
   -ssltruststorepassword JKSpassword
   ```

   d) Edit the file *<SEARCH_HOME>*/OPSearch/opsearchtools/openpages_search.properties. Change the port number to the SSL port that your database server is using: OPSearchTool.DatabasePort = your_db_ssl_port_number.

4. Enable global search.

   a) Log in to IBM OpenPages GRC Platform with administrative privileges.

   b) Navigate to **Administration** > **Global Search** and select **Enable**.

Note: In some rare cases, you might need to pass additional parameters to Java's runtime environment. If this is the case, you can edit one of the following files to do so.

- For DB2, edit *<SEARCH_HOME>*/OPSearch/opsearchtools/DatabasePropertyFile_DB2.properties
- For Oracle, edit *<SEARCH_HOME>*/OPSearch/opsearchtools/DatabasePropertyFile_Oracle.properties

Disabling the SSL database connection between the search server and the database server

If you need to disable the SSL connection between the search server and the database server, follow these steps.

Procedure

1. Disable global search.
   a) Log in to IBM OpenPages GRC Platform with administrative privileges.
   b) Navigate to **Administration** > **Global Search** and select **Disable**.
2. Disable SSL on the database server.
3. Start global search.
   a) Log in to IBM OpenPages GRC Platform with administrative privileges.
   b) Navigate to **Administration** > **Global Search** and select **Enable**.

Oracle Transparent Data Encryption (TDE)

You can use Oracle Transparent Data Encryption (TDE) to encrypt the OpenPages and Cognos table spaces in the OpenPages database.

This task is optional.

Note: This task is for existing databases. You can also set up TDE when you do a fresh installation. For more information, see the *IBM OpenPages GRC Installation and Deployment Guide*.

IBM OpenPages GRC Platform supports the ability to implement TDE, but TDE is an Oracle feature. You need to be familiar with data encryption of Oracle databases and you need to configure and maintain TDE. If you have questions about TDE, refer to the Oracle documentation.

Restriction: OpenPages supports Oracle TDE only for table spaces. Column-based TDE is not supported.

To implement Oracle TDE, you need to complete two main tasks:

1. Configure a keystore. You can do this step at any time after you install OpenPages.

   Your database administrator needs to create a keystore. The steps and requirements for keystores are determined by Oracle. IBM is not responsible for the configuration or maintenance of the keystore.
2. Encrypt the table spaces that support encryption.

   To implement Oracle TDE on an existing installation of OpenPages, manual database steps are required. These manual steps require database administrator privileges and skills. If you do not have database administration experience, review these manual steps with a database administrator before you set up Oracle TDE.

   A table space can be encrypted only when it is initially created. You cannot alter an existing table space to enable encryption. Instead, you drop the table spaces, re-create them with TDE enabled, and then restore the schema.

   Note: Oracle does not support encryption on system, undo, or temporary table spaces.

For more information about TDE, refer to the Oracle documentation, such as the Oracle Database Advance Security Guide (https://docs.oracle.com/database/121/ASOAG/toc.htm).

Prerequisites and process overview

Ensure that your environment meets prerequisites for Oracle TDE and review the configuration process.

Note: These instructions are specific to Oracle version 12.1.0.2.

Ensure that your environment meets the following prerequisites:

1. IBM OpenPages GRC Platform 7.4 or later is installed.
2. The Oracle instance is open and accepting connections.
3. All users must be off of the system until all steps in the Oracle TDE configuration process are complete.
4. The database compatibility parameter is set to at least 11.2.0.0 or higher.

Complete the following process to configure Oracle TDE:

1. Configure a software key store. Refer to the Oracle documentation: Configuring Transparent Data Encryption
2. Encrypt the OpenPages and Cognos table spaces that support encryption:
   a. Verify the value of the database compatible parameter.
   b. Do a full backup of the OpenPages schema.
   c. Do a full backup of the Cognos schema.
   d. Shut down all OpenPages components.
   e. Drop the OpenPages and Cognos table spaces.
   f. Re-create the OpenPages and Cognos table spaces.
   g. Verify that the table spaces are encrypted.
   h. Restore the OpenPages schema.
   i. Restore the Cognos schema.

Encrypting OpenPages and Cognos table spaces

You can encrypt the OpenPages and Cognos table spaces by using Oracle TDE.

Before you begin

Ensure that no users are on the system before you begin.

Do this procedure after you set up the keystore.

Procedure

1. Log on to the OpenPages database instance as the instance owner.
2. Start SQL*Plus.
3. Verify that the database compatible parameter is set to 11.2.0.0 or later.

   ```
   select value from GV$SYSTEM_PARAMETER where name = 'compatible';
   ```

4. Do a full backup of the OpenPages and Cognos databases.

   For more information, see “DB2 databases for OpenPages GRC Platform backup and restore” on page 394 or “Backing up the OpenPages database (Oracle)” on page 426.
5. Shut down all OpenPages and Cognos components: application servers (admin and non-admin), reporting servers (active and standby), and the search server.

   For more information, see Chapter 20, “Starting and stopping servers,” on page 549.
6. Drop all OpenPages and Cognos table spaces.

   Do the following steps if your environment meets these criteria:

   - OpenPages and Cognos use the same database.

- You are using a standard deployment, where each table space uses a single data file.

If you have multiple data files per table space or if you have customized your deployment in any way, your DBA staff will need to analyze your environment to determine what actions are needed to drop the table spaces.

a) Determine the list of table spaces.

The default table space names are:

```
AURORA
INDX
AURORA_SNP
AURORA_NL
AURORA_NLI
AURORA_CLOB_DATA
AURORA_DOMAIN_INDX
CRN
```

Run the following query as a DBA user get a list of the existing table spaces:

```
select tablespace_name from dba_tablespaces;
```

b) Run the following query to collect information about the table spaces.

You will use this information in a later step.

If you use custom table space names, modify the WHERE clause.

```
select dt.tablespace_name,
       df.file_name,
       ceil(df.bytes/1048576)||' M' as file_size
  from DBA_TABLESPACES dt,
       DBA_DATA_FILES df
 where dt.tablespace_name = df.tablespace_name
   and dt.tablespace_name in
         ('AURORA','INDX','AURORA_SNP','AURORA_NL','AURORA_NLI',
          'AURORA_CLOB_DATA','AURORA_DOMAIN_INDX','CRN');
```

Example output:

```
TABLESPACE_NAME      FILE_NAME                                          FILE_SIZE
-------------------- -------------------------------------------------- ----------
AURORA               /home/oracle/app/oradata/aurora.dbf                640 M
AURORA_CLOB_DATA     /home/oracle/app/oradata/aurora_clob_data.dbf      128 M
AURORA_DOMAIN_INDX   /home/oracle/app/oradata/aurora_domain_indx.dbf    128 M
AURORA_NL            /home/oracle/app/oradata/aurora_nl.dbf             128 M
AURORA_NLI           /home/oracle/app/oradata/aurora_nli.dbf            128 M
AURORA_SNP           /home/oracle/app/oradata/aurora_snp.dbf            256 M
INDX                 /home/oracle/app/oradata/indx.dbf                  640 M
CRN                  /home/oracle/app/oradata/crn.dbf                   512 M
```

Attention: If a table space name appears twice in the output, the database uses more than one data file per table space. In this case, contact your database administrator before you continue.

c) Delete the database objects.

Log in to SQL*Plus as the OpenPages database user and run the following script:

```
@AuroraDbDelete.sql
```

When the script completes, log out of SQL*Plus.

d) Drop the table spaces.

Log in to SQL*Plus as a DBA user and run the following commands. If you use custom table space names, use the names that you found in step 6a.

```
drop tablespace AURORA including contents and datafiles;
drop tablespace INDX including contents and datafiles;
drop tablespace AURORA_SNP including contents and datafiles;
```

```
drop tablespace AURORA_NL including contents and datafiles;
drop tablespace AURORA_NLI including contents and datafiles;
drop tablespace AURORA_CLOB_DATA including contents and datafiles;
drop tablespace AURORA_DOMAIN_INDX including contents and datafiles;
drop tablespace CRN including contents and datafiles;
```

7. Re-create the table spaces with Oracle TDE configured.
   a) Create a `.sql` file that contains the commands.

   Copy the following template into a file. Make the following changes to the file:

   - If you use custom table space names, replace the table space names with the names from step 6a.
   - Replace the placeholders with the values from step 6b.
   - Decide which encryption algorithm to use, and uncomment it from the `define encrypt_var=''` list.
   - Save the file.

```
-------------------------------------------------------------------------------
--            **** Oracle Transparent Data Encryption ****
-- You can modify the encryption variable below or use one of the provided
-- options.  To use a provided option, uncomment the desired algorithm from
-- the list below.
-------------------------------------------------------------------------------
define encrypt_var=''
--define encrypt_var='ENCRYPTION USING ''3DES168'' DEFAULT STORAGE(ENCRYPT)'
--define encrypt_var='ENCRYPTION USING ''AES128'' DEFAULT STORAGE(ENCRYPT)'
--define encrypt_var='ENCRYPTION USING ''AES192'' DEFAULT STORAGE(ENCRYPT)'
--define encrypt_var='ENCRYPTION USING ''AES256'' DEFAULT STORAGE(ENCRYPT)'

create tablespace AURORA datafile '<file name from query>'
  size <file size from query> M reuse autoextend on
  next 128 M &&encrypt_var;

create tablespace INDX datafile '<file name from query>'
  size <file size from query> M reuse autoextend on
  next 128 M &&encrypt_var;

create tablespace AURORA_SNP datafile '<file name from query>'
  size <file size from query> M reuse autoextend on
  next 128 M &&encrypt_var;

create tablespace AURORA_CLOB_DATA datafile '<file name from query>'
  size <file size from query> M reuse autoextend on
  next 128 M &&encrypt_var;

create tablespace AURORA_DOMAIN_INDX datafile '<file name from query>'
  size <file size from query> M reuse autoextend on
  next 128 M &&encrypt_var;

create tablespace AURORA_NL nologging datafile '<file name from query>'
  size <file size from query> M reuse autoextend on
  next 128 M extent management local uniform size 2 M &&encrypt_var;

create tablespace AURORA_NLI nologging datafile '<file name from query>'
  size <file size from query> M reuse autoextend on
  next 128 M extent management local uniform size 2 M &&encrypt_var;

create tablespace CRN datafile '<file name from query>'
  size <file size from query> M reuse autoextend on
  next 128 M &&encrypt_var;
```

   Sample file:

```
-------------------------------------------------------------------------------
--            **** Oracle Transparent Data Encryption ****
-- You can modify the encryption variable below or use one of the provided
-- options.  To use a provided option, uncomment the desired algorithm from
-- the list below.
-------------------------------------------------------------------------------
--define encrypt_var=''
--define encrypt_var='ENCRYPTION USING ''3DES168'' DEFAULT STORAGE(ENCRYPT)'
define encrypt_var='ENCRYPTION USING ''AES128'' DEFAULT STORAGE(ENCRYPT)'
--define encrypt_var='ENCRYPTION USING ''AES192'' DEFAULT STORAGE(ENCRYPT)'
--define encrypt_var='ENCRYPTION USING ''AES256'' DEFAULT STORAGE(ENCRYPT)'
```

```
create tablespace AURORA datafile
  '/home/oracle/app/oradata/aurora.dbf'
  size 640 M reuse autoextend on next 128 M &&encrypt_var;

create tablespace INDX datafile
  '/home/oracle/app/oradata/indx.dbf'
  size 640 M reuse autoextend on next 128 M &&encrypt_var;

create tablespace AURORA_SNP datafile
  '/home/oracle/app/oradata/aurora_snp.dbf'
  size 256 M reuse autoextend on next 128 M &&encrypt_var;

create tablespace AURORA_CLOB_DATA datafile
  '/home/oracle/app/oradata/aurora_clob_data.dbf'
  size 128 M reuse autoextend on next 128 M &&encrypt_var;

create tablespace AURORA_DOMAIN_INDX datafile
  '/home/oracle/app/oradata/aurora_domain_indx.dbf'
  size 128 M reuse autoextend on next 128 M &&encrypt_var;

create tablespace AURORA_NL nologging datafile
  '/home/oracle/app/oradata/aurora_nl.dbf'
  size 128 M reuse autoextend on next 128 M extent management
  local uniform size 2 M &&encrypt_var;

create tablespace AURORA_NLI nologging datafile
  '/home/oracle/app/oradata/aurora_nli.dbf'
  size 128 M reuse autoextend on next 128 M extent management
  local uniform size 2 M &&encrypt_var;

create tablespace CRN datafile
  '/home/oracle/app/oradata/crn.dbf'
  size 512 M reuse autoextend on next 128 M &&encrypt_var;
```

b) Log in to SQL*Plus as a DBA user and run the file that you created.

For example, if your file is named `tbsp_create.sql`, log into SQL*Plus as a DBA user and run the following commands:

```
spool tbsp_create.log
@tbsp_create.sql
exit;
```

8. Grant space privileges to the OpenPages and Cognos users on the new table spaces.

Use the following syntax. If you use custom table space names, replace the table space names with the names from step 6a.

```
alter user <openpages db user> quota unlimited on AURORA;
alter user <openpages db user> quota unlimited on INDX;
alter user <openpages db user> quota unlimited on AURORA_NL;
alter user <openpages db user> quota unlimited on AURORA_NLI;
alter user <openpages db user> quota unlimited on AURORA_SNP;
alter user <openpages db user> quota unlimited on AURORA_CLOB_DATA;
alter user <openpages db user> quota unlimited on AURORA_DOMAIN_INDX;
alter user <cognos db user> quota unlimited on CRN;
```

Example:

```
alter user openpage quota unlimited on AURORA;
alter user openpage quota unlimited on INDX;
alter user openpage quota unlimited on AURORA_NL;
alter user openpage quota unlimited on AURORA_NLI;
alter user openpage quota unlimited on AURORA_SNP;
alter user openpage quota unlimited on AURORA_CLOB_DATA;
alter user openpage quota unlimited on AURORA_DOMAIN_INDX;
alter user cognos quota unlimited on CRN;
```

9. Verify that the table spaces are encrypted.

Log in to the OpenPages database as a DBA user and run the following command. If you use custom table space names, replace the table space names in the `WHERE` clause with the names from step 6a.

```
select tablespace_name, encrypted, status
   from dba_tablespaces
```

```
   where tablespace_name in
        ('AURORA','INDX','AURORA_SNP','AURORA_NL','AURORA_NLI',
        'AURORA_CLOB_DATA','AURORA_DOMAIN_INDX','CRN');
```

Verify that the output is similar to the following text:

```
TABLESPACE_NAME                ENC STATUS
------------------------------ --- ---------
AURORA                         YES ONLINE
AURORA_CLOB_DATA               YES ONLINE
AURORA_DOMAIN_INDX             YES ONLINE
AURORA_NL                      YES ONLINE
AURORA_NLI                     YES ONLINE
AURORA_SNP                     YES ONLINE
INDX                           YES ONLINE
CRN                            YES ONLINE

8 rows selected.
```

10. Restore the OpenPages schema, and then restore the Cognos schema.

    For more information, see "DB2 databases for OpenPages GRC Platform backup and restore" on page 394 or "Import the production data into the test environment" on page 443 if you are using Oracle.
11. Restart all OpenPages and Cognos components: application servers (admin and non-admin), reporting servers (active and standby), and the search server.

    For more information, see Chapter 20, "Starting and stopping servers," on page 549.

Shortening the URL for OpenPages GRC Platform

You can shorten the IBM OpenPages GRC Platform application URL. You might shorten the URL to support privacy or to support some mobile uses of the URL. To shorten the URL, change the values for properties in various files.

Before you begin

Before you modify the files that are referenced in this procedure, back up the files.

About this task

In the following example of the default and the shortened URL, the default port number 10108 is used with the IBM WebSphere application server:

Default URL
http://*server_name*:10108/openpages

Shortened URL
http://*server_name*:10108/

OP_Home in the file path represents the installation location of the OpenPages GRC Platform application.

The default path for a Microsoft Windows installation is `c:\OpenPages`.

The default path for an AIX or Linux installation can be `/opt/OpenPages`.

Procedure

1. Stop the Cognos service and the OpenPages GRC Platform Framework Model Generator service. For more information, see "Starting and stopping the Cognos services" on page 560.
2. Log on to the IBM WebSphere administration console. Navigate to **Applications** > **Application Types**, and click **WebSphere enterprise applications**.
   a) Click the application **op-apps**.
   b) Under **Web Module Properties**, click **Context root for Web modules**.
   c) For the web module **Sarbanes-Oxley Self-Assessment Application Module**, replace the current value for the Context Root with the new value:

Current value
`/openpages`

New value
`/`

d) Click **save directly to the master configuration**.

e) Stop and start the **op-apps** application.

3. On the OpenPages server, navigate to the following folder:

Windows:
OP_Home`:\OpenPages\aurora\conf`

AIX or Linux:
OP_Home`/aurora/conf`

a) For each of the properties files that are listed in the following table, open the file in a notepad or XML editor. Change the current value to the new value, and then save the file:

Table 168: Shorten URL, property values for use with IBM Websphere application server

File name	Current value	New value
`aurora.properties`	application.url.path=http\://*server_name*\:10108/openpages	application.url.path=http\://*server_name*\:10108
server_name-OPNode1Server1-server.properties	url.path.openpages=http\://*server_name*\:10108/openpages	url.path.openpages=http\://*server_name*\:10108
server_name-OPNode1Server1-sosa.properties	application.url.path=http\://*server_name*\:10108/openpages	application.url.path=http\://*server_name*\:10108
server_name-OPNode1Server1-sosa.properties	application.context=/openpages	application.context=

4. On the Cognos server, navigate to the following folder:

Windows:
<Cognos_Home>`\configuration`

AIX or Linux:
<Cognos_Home>`/configuration`, where *<Cognos_Home>* might be `/opt/ibm/Cognos/analytics`.

a) Open the `OpenPagesSecurityProvider_OpenPagesSecurityRealm.properties` file in a notepad or XML editor.

b) Change the current value to the new value, and then save the file:

Current value
`openpages.application.url=http\://`*server_name*`\:10108/openpages`

New value
`openpages.application.url=http\://`*server_name*`\:10108`

5. Restart the OpenPages GRC Platform application servers. For more information, see "Starting all application services in Windows using a script" on page 551 or "Starting all application servers in AIX and Linux using a script" on page 552.

6. Start the Cognos service and the OpenPages Framework Model Generator service. For more information, see "Starting and stopping the Cognos services" on page 560.

7. After the services are started, log in to the application, and click **Administration** > **Settings**. Expand the following folders: **Platform** > **Reporting Schema** > **Object URL Generator**. Open the **Detail Page**, replace the current value with the new value, and then click save.

   Current value
   `/openpages/view.resource.do`

   New value
   `/view.resource.do`
8. Re-create the reporting schema. For more information, see "Creating or recreating the reporting schema" on page 91.

Parameters for cluster members

When working with cluster members, there are values for common parameters. You must enter these parameter values consistently across all of the tasks.

For example, 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 `OP_Host`, then you must enter `OP_Host` whenever you are asked to provide the value for `<server_name>`.

The tasks for working with cluster members are:

- "Create the OpenPages GRC Platform application managed server instances" on page 483
- "Modifying values in the Sosa property file" on page 491

Table 169: Parameters for cluster members in IBM WebSphere

Parameter	Description
`<OP_Home>`	The installation location of the IBM OpenPages GRC Platform application. The default path for a Windows installation is `c:\OpenPages`. The default path for an AIX and Linux installation is `/opt/OpenPages`.
`<server_name>`	The host name of the machine on which you are adding the managed server instance. For example, `OP_Host`
`<server#>`	The number of the managed server you are adding to the cluster. For example, If you currently have one managed server on `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` For example, 10101

Table 169: Parameters for 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` For example, 10108
<opadmin_WAS_username>	If IBM WebSphere global security is configured, this is the OpenPages administrator user name for accessing the IBM WebSphere Integrated Solutions Console.
<opadmin_WAS_password>	If IBM WebSphere global security is configured, this is the OpenPages administrator password for accessing the IBM WebSphere Integrated Solutions Console. Default: openpages

Configuring HTTP compression in OpenPages GRC Platform

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 GRC Platform application servers, HTTP compression is installed during the installation process.

By default, HTTP compression is disabled on the 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 OpenPages GRC Platform application and, or Cognos 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 Cognos servers.

Note: Files that are already compressed, such as image files, PDF, and ZIP files will not be compressed to improve performance.

See these topics for details:

- “Enabling or disabling HTTP compression on OpenPages GRC Platform Application Servers” on page 530
- “Enabling or disabling compression on the Cognos Server using Windows IIS” on page 531
- “Enabling compression on the Cognos Server using Apache Web Server” on page 532
- “Disabling compression on the Cognos Server using Apache Web Server” on page 533

For information on installing and configuring HTTP Compression for Microsoft Windows IIS 7 only, see Appendix C, “Installing and configuring HTTP compression,” on page 767

Enabling or disabling HTTP compression on OpenPages GRC Platform Application Servers

Follow these steps to enable or disable HTTP compression on IBM OpenPages GRC Platform application servers via settings in the application user interface.

Note: These steps apply to all OpenPages GRC Platform application servers in a clustered environment.

Procedure

1. Log on to the OpenPages GRC Platform application user interface as a user with administrative permissions.
2. Access the Settings page.
3. Set the value in the **Show Hidden Settings** setting to `true`.
4. Expand the **Applications** > **Common** > **Configuration** > **HTTP Compression** folder hierarchy.

   Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.
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 compression on the Cognos Server using Windows IIS

You can enable or disable compression on the Cognos Server using Windows IIS.

Note: This information applies only to a Cognos server running IIS 7 on Windows Server 2008. Before you can enable HTTP compression on a Cognos server running Windows, HTTP compression must first be installed and configured. To verify and/or configure static or dynamic compression on Cognos servers, see Appendix C, “Installing and configuring HTTP compression,” on page 767.

Procedure

1. From the Windows **Start** menu on the Cognos server, select **Control Panel**.
2. Open Administrative Tools as follows:
   a) Do one of the following:

Table 170: Microsoft Windows server versions and instructions to open Administrative Tools	
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, `cognos`).
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 Cognos Server using Apache Web Server

You can enable compression on the Cognos server using Apache Web Server.

HTTP compression can be enabled or disabled on the Apache Web Server for Windows, AIX, and Linux 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 Cognos server, navigate to the *<Apache_Home>*|`conf` directory.

   Where: *<Apache_Home>* is the installation location of the Apache Web Server. For example, for Windows, a directory structure could be `C:\Program Files (x86)\Apache2.2` and for AIX and Linux, the directory structure could be `/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. 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 and Linux:
     - Log on to the Cognos server as the root user.
     - Navigate to the *<Apache_Home>*`/bin` directory.
     - Enter the following command to stop the server:

       ```
       ./apachectl stop
       ```

– Type the following command to re-start the server:

```
./apachectl start
```

Disabling compression on the Cognos Server using Apache Web Server

You can disable compression on the Cognos server using Apache Web Server.

Note: This information applies to Windows, AIX and Linux environments.

Procedure

1. On the Cognos server, navigate to the *<Apache_Home>*|`conf` directory.

   Where: *<Apache_Home>* is the installation location of the Apache Web Server. For example, for Windows, a directory structure could be `C:\Program Files (x86)\Apache2.2` and for AIX and Linux, the directory structure could be `/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 and Linux:
     – Log on to the Cognos server as the root user.
     – Navigate to the *<Apache_Home>*`/bin` directory.
     – Enter the following command to stop the server:

```
./apachectl stop
```

     – Type the following command to re-start the server:

```
./apachectl start
```

Factors that affect performance of activity and grid views

When you design activity or grid views, keep in mind the following factors that can affect the performance.

Number of paths
The more paths in the activity view the more work the application must do to traverse those paths and provide a result. The more paths that you specify the longer it takes to provide a result.

Depth of paths
Each object type in the path results in an incremental increase in the work that is required to traverse the path. The deeper a certain path is, the longer it takes to provide a result for that path.

Number of child objects per top-level object
The ratio of top-level objects to child objects determines how much work the application must do to gather the total result set. The more child objects per top-level object, the longer it takes to provide a result.

Security rules (RLS/FLS)
Security rules are processed in the context of the individual instance of an object. The mere inclusion of even a simple security rule increases the work that is required in the application to obtain a result set. As the complexity of the security rule increases, the time it takes to provide a result also increases.

Improve performance of OpenPages GRC Platform application functions on a DB2 server

You can improve the performance of IBM OpenPages GRC Platform application functions by collecting performance statistics for the IBM DB2 server, and by rebinding OpenPages GRC pl/sql packages.

Examples of application functions include importing instance data using FastMap, importing metadata using Object Manager, and updating OpenPages GRC repository using SCOR rules.

Up-to-date statistics are necessary for the proper performance of OpenPages GRC applications that use a DB2 server. You can use a script to force the DB2 server to collect statistics, and by default, rebind all OpenPages GRC pl/sql packages. The script requires all OpenPages GRC application services to stop before it runs. For details on stopping servers, see Chapter 20, “Starting and stopping servers,” on page 549.

You run the script from the primary OpenPages GRC application server. You do not need to run this script from all cluster member servers, but you must stop all cluster member services before running the script to rebind OpenPages GRC pl/sql packages.

If a database is still running, you see the error SQL1026N. If this happens, verify that OpenPages GRC services are not running, and disconnect all active connections to the database before continuing.

You can run the script on Microsoft Windows, AIX, and Linux.

1. For Windows users only, type the following command in a command prompt window to initialize the DB2 command line processor (CLP):

   ```
   db2cmd
   ```

2. Browse to the *<OP_HOME>* | `aurora` | `bin` | `db2stats` folder.
3. Run the following script:
   - On Windows: `CollectSchemaStatistics.bat [-n] [-i]`
   - On AIX and Linux: `CollectSchemaStatistics.sh [-n] [-i]`

Use these parameters as required:

- [-n] to skip rebinding of database packages.
- [-i] to run the script in interactive mode.

The script execution time varies depending on OpenPages GRC application usage.

You can schedule this script to run by using a task scheduler, cronjob, or similar utility. The suggested schedule to use is as follows:

- Schedule the script to run daily without rebinding of OpenPages GRC pl/sql packages.
- Schedule the script to run once a week with rebinding of OpenPages GRC pl/sql packages.

Server tuning settings

To avoid time-outs and other issues when using IBM OpenPages GRC Platform, you must configure the servers and the database:

Important: All tuning settings assume a maximum of 1000 concurrent users per node.

Configuring the database

Configure the IBM DB2 database to avoid time-out issues.

Procedure

1. Open the database console running as a DB2 administrator.
2. Set the tuning parameters using the following command:

```
db2 update db cfg for <DATABASE_NAME> using <VARIABLE> <VALUE>
```

For example, `db2 update db cfg for <DATABASE_NAME> using SELF_TUNING_MEM ON`

The following table describes the tuning parameter settings to use. Values shown in brackets are informational when the parameter is set to AUTOMATIC. This enables DB2 to control the parameter and reflects the current setting.

Table 171: Database tuning parameters

Parameter	Description	Value (default)
SELF_TUNING_MEM	Self tuning memory	ON
DATABASE_MEMORY	Size of database shared memory (4KB)	AUTOMATIC (2683751)
DB_MEM_THRESH	Database memory threshold	10
LOCKLIST	Max storage for lock list (4KB)	AUTOMATIC (82212)
MAXLOCKS	Percentage of lock lists per application	AUTOMATIC (97)
PCKCACHESZ	Package cache size (4KB)	AUTOMATIC (419456)
SHEAPTHRES_SHR	Sort heap threshold for shared sorts (4KB)	AUTOMATIC (63309)
SORTHEAP	Sort list heap (4KB)	AUTOMATIC (12661)
DBHEAP	Database heap (4KB)	AUTOMATIC (5405)
CATALOGCACHE_SZ	Catalog cache size (4KB)	2000
LOGBUFSZ	Log buffer size (4KB)	2560
UTIL_HEAP_SZ	Utilities heap size (4KB)	306174
STMTHEAP	SQL statement heap (4KB)	512000

Table 171: Database tuning parameters (continued)		
Parameter	**Description**	**Value (default)**
APPLHEAPSZ	Default application heap (4KB)	25600
APPL_MEMORY	Application Memory Size (4KB)	AUTOMATIC (40000)
STAT_HEAP_SZ	Statistics heap size (4KB)	AUTOMATIC (4384)
DLCHKTIME	Interval for checking deadlock (ms)	10000
LOCKTIMEOUT	Lock timeout (sec)	-1
CHNGPGS_THRESH	Changed pages threshold	80
NUM_IOCLEANERS	Number of asynchronous page cleaners	AUTOMATIC (10)
NUM_IOSERVERS	Number of I/O servers	AUTOMATIC (44)
SEQDETECT	Sequential detect flag	YES
DFT_PREFETCH_SZ	Default prefetch size (pages)	AUTOMATIC
TRACKMOD	Track modified pages	NO
	Default number of containers	1
DFT_EXTENT_SZ	Default tablespace extent size (pages)	32
MAXAPPLS	Max number of active applications	300
AVG_APPLS	Average number of active applications	10
MAXFILOP	Max DB files open per application	61440

3. Save your changes.
4. Validate the changes using the following command:

```
db2 get db cfg for <DATABASE_NAME>
```

Configuring the reporting server

Configure the reporting server to avoid time-out issues.

About this task

The reporting server is a component of Cognos Analytics. You configure the reporting server using IBM Cognos Configuration and IBM Cognos Administration.

Procedure

1. Log on to the Cognos server as a user with administrative permissions.
2. Go to the <*COGNOS_Home*>\bin64 directory.
3. Double-click the `cogconfigw.exe` file to start IBM Cognos Configuration, the Cognos Analytics configuration tool.
4. In the **Explorer** pane, expand **IBM Cognos services**, and click the **IBM Cognos** service.
5. In the properties pane, set the **Maximum memory for Tomcat in MB** property to **1024**.

6. From the **File** menu, click **Save** to save the updated Cognos Analytics configuration.
7. Go to IBM Cognos Administration, click the **Configuration** tab, and then click **Dispatchers and Services**.
8. Click the dispatcher that is used by your Cognos Analytics installation, and in the list of services find **ReportService**.
9. In the **Actions** column, click the **Set properties - ReportService** icon associated with the report service.
10. In the report service properties page, click the **Settings** tab, and specify the following settings.

    Note: To filter on the tuning settings in the list, under **Category**, click **Tuning**.

    - Set the **Number of low affinity connections for the report service during non-peak period** to **8**.
    - Set the **Maximum number of processes for the report service during non-peak period** to **8**.
    - Set the **Number of low affinity connections for the report service during peak period** to **8**.
    - Set the **Maximum number of processes for the report service during peak period** to **12**.
11. Click **OK** to apply the settings.

Using log files

The IBM OpenPages GRC Platform application writes error and other messaging information to a standard set of log files. You can use these log files to troubleshoot reporting and general user errors that may occur.

Configuring application thread-dump logs for cluster members

You can configure application thread-dump logs for cluster members

By default, application thread-dump logs are disabled. Use the instruction that follows to configure service thread-dump logs for cluster members.

Log folder location: *<OP_Home>* | `aurora` | `logs`

Table 172: Installation location of the OpenPages GRC Platform application

Operating system	Installation location
Windows	By default, *<OP_Home>* is `C:\OpenPages`
AIX and Linux	By default, *<OP_Home>* is `/opt/OpenPages`

Log file names are as follows:

IBM WebSphere

`OPNode<#>Server<#>-javacore.<time_stamp>.txt`.

For 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 GRC Platform 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:

Table 173: Property values and how to change them	
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 OpenPages GRC Platform servers after changing the value of this property as the application monitors this property for changes.

Configuring extended access logging on IBM WebSphere

You can configure extended access logging on IBM WebSphere.

Note: This information applies only to IBM WebSphere Application Server environments.

1. Start the IBM OpenPages GRC Platform 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 IBM WebSphere global security is not enabled, the URL is:
   `http://<host_name>:<port>/ibm/console` where

   `<host_name>` is the name of the server where IBM WebSphere is installed. The default port is 9060.
3. Expand **Servers** then **Server Types**, and click the **WebSphere application servers** link.
4. In the list on the **Application servers** page, click the name of the OpenPages GRC Platform 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 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 GRC Platform application. By default, this is `c:\OpenPages` on Windows, and `/opt/OpenPages` on AIX and Linux.

<host_name> is the name of the OpenPages GRC Platform application server.

<#> is the number of the node or server within that node (for example, `OPNode1Server1`).

Collect log files and diagnostic data

You can use the LogCollector tool to collect log files and diagnostic data from the IBM OpenPages GRC Platform environment and from OpenPages databases.

The LogCollector tool collects log files and diagnostic data on an application server.

In a horizontal cluster environment, run the tool on each application server in your environment.

In a vertical cluster, with multiple application servers installed on the same machine, the tool gathers logs from all servers. The tool gathers logs from reporting servers only when they are installed on the same machine as one of the application servers. If the search server is also installed on the same machine, for example in a development environment, the tool also collects the search server logs.

The LogCollector tool is in the *<OP_HOME>*`/bin` directory.

The tool uses the following command options:

`--configuration` or `-c` to specify a configuration file path. If you do not include this option, the default is `LogCollector.xml`. Using `--configuration` or `-c` is optional.

Note: For all command options, the long name command option uses two hyphens (--), whereas the short name uses only 1 hyphen (-).

`--database` or `-d` to collect log and diagnostic data from only the database.

`--file` or `-f` to collect only log and diagnostic files.

`--property` or `-p` to set property values. Using `--property` or `-p` is optional.

You must include `-p` for each property that you use. For example, `-p DB_OP_USER` *`username`* `-p DB_OP_PASSWORD` *`password`*. The properties that you can use are:

Property	Description
DB_OP_USER	The OpenPages database user name
DB_OP_PASSWORD	The OpenPages database user's password
DB_TYPE	The database type. This value can be db2 or `oracle`.

Property	Description
DB_URL	The database JDBC URL.
BPM_HOME	The BPM home location.

`--target` or `-t` to specify a target package file. If you do not include this option, the default is `LogCollector_<timestamp>.zip`. Using `--target` or `-t` is optional.

`--help` or `-h` to display command help.

This video demonstrates how to collect log files:

https://youtu.be/81X6H0bSlDg

Example: Getting all information

1. Log in as the Super Administrator user.
2. Open a Command Prompt window.
3. Go to the *<OP_HOME>*`/bin` directory. For example, on Microsoft Windows operating systems, go to `C:\OpenPages\bin`. On UNIX operating systems, go to `/opt/OpenPages/bin`.
4. Enter the following command:

   On Microsoft Windows operating systems: `LogCollector.cmd`

   On UNIX operating systems: `./LogCollector.sh`

The tool generates a package file that is named `LogCollector_<timestamp>.zip` in the `C:\OpenPages\bin` directory or the `/opt/OpenPages/bin` directory.

Example: Specifying a target package file

1. Log in as the Super Administrator user.
2. Open a Command Prompt window.
3. Go to the *<OP_HOME>*`/bin` directory. For example, on Microsoft Windows operating systems, go to `C:\OpenPages\bin`. On UNIX operating systems, go to `/opt/OpenPages/bin`.
4. Enter the following command:

   On Microsoft Windows operating systems: `LogCollector.cmd -t LogCollector.zip`

   On UNIX operating systems: `./LogCollector.sh -t LogCollector.zip`

The tool generates a package file that is named `LogCollector.zip` in the `C:\OpenPages\bin` directory or the `/opt/OpenPages/bin` directory.

Example: Getting information from an IBM DB2 database

1. Log in as the Super Administrator user.
2. Open a Command Prompt window.
3. Go to the *<OP_HOME>*`/bin` directory. For example, on Microsoft Windows operating systems, go to `C:\OpenPages\bin`. On UNIX operating systems, go to `/opt/OpenPages/bin`.
4. Enter the following command:

   On Microsoft Windows operating systems: `LogCollector.cmd -d -p DB_TYPE db2 -p DB_URL jdbc:db2://localhost:50000/OPX -p DB_OP_USER openpage -p DB_OP_PASSWORD password`

On UNIX operating systems: `./LogCollector.sh -d -p DB_TYPE db2 -p DB_URL jdbc:db2://localhost:50000/OPX -p DB_OP_USER openpage -p DB_OP_PASSWORD password`

The tool generates a package file that is named `LogCollector_<timestamp>.zip` in the `C:\OpenPages\bin` directory or the `/opt/OpenPages/bin` directory.

OpenPages GRC Platform Standard Application Server log files

The IBM OpenPages GRC Platform Standard Application Server log files are located in *<OP_Home>* | `aurora` | `logs`. File names vary depending on your environment.

Log file names on IBM WebSphere Application Server

Log file names on the IBM WebSphere application server contain information to understand what occurs during startup and application usage.

Where <host_name> is the name of the IBM OpenPages GRC Platform application host.

<#> represents the number of the node and the number of the server within that node (for example, OPNode1Server1).

Table 174: 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 OpenPages GRC Platform application caches on the OpenPages server.
<host_name>-OPNode<#>Server<#>-aurora.log	Errors, exceptions, and informational messages written during OpenPages GRC Platform application use.
<host_name>-OPNode<#>Server<#>-auroratools.log	Errors, exceptions, and informational messages written during OpenPages GRC Platform application use that are invoked by OpenPages utilities. For example, Notification Manager, Object Manager, etc.

Deployment Manager (DMGR) Server log files

The Deployment manager server log files contain information about starting and stopping server components. It also provides log files for errors and the status of the J2EE resources that are being used.

Log folder location: *<OP_Home>* | `profiles` | `OpenPagesDmgr` | `logs` | `dmgr` where *<OP_Home>* is the location of the IBM OpenPages GRC Platform application. By default, this value is `c:\OpenPages` on Windows, and `/opt/OpenPages` on AIX.

Table 175: DMGR server log files and the information they contain

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 that are written by the underlying IBM WebSphere application server.

Table 175: DMGR server log files and the information they contain (continued)	
This log file...	**Contains this type of information...**
SystemOut.log	Log entries written by the underlying IBM WebSphere application server about the status of various J2EE resources being used.

Node agent log files

The node agent log files contain information about starting and stopping server components, errors, and the status of the J2EE resources that are being used.

Log folder location: *<OP_Home>*|`profiles`|<host_name>-Node1|`logs`|`nodeagent` where <host_name> is the name of the IBM OpenPages GRC Platform application server.

Table 176: Node agent log files and the information they contain	
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 log files

The application cluster member log files contain information about starting and stopping server components, errors, and the status of the J2EE resources that are being used.

Log folder location:

```
<OP_Home>|profiles|<host_name>-OPNode<#>|logs|<host_name>-OPNode<#>Server<#>
```

where <host_name> is the name of the IBM OpenPages GRC Platform application server.

<#> is the number of the node or server within that node (for example, `OPNode1Server1`).

Table 177: Application cluster member log files and the information they contain	
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.

Changing the size and number of backups of the aurora log file

An IBM OpenPages GRC Platform administrator can control the maximum size of the aurora log file and how many backup files are created when the file reaches its maximum size.

About this task

The default maximum file size of the `auroralogging.properties` is 1024 KB. The default number of backups is 10.

Procedure

1. Log on to the OpenPages application server.
2. Go to *<OP_HOME>* | `aurora` | `conf` where *<OP_HOME>* is the OpenPages installation location.

   The default *OP_HOME* location for AIX and Linux operating systems is `/opx/OpenPages`. The default *OP_HOME* location for the Microsoft Windows operating system is `C:\OpenPages`.
3. Back up the `auroralogging.properties` file.
4. Open the `auroralogging.properties` file with a text editor.
5. To change the maximum file size of the `auroralogging.properties` file, modify the `log4j.appender.FILE.MaxFileSize` property.

   For example, to change the maximum file size to 5120 KB, change the property to the following:

   ```
   log4j.appender.FILE.MaxFileSize=5120KB
   ```
6. To change the number of backups of the `auroralogging.properties` file, modify the `log4j.appender.FILE.MaxBackupIndex` property.

   For example, to change the number of backups to 20, change the property to the following:

   ```
   log4j.appender.FILE.MaxBackupIndex=20
   ```

Troubleshooting browser issues

If you have a problem with a browser, review these topics to determine whether a solution is available.

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. Restart the browser to effect the change.

Setting a session inactivity timeout value

The IBM OpenPages GRC Platform system will timeout a user session after a set period of browser inactivity.

You can modify the value of the inactivity timeout period for the application server and for the reporting server. In general, the timeout period for the IBM Cognos reporting server should be set to a value greater than the application server timeout period.

In this example, the IBM Cognos server inactivity timeout value is set to 90 minutes, and the application server timeout value is set to 60 minutes. If a user performs various tasks in the OpenPages GRC Platform application for 45 minutes, then returns to view a report, they will be able to do so without having to log on to the reporting server again. However, if the reporting server has a smaller session inactivity value set, such as 15 minutes, then that same user would be required to log on to the reporting server. By default, the IBM WebSphere Application Server has a 30-minute timeout period. The default timeout period for IBM Cognos is 5400 seconds (equivalent to 90 minutes).

Setting session inactivity timeout values in an IBM WebSphere environment
You can set session inactivity timeout values in an IBM WebSphere environment.

Before you begin

You can modify the value of the inactivity timeout period for the application server and for the reporting server. The timeout period for the IBM Cognos reporting server should be set to a value greater than the application server timeout period. For example, setting the IBM Cognos server inactivity timeout value to 90 minutes, and the application server timeout value to 60 minutes. The user can return to a report without logging on to the reporting server, if the user does this within the timeout value. However, if the reporting server has a smaller session inactivity value set, such as 15 minutes, the user would be required to log on to the reporting server. By default, the IBM WebSphere Application Server has a 30-minute timeout period. The default timeout period for IBM Cognos is 5400 seconds (equivalent to 90 minutes).

Procedure

1. Log on to the IBM OpenPages GRC Platform application server as a user with administrative permissions.
2. Stop all OpenPages GRC Platform services.
3. Navigate to the *<OP_Home>*/profiles/*<server_name>*-*<node>*/config/cells/OpenPagesCell/applications/op-apps.ear/deployments/op-apps/sosa.war/WEB-INF/ directory.

   Where: *<OP_Home>* is the location of the OpenPages GRC Platform application. By default, this is c:\OpenPages on Windows, and /opt/OpenPages on AIX. *<server_name>* is the name of the application server.
4. In a text editor, open the web.xml file and look for the following lines:

```
<!-- Set the default session timeout (in minutes) -->
<session-config>
<session-timeout>30</session-timeout>
</session-config>
```

5. Set the <session-timeout> parameter to the value in minutes.
6. Navigate to the *<OP_Home>*/profiles/OpenPagesDmgr/config/cells/OpenPagesCell/applications/op-apps.ear/deployments/op-apps/sosa.war/WEB-INF/ directory.
7. If this is a load-balanced environment, repeat this procedure for each application server in the load-balanced environment.
8. Restart all OpenPages GRC Platform services (see Chapter 20, “Starting and stopping servers,” on page 549) to effect the change.

Setting session inactivity timeout values for IBM Cognos
You can set a session inactivity timeout value for the IBM Cognos reporting server.

Procedure

1. Log on to the IBM Cognos server as a user with administrative permissions.
2. Go to the *<COGNOS_Home>* bin64 directory.

Table 178: Installation location of the IBM Cognos reporting server	
Operation system	**Installation location**
Windows	For example, *<COGNOS_Home>* is `C:\Program Files\ibm\cognos\analytics`
AIX and Linux	For example, *<COGNOS_Home>* is `/opt/ibm/cognos/analytics`

3. Double-click the `cogconfigw.exe` file to start the IBM Cognos Configuration tool.
4. Expand **Security** and click **Authentication**.
5. Find the **Inactivity timeout in seconds** property and type a new value (in seconds) that is greater than the application server timeout value. For example, you could enter `7200` (equivalent to 120 minutes) if the application server timeout value is set to 90 minutes.
6. Save the configuration changes.
7. Restart the IBM Cognos server.

Setting the Cognos Application Firewall for browser security

To prevent URL redirection attacks in Cognos, enable Cognos Application Firewall 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/ibmcognos/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 *Cognos Analytics V11.0 Installation and Configuration Guide*, Configuration options chapter, section "Configure IBM Cognos 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 OpenPages 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 previously) 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 or Linux shell.

b) Navigate to the *<COGNOS_HOME>*|`bin64` or *<COGNOS_HOME>*|`bin` directory. where *<COGNOS_HOME>* is the installation location of the Cognos application.

c) Execute the following command:

Windows:
```
cogconfig.bat
```
AIX and Linux:
```
./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.

Browser display issues and Internet Explorer

If the text zoom feature of Microsoft Internet Explorer is used, scrollbars may appear around some sections of the IBM OpenPages GRC Platform application.

To avoid this issue, reduce your zoom level to a point where the scrollbars disappear.

Internet Explorer security issues and running reports

Depending on how Internet Explorer browser security is configured on client machines, Cognos reports may not launch successfully from the IBM OpenPages GRC Platform application user interface.

If a client machine using the Internet Explorer browser is unable to run Cognos reports from the OpenPages GRC Platform application user interface, then do the following:

- Add each reporting server to the **Trusted sites** zone in Internet Explorer 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 help.

Custom helpers and Internet Explorer 11

If you have custom helpers that do not work in Internet Explorer 11, you can force the page into behaving as if it is in an older version of IE.

About this task

Insert a meta tag like the following:

```
<meta http-equiv="X-UA-Compatible" content="IE=9" />
```

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 Chapter 13, “Localizing text,” on page 277.

Browser best practices

An IBM OpenPages GRC Platform browser session is active until one of three conditions is met.

- The user logs out of the OpenPages GRC Platform application.
- The session expires.
- The browser instance is closed.

The following are some suggested best practices for enhancing browser security that the users should be aware of:

- Logging off from OpenPages GRC Platform after they finish their work, and closing the browser window to ensure that no sensitive information is stored in the browser cache.
- Blocking their computers from external use when the users are not physically present - either by keeping their computers on stand-by or by locking their accounts.
- Copying (not clicking) a link to the 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 that is based on commonly known levels of inactivity for their organization. For more information, see “Setting a session inactivity timeout value” on page 543.
- Configuration of the **Cross-site Scripting Filter** setting to check all HTTP GET requests sent to the OpenPages application server.

Chapter 20. Starting and stopping servers

You can start and stop the IBM OpenPages GRC Platform application servers, the database server, the Cognos server, and the search server.

Starting application servers

You can start IBM OpenPages GRC Platform in Windows, AIX, and Linux environments.

In a Windows environment, the services that are required to start the OpenPages GRC Platform application servers can be configured to start automatically.

In an AIX and Linux environment, you manually run scripts to start the OpenPages GRC Platform application servers.

Important:

- Start the deployment manager first:
  - On Windows: start the IBMWAS<*version*>Service - <*OpenPagesdmgr-name*> service
  - On Linux or AIX: run the `startManager` script

  Then run the other services and 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 a cluster member.

Microsoft Windows services

For the IBM OpenPages GRC Platform application to run, all of the required Microsoft Windows services must be started and the services of supporting applications must be running.

Note: This information applies only to Windows environments.

Table 179: Service descriptions

Service Name	Description
IBMWAS<*version*>Service - <*OpenPages-dmgr-name*>	Starts or stops the OpenPages deployment manager service. **Note:** In a horizontal-cluster or shared-cell environment, cluster members might not have an <*OpenPages-dmgr-name*> service.
IBMWAS<*version*>Service - <*OpenPages-node-name*>	Starts or stops an OpenPages node service.
IBMWAS<*version*>Service - <*OpenPages-node-server-name*>Server<*#*>	Starts or stops an OpenPages application server cluster member. In a clustered environment, the number for each cluster member increments by 1.

Microsoft Windows commands

In a Microsoft Windows environment, IBM OpenPages GRC Platform includes a number of commands to initiate and launch the application environment.

The application runs only if all of the services are started and all of the services for all supporting applications are running.

Note: These commands can be run individually or you can use wrapper commands to start and stop OpenPages GRC Platform.

The following table lists the commands required to start and stop the application.

Table 180: OpenPages GRC Platform commands on Windows

Script Name	Description
startManager.bat	Starts the OpenPages Deployment Manager.
startNode.bat	Starts the OpenPages node agent.
startServer.bat	Starts the OpenPages application server.
stopManager.bat	Stops the OpenPages Deployment Manager.
stopNode.bat	Stops the OpenPages node agent.
stopServer.bat	Stops the OpenPages application server.
startAllServers.bat	Starts all OpenPages services in the correct sequence.
stopAllServers.bat	Stops all OpenPages services in the correct sequence.

AIX and Linux scripts

In the AIX and Linux environments, IBM OpenPages GRC Platform includes a number of scripts to initiate and launch the application environment.

The application runs only if all of the services are started and all of the services for all supporting applications are running.

Note: These scripts can be run individually or you can use wrapper scripts to start and stop OpenPages GRC Platform.

The following table lists the scripts required to start and stop the application.

Table 181: OpenPages GRC Platform scripts on AIX and Linux

Script Name	Description
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.
startAllServers.sh	Starts all OpenPages services in the correct sequence.
stopAllServers.sh	Stops all OpenPages services in the correct sequence.

Determining application readiness

This procedure lets you determine whether the application is ready to be accessed after starting up servers.

Procedure

1. Open the log file specified in the following table.

Table 182: Log files and their locations		
If this...	**Navigate to this folder...**	**View this log file...**
Windows, AIX, and Linux	*<OP_HOME>*|profiles|*<OpenPages-node-name>*|logs|*<OpenPages-node-server-name>*Server*<#>*	startServer.log

   Where

   <OP_HOME> represents the installation location of the OpenPages GRC Platform application.

   <OpenPages-node-name> is the name of the node in which the servers run.

   *<OpenPages-node-server-name>*Server *<#>* is the name of the current server within the *<OpenPages-node-name>* node that the current server is in, and *<#>* is the number of the server within that node.
2. Scroll to the end of the log file and search for a message stating that the server is "open for e-business; process id is *<process-id>*". If this line appears, the server is running in production mode and the application is ready to be accessed.

Automatically starting application servers in Windows

By default, all IBM OpenPages GRC Platform services are configured as `Manual` (they do not start upon reboot).

You can configure all OpenPages GRC Platform 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 GRC Platform services start.

Starting all application services in Windows using a script

The `StartAllServers.cmd` script included with IBM OpenPages GRC Platform starts all OpenPages services in the proper sequence.

Note: This information applies only to Microsoft Windows environments.

Procedure

1. Log on to the OpenPages GRC Platform 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 GRC Platform application. By default, this is: `c:\OpenPages`.

   b) Run the following command to start the OpenPages GRC Platform services:

      ```
      StartAllServers.cmd
      ```

      When all services have been started, the Command Prompt window closes.

Starting application services individually using Windows services

In the Windows environment, you start the IBM OpenPages GRC Platform application by starting the required OpenPages services.

Note: This information applies only to Windows environments.

Procedure

1. Log on to the OpenPages GRC Platform application server as a user with administrative privileges.
2. Click the Windows **Start** menu and select **All Programs**.
3. From the **Administrative Tools** list, click **Services**.
4. Start the IBMWAS*<version>*Service - *<OpenPages-dmgr-name>* service, if present.
5. Start the IBMWAS*<version>*Service - *<OpenPages-node-name>* service.
6. Start the IBMWAS*<version>*Service - *<OpenPages-node-server-name>*Server*<#>* services, where *<#>* represents the number of the cluster member.

   Note: If there is more than one cluster member on the current system, you must start the service (*<OpenPages-node-server-name>*Server*<#>*) for each cluster member in sequence.

   When the services are starting, Windows Services may indicate that the services have started, but background OpenPages processes may still be running. It might take a few minutes for the OpenPages services to be operational.

Starting all application servers in AIX and Linux using a script

The `startAllServers.sh` script included with IBM OpenPages GRC Platform will start all OpenPages services in the proper sequence.

Note: This information applies only to AIX and Linux environments.

Procedure

1. Log on to the OpenPages GRC Platform application server as a user with administrative privileges.
2. Open an AIX or Linux shell window.
3. Go to the *<OP_HOME>*`/bin` directory.
4. Run the following script to start OpenPages GRC Platform services:

```
./startAllServers.sh
```

Starting application servers in AIX and Linux individually using scripts

Use the following steps to start the IBM OpenPages GRC Platform services manually. In the AIX and Linux environments, you run a set of scripts to start the OpenPages application.

Note: This information applies only to AIX and Linux environments.

Procedure

1. Log on to the OpenPages GRC Platform application server as a user with administrative privileges.
2. Use an AIX or Linux shell to navigate to the *<DMGR profile directory>*`/`*<OpenPages-dmgr-name>*`/bin directory`, where *<DMGR profile directory>* is the same directory as the one provided on the installer's Deployment Manager card.

3. Enter the following command to launch a script that starts the OpenPages GRC Platform Deployment Manager:

```
./startManager.sh
```

4. After the script completes successfully, navigate to <*DMGR profile directory*>/<*OpenPages-dmgr-name*>/bin, where <*DMGR profile directory*> is the same directory as the one provided on the installer's Deployment Manager card.
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 <OpenPages-node-server-name>Server<#>
```

Where <OpenPages-node-server-name> is the name of the current server within the <OpenPages-node-name> node that the current server is in, and <#> is the number of the server within that node. For example, OpenPagesNodeServerServer1.

Note: If there is more than one managed server on the current system, you must run the start script (./startServer.sh <*OpenPages-node-server-name*>Server<#>) for each managed server in sequence, starting with server number 1, then server number 2, and so on.

Start or stop the global search services

You can start and stop the global search services by using operating system services or by using scripts.

Note: Do not combine the two methods. If you start global search as a Microsoft Windows service, for example, stop global search by stopping the Windows service.

Starting the global search services by using a script

You can start the global search services by running a script from a command line.

Before you begin

On the Windows operating system, disable the Microsoft Windows service that is called **IBM OpenPages GRC - Global Search service**, if it is enabled. Otherwise, the StartSearchServer.cmd script interferes with the Windows services.

Make sure that the database server is reachable and is running. Otherwise, the search services will not connect and will not start.

Procedure

1. Start the search services:
   - For Windows, at a command prompt enter the following commands:

     ```
     cd <SEARCH_HOME>\opsearchtools\
     StartSearchServer.cmd
     ```

   - For UNIX, at a command line, enter the following commands:

     ```
     cd <SEARCH_HOME>/opsearchtools/
     ./StartSearchServer.sh
     ```

2. Open a browser and point to your search server at ports 8983 and 8985. Make sure that the Solr search platform can be reached.
   For example, http://<*search-server*>:8983/ and http://<*search-server*>:8985/.

   If the verification fails, repeat the preceding step.
3. Log on to IBM OpenPages GRC Platform as an administrator.
4. Click **Administration** > **Global Search** > **Enable**.

Stopping the global search services by using a script

You can stop the global search services by running a script from a command line.

Before you begin

On the Windows operating system, disable the Microsoft Windows service called **IBM OpenPages GRC - Global Search service**, if it is enabled. Otherwise, the `StopSearchServer.cmd` script interferes with the Windows services.

Procedure

1. Log on to IBM OpenPages GRC Platform as an administrator.
2. Click **Administration** > **Global Search** > **Disable**.
3. Stop the search services:
   - For Windows, at a command prompt, enter the following commands:

     ```
     cd <SEARCH_HOME>\opsearchtools\
     StopSearchServer.cmd
     ```

   - For UNIX, at a command line, enter the following commands:

     ```
     cd <SEARCH_HOME>/opsearchtools/
     ./StopSearchServer.sh
     ```

4. For either Windows or UNIX, verify that global search is fully stopped.
   a) In the directory *<SEARCH_HOME>*`/opsearchtools/`, examine the files `opsearchtool_openpages.state` and `opsearchtool_folderacl.state` and verify that the PID value is `-1`.
   b) Open a browser and point to your search server at ports 8983 and 8985. Make sure that the Solr search platform cannot be reached.
   For example, `http://`*<search-server>*`:8983/` and `http://`*<search-server>*`:8985/`.

   If the stop verification fails, repeat the preceding step and then follow the steps in “ Forcing a reset of global search” on page 792.

Starting the global search services on Windows

You can start global search as a Microsoft Windows service. The service is called **IBM OpenPages GRC - Global Search**.

About this task

By default, the service is set to start manually, but you can change the service to start automatically.

Note: Make sure that the database server is reachable and is up and running. Otherwise, the search services will not connect and will not start.

Procedure

1. Log on to the search server as a user with administrative privileges.
2. Open the **Services** snap-in (`services.msc`).
3. Locate the service that is called **IBM OpenPages GRC - Global Search**.
4. Click **Start**.
5. If you want the service to start automatically when Windows starts, change the **Startup Type** to **Automatic**.
6. Open a browser and point to your search server at ports 8983 and 8985. Make sure that the Solr search platform can be reached.
   For example, `http://`*<search-server>*`:8983/` and `http://`*<search-server>*`:8985/`.

If the verification fails, repeat the preceding step.

7. Log on to IBM OpenPages GRC Platform as an administrator.
8. Click **Administration** > **Global Search** > **Enable**.

Starting the global search services on Linux or AIX

You can start global search as a service.

About this task

Use the steps in this topic as a guide. Depending on your environment and organization policies, you might decide to use a different method to set up the search service. If you want to use a different method, open the `openpages-search` file and check the commands, and the order of the commands. Modify the commands to meet the needs of your environment.

Note: Make sure that the database server is reachable and is up and running. Otherwise, the search services will not connect and will not start.

Procedure

1. Log on to the search server.
2. Open a shell as the root user.
3. Copy the *<SEARCH_HOME>*`/opsearchtools/openpages-search` file to the `/etc/init.d/` directory.
4. Copy the *<SEARCH_HOME>*`/opsearchtools/openpages-searchcfg` file to the `/etc/sysconfig/` directory.
5. Set the execution permission on the `openpages-search` file by running the following command: `chmod +x /etc/init.d/openpages-search`
6. If you want the service to start automatically when the system restarts, run the following commands:

```
chkconfig --add openpages-search
chkconfig openpages-search on
service openpages-search start
```

7. Start the global search services by running the following command: `service openpages-search start`
8. Open a browser and point to your search server at ports 8983 and 8985. Make sure that the Solr search platform can be reached.
   For example, `http://`*<search-server>*`:8983/` and `http://`*<search-server>*`:8985/`.

   If the verification fails, repeat the preceding step.
9. Log on to IBM OpenPages GRC Platform as an administrator.
10. Click **Administration** > **Global Search** > **Enable**.

Stopping the global search services

If global search is running as a service, you can use the operating system to stop the global search services.

About this task

If you used the `StartSearchServer.sh|.cmd` script to start the global search services, use the `StopSearchServer.sh|.cmd` script to stop the services. For more information, see "Stopping the global search services by using a script" on page 554.

Procedure

1. Log on to IBM OpenPages GRC Platform as an administrator.
2. Click **Administration** > **Global Search** > **Disable**.

3. Log on to the search server as a user with administrative privileges.
4. Stop the search services.

   On Windows:

   a. Open the **Services** snap-in (`services.msc`)

   b. Locate the service that is called **IBM OpenPages GRC - Global Search**.

   c. Click **Stop**.

   On Linux or AIX, run the following command:

   ```
   service openpages-search stop
   ```

5. Verify that global search is fully stopped.

   a) In the directory *<SEARCH_HOME>*`/opsearchtools/`, examine the files `opsearchtool_openpages.state` and `opsearchtool_folderacl.state` and verify that the PID value is `-1`.

   b) Open a browser and point to your search server at ports 8983 and 8985. Make sure that the Solr search platform cannot be reached.
   For example, `http://`*<search-server>*`:8983/` and `http://`*<search-server>*`:8985/`.

   If the stop verification fails, repeat the preceding step and then follow the steps in “ Forcing a reset of global search” on page 792.

Stopping application servers

You can stop the IBM OpenPages GRC Platform application server in the Windows, AIX and Linux environments as required.

IBM WebSphere Application Server global security is enabled by default on the application servers. When stopping an application server, you must provide the WebSphere administrative user name and password as arguments to all stop scripts on all operating systems.

Stopping the application server prevents IBM OpenPages GRC Platform from being accessed.

Important: If you are running OpenPages GRC Platform in a load-balanced environment, stop the server on each cluster member first before stopping the cluster administrator.

Stopping application servers in a Windows environment

In a Windows environment, all IBM OpenPages GRC Platform services can be configured to stop automatically or you can stop the services manually, using one of the following three methods.

Stopping the application server prevents IBM OpenPages GRC Platform from being accessed.

Important: If you are running OpenPages GRC Platform in a load-balanced environment, stop the server on each cluster member first before stopping the cluster administrator.

Automatically stopping application servers in Windows

Windows automatically and gracefully stops the IBM OpenPages GRC Platform application when a server shuts down.

Note: This information applies only to Windows environments.

Stopping the application server prevents the OpenPages application from being accessed.

Important: If you are running OpenPages GRC Platform in a load-balanced environment, you must stop the server on each cluster member first before stopping the cluster administrator.

Stopping all application services in Windows using a script

The `StopAllServers.cmd` script included with IBM OpenPages GRC Platform will stop all OpenPages services in the proper sequence.

Stopping the application server prevents the OpenPages application from being accessed.

Important: 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.

Procedure

1. Log on to the OpenPages GRC Platform application server as a user with administrative privileges.
2. Launch a Command Prompt window (using the **Run as Administrator** option).
3. Navigate to the *<OP_HOME>*`\bin` directory.
4. Enter the following command to launch a script that stops the OpenPages services:

```
StopAllServers.cmd <username> <password>
```

   Where <username> and <password> are the administrative user name and password for IBM WebSphere Application Server.

   When all services have been stopped, the Command Prompt window closes.

Stopping application services individually using Windows services

You can stop the IBM OpenPages GRC Platform application without shutting down or rebooting the computer.

Stopping the application server prevents the application from being accessed.

Important: 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.

Use the following steps to stop OpenPages services manually.

Important: Stopping the OpenPages GRC Platform Admin service before you stop each cluster member causes 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 GRC Platform application by stopping the required OpenPages services.

Procedure

1. Log on to the OpenPages GRC Platform 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 IBMWAS*<version>*Service - *<OpenPages-node-server-name>*Server*<#>* services.
5. Stop the IBMWAS*<version>*Service - *<OpenPages-node-name>* service.
6. Stop the IBMWAS*<version>*Service - *<OpenPages-dmgr-name>* service, if present.

Results

When the services are stopped successfully, the OpenPages application is properly shut down.

Stopping all application servers in AIX and Linux using a script

The `stopAllServers.sh` script included with IBM OpenPages GRC Platform stops all OpenPages services in the proper sequence.

Stopping the application server prevents the application from being accessed.

Important: If you are running OpenPages GRC Platform in a load-balanced environment, you must stop the server on each cluster member first before stopping the cluster administrator.

Procedure

1. Log on to the OpenPages GRC Platform application server as a user with administrative privileges.
2. Use an AIX or Linux shell to navigate to the *<DMGR profile directory>*/*<OpenPages-dmgr-name>*/bin directory, where *<DMGR profile directory>* is the same directory as the one provided on the installer's Deployment Manager card.
3. Enter the following command to launch a script that stops OpenPages GRC Platform services:

```
./stopAllServers.sh <username> <password>
```

Where *<username>* and *<password>* are the administrative user name and password for the IBM WebSphere Application Server.

Stopping application servers in AIX and Linux individually using scripts

In the AIX and Linux environments, you run a set of scripts to stop the IBM OpenPages GRC Platform application.

Stopping the application server prevents the application from being accessed.

Important: 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.

Procedure

1. Log on to the OpenPages GRC Platform application server as a user with administrative privileges.
2. Go to the *<OP_HOME>*/profiles/<OpenPages-node-name>/bin directory.
3. 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 -username <username> -password <password>
<OpenPages-node-server-name>Server<#>

./stopNode.sh -username <username> -password <password>
```

Where <OpenPages-node-server-name> is the name of the current server within the <OpenPages-node-name> node that the current server is in, and <#> is the number of the server within that node. For example, OpenPagesNodeServerServer1.

Where <username> and <password> are the administrative user name and password for IBM WebSphere Application Server.

If there is more than one managed server on the current system, you must run the stop server script (./stopServer.sh *<OpenPages-node-server-name>*Server*<#>*) for each managed server before running the stop node agent script (./stopNode.sh). The managed servers can be stopped in any order.

4. After the scripts complete successfully, go to the *<DMGR profile directory>*/*<OpenPages-dmgr-name>*/bin directory where *<DMGR profile directory>* is the same directory as the one provided on the installer's Deployment Manager card.
5. Enter the following command to launch a script that stops the OpenPages GRC Platform Deployment Manager:

```
./stopManager.sh -username <username> -password <password>
```

Where <username> and <password> are the administrative user name and password for the IBM WebSphere Application Server.

When the script completes successfully, the OpenPages application is properly shut down.

Starting and stopping the Oracle database server in a Windows environment

You can start or stop database services using Windows services that are associated with the IBM OpenPages GRC Platform Oracle database instance.

Note: This information applies only to Windows environments.

Table 183: OpenPages GRC Platform Oracle services on Windows

Service Name	Description
OracleOraDB12Home1TNSListener	Runs the Oracle Database listener service that 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, for example OP.
OracleVssWriter<SID>	Where <SID> represents the database instance identifier, for example OP.

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 previous table, do the following:
   - To start the server, right-click the service name and select **Start**.
   - To stop the server, right-click the service name and select **Stop**.

Starting and stopping the Oracle database server in an AIX and Linux environment

Use the following steps to start or stop the Oracle database server.

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>/bin
   ```

   For example: `/opt/oracle/app/product/12.1/dbhome_1/bin`.
3. To start Oracle, do the following steps.
   a) Log in to SQL*Plus.

   ```
   sqlplus / as sysdba
   ```

b) Run the following command to start Oracle.

```
startup
```

4. To stop Oracle, do the following steps.
   a) Log in to SQL*Plus.

```
sqlplus / as sysdba
```

   b) Run the following command to start Oracle.

```
stop immediate
```

Starting and stopping the Cognos services

There are different procedures to start or stop the Cognos services in the Windows, AIX and Linux environments. The services are the `IBM Cognos` service and the `OpenPages Framework Model Generator` service

These procedures are:

- “Using the IBM Cognos configuration tool to start and stop the IBM Cognos service” on page 560
- “Using the Windows operating system to start and stop the IBM Cognos service” on page 561
- “Using the AIX or Linux operating system to start and stop IBM Cognos service” on page 561
- “Starting and stopping the OpenPages GRC Platform Framework Model Generator service on Windows” on page 561
- “ Starting and stopping the OpenPages GRC Platform Framework Model Generator service on AIX or Linux” on page 561

Using the IBM Cognos configuration tool to start and stop the IBM Cognos service

You can use the IBM Cognos Configuration tool to start or stop the `IBM Cognos` service.

Note: The IBM Cognos Configuration tool displays the status of the start-up, which can be helpful with troubleshooting, if necessary.

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 or Linux shell, and navigate to the *<COGNOS_HOME>*`/bin64` directory.

   <COGNOS_HOME> represents the installation location of the Cognos application. By default, this is:

   Windows
   `cogconfig.bat`

   AIX and Linux
   `./cogconfig.sh`

   b) Execute one of the following commands to open the tool:
3. Do one of the following:
   - To 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 service has already started.
   - To stop the service, click **Actions** | **Stop**.

Using the Windows operating system to start and stop the IBM Cognos service

Use the following steps to start or stop the IBM Cognos 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 start the server, right-click the IBM Cognos service and select **Start**.
   - To stop the server, right-click the IBM Cognos service and select **Stop**.

Using the AIX or Linux operating system to start and stop IBM Cognos service

Use the following steps to start or stop the IBM Cognos service in an AIX or Linux 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 or Linux shell and navigate to the bin directory as follows:
   <COGNOS_HOME>/bin64

   Where
   <COGNOS_HOME> is the installation location of the Cognos application.
3. Do one of the following:
   - To start the service, enter the following command: `./cogconfig.sh -s`
   - To stop the service, enter the following command: `./cogconfig.sh -stop`

Starting and stopping the OpenPages GRC Platform Framework Model Generator service on Windows

Use the following steps to start or stop the IBM OpenPages GRC Platform Framework Model Generator service in a Microsoft Windows environment.

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 start the server, right-click the IBMOpenPagesFrameworkModelGenerator service and select **Start**.
   - To stop the server, right-click the IBMOpenPagesFrameworkModelGenerator service and select **Stop**.

Starting and stopping the OpenPages GRC Platform Framework Model Generator service on AIX or Linux

Use the following steps to start or stop the IBMOpenPagesFrameworkModelGenerator service in an AIX or Linux environment.

Procedure

1. Log on to the reporting server as a non-root user with administrative privileges.

2. Open an AIX or Linux shell as a user with administrative privileges and navigate to the following directory:

   ```
   <CommandCenter_Home>/wlp/bin
   ```

   Where *<CommandCenter_Home>* is the installation location ofIBM OpenPages CommandCenter. By default, this is: `/opt/OpenPages/CommandCenter`.
3. To start the service, run the following command.

   ```
   server start IBMOpenPagesFrameworkModelGenerator
   ```
4. To stop the service, run the following command.

   ```
   server stop IBMOpenPagesFrameworkModelGenerator
   ```

Chapter 21. Comparing IBM OpenPages GRC Platform environments

You can find differences between two environment configuration XML files by using **Compare Environments**. Use Compare Environments to identify and resolve issues before you migrate configurations from one environment to another.

Compare Environments compares XML files that you generate in each environment. You can generate the XML files by using Export Configuration or by using ObjectManager. Compare Environments looks at the XML files and identifies any differences in the files. Compare Environments also uses validation rules to check the XML files for any errors and for changes that might cause issues during a migration.

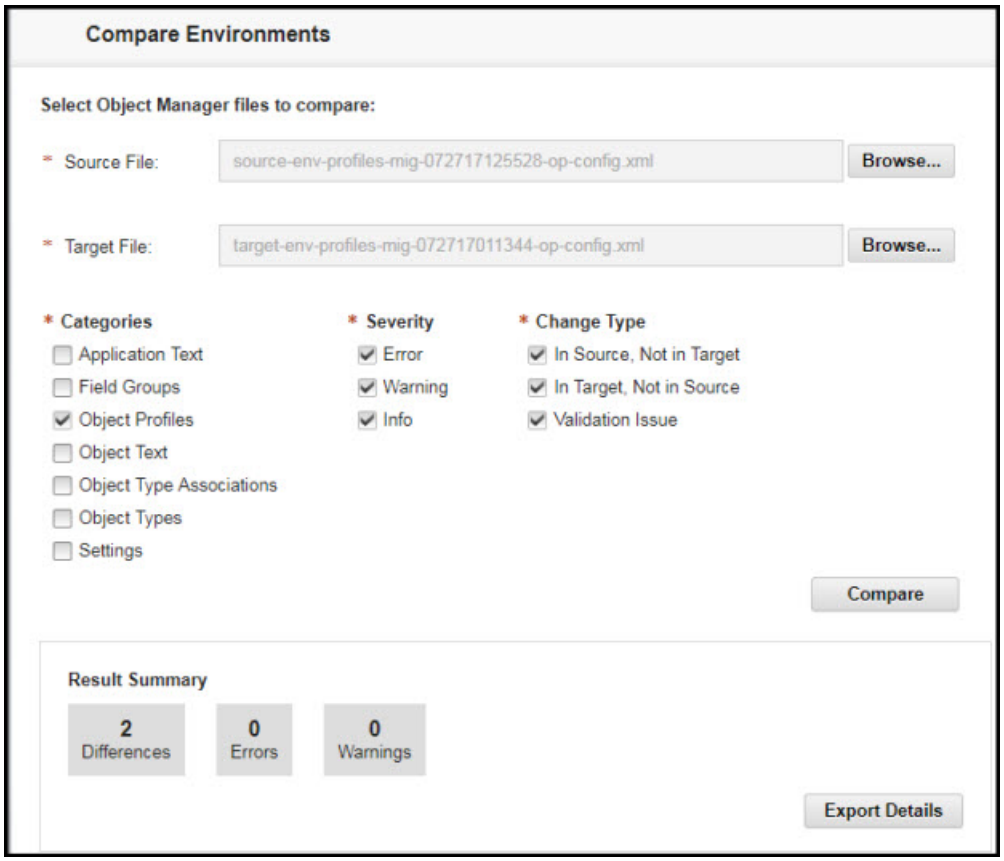
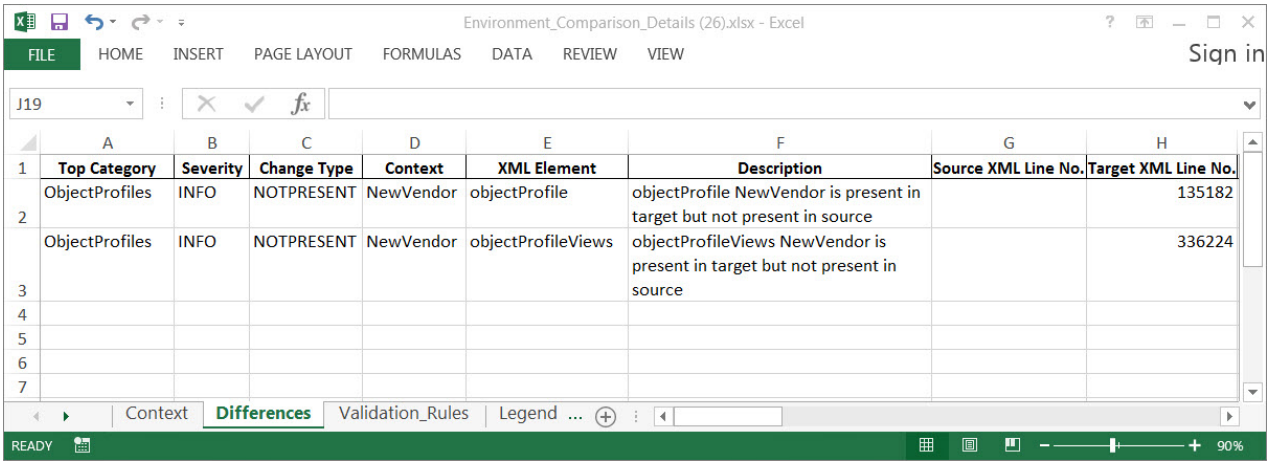


Figure 19: Comparing profiles in a source and target environment



	A	B	C	D	E	F	G	H
1	Top Category	Severity	Change Type	Context	XML Element	Description	Source XML Line No.	Target XML Line No.
2	ObjectProfiles	INFO	NOTPRESENT	NewVendor	objectProfile	objectProfile NewVendor is present in target but not present in source		135182
3	ObjectProfiles	INFO	NOTPRESENT	NewVendor	objectProfileViews	objectProfileViews NewVendor is present in target but not present in source		336224
4								
5								
6								
7								

Figure 20: Results of the comparison: A profile does not exist in the source environment

The source and target files can be from environments that are running different versions of IBM OpenPages GRC Platform. Further, you can run Compare Environments on a system that is running a version that is different from both the source and target environments.

Note: Compare Environments compares only the content of the XML files that you specify. It does not compare any other aspects of your source and target environments.

Compare Environments can use significant system resources. Follow these guidelines when you are using it:

- Do not run Compare Environments on production environments.
- Do not run Compare Environments on servers that are busy with other activities.
- The XML files that you want to compare might be very large. If so, the time it takes to upload the files to the system might take several minutes or longer. Consider this factor before using a connection with slow upload speeds.

Use the following process to compare environments:

- Decide what you want to compare.
- Generate an XML file in the source environment.
- Generate an XML file in the target environment.
- Use the filters on the **Compare Environments** page to filter on the configuration data that you want to compare.

  By using the filters, you can reduce the amount of time it takes to compare the XML files. Filters can also help you to focus on the results that you need by removing potentially distracting information from the results. Comparison results can include hundreds of thousands of rows.
- Run the comparison.
- Download the detailed results.
- Analyze the results.
- Fix any errors and review any warning messages.

When you compare environments, keep the following points in mind:

- Compare Environments uses the source environment file as the point of reference. If you reverse the source and target files, the results are different, and this is expected.
- Compare Environments ignores any data that it does not support.
- The source environment, the target environment, and the environment where you run Compare Environments can each have a different version of OpenPages installed.
- Currency fields are different from other fields. Currency fields have a different XML structure from other types of fields.

  - Currency fields are represented in the XML like a field group (by using the `bundleType` element).
  - Currency fields are implemented with a nested field group that contains the currency attributes, such as the exchange rate, base amount, local amount, currency code, base code, and so on. If Compare Environments finds differences in a currency field, it logs the change at both the currency field level and at the nested field group level.
- When Compare Environments finds an element that is missing from the source file or from the target file, it logs the difference at the level of that element only. Compare Environments does not log differences for the element's children.

  The only exception to this rule is for currency fields. If a currency field is missing, Compare Environments logs the missing field and its child field group.
- The line numbers that you see in the output might be different from what you expect to see based on the XML file. The line numbers that are shown in the output are the line numbers where the closing tags occur in the XML file. An element can span several lines, for example if the element has attributes on different lines.

  For example, the line number reported in the output for the following `Year` field is 83, the line on which the closing tag occurs.

```
81      <includedField name="Year"
82          readOnly="false"
83          required="false">
```

- If you added a custom object type in OpenPages, the object type definition in the XML file contains at least two `contentTypeRelationship` elements, attachment and association. These content type relationships are added by default. Compare Environments reports on these elements.

  For example, suppose that you added a custom object type in the source environment and it does not exist in the target environment. When you defined the custom object type, you set up a parent association. When you generate and compare the XML files, Compare Environments logs two information messages about object type associations: one about the parent object association that you added, and another about the attachment association, which was added by default.
- In certain cases, when you use the **Administration** pages, default configuration elements are created in the background. These changes might not be apparent in the user interface at the time.

  For example, when you view the details of a profile for the first time and add an included object type such as SOXBusEntity, default entries for the Overview navigation view are added automatically. If you export object profiles without making any additional changes, the XML file includes the additional elements for the Overview view in the object profile.

This video demonstrates how to use Compare Environments to identify and resolve issues before you migrate configurations from one environment to another:

https://youtu.be/knGObg_VGXs

Review configuration settings

Before you compare environments, review the configuration settings that impact the process to ensure that they meet your requirements.

Settings > Applications > Common > Max File Upload Size
: This setting specifies the maximum size of an upload. The limit is on the total upload size of both files. If your XML files are large, you might need to increase the value of this setting. Also, consider using the filters on the **Export Configuration** page to reduce the file size. Or, if you are using ObjectManager, change the ObjectManager properties to generate smaller files.

  After you change this setting, restart the application server. For more information, see "Configuring large files for upload" on page 327.

Settings > Platform > CompareEnvironments > Export Max Rows
This setting specifies the maximum number of rows that are exported in the detailed results spreadsheet. If you are working with large files, you might need to increase the value of this setting. If you do so, you might also need to increase the value of the Max Memory setting. For more information, see “Maximum number of rows to export from the Compare Environments tool” on page 345.

Settings > Platform > CompareEnvironments > Max Memory
This setting specifies the maximum Java heap size that can be used by Compare Environments. For more information, see “Java heap size for the Compare Environments tool” on page 345.

Supported items

Compare Environments supports the comparison of many configuration items. Compare Environments ignores any items that it does not support.

Compare Environments supports the following items:

- Object types, including object type associations (parent or child), associated field groups, and file type information
- Field groups
- Fields, including field types, display types, and display type attributes
- Computed field details, including equation, primary namespace, alternative namespaces, object ID, and reporting period ID
- Enumerated string values for enumerated string fields
- Object profiles, including object profile views
- Settings
- Object text
- Application text

For information about how items are represented in XML, export results from the Compare Environments tool and then click the **Legend** tab of the exported workbook.

Compare Environments does not support some items, for example:

- Filters
- Field dependencies
- Dependent picklists
- Workflows in IBM Business Process Manager
- Security (groups, users, role templates, custom security, security rules)
- Object resets
- Configuration settings for apps and features that have their own configuration pages, such as the approval app, IBM OpenPages Loss Event Entry, IBM Regulatory Compliance Analytics data import, IBM OpenPages Regulatory Compliance Management, and classifiers for cognitive services
- Questionnaire Assessments
- Triggers
- Custom query subjects
- JSPs
- For activity views, a maximum of three levels of associated object types is supported
- Instance data

Prepare the files to compare

To compare two environments, you need to export an XML file from each environment.

You can use Export Configuration or ObjectManager to export files from the source and target environments.

Export Configuration XML files might include other types of items in addition to the ones you selected for export. For example, if you export a profile, Export Configuration also exports items that the profile depends on, such as views.

Use the same method to generate the XML file for each environment whenever possible. If you use a different method for each file, the results include a larger number of differences than if you had used the same method for the two files. These additional differences are expected, since the XML files generated by Export Configuration and by ObjectManager can contain different levels of detail.

Preparing files by using Export Configuration

You can prepare the XML files to compare by using Export Configuration.

Procedure

1. Export configurations in the source environment.

   For more information, see "Exporting configuration items from the source environment" on page 583.

   The tool generates a `.jar` file.
2. Download the `.jar` file.
3. Decompress the `.jar` file.

   Note: You might need to change the extension to `.zip`, depending on the data extraction tool that you are using.
4. Go to the `loader-data` directory and locate the `openpages-env-mig-<timestamp id>-op-config.xml` file.
5. Give the file a meaningful name.
   For example, `source-openpages-env-mig-<timestamp id>-op-config.xml`
6. Repeat these steps in the target environment. Give the XML file a meaningful name such as `target-openpages-env-mig-<timestamp id>-op-config.xml`.

Preparing files by using ObjectManager

You can prepare the XML files to compare by using ObjectManager.

Procedure

1. In the source environment, go to the *<OP_HOME>*`/bin/` directory.
2. Edit the *<OP_HOME>*`/bin/ObjectManager.properties` file. Configure the areas that you want to export.
   - To export all configuration data, set the following setting to true:

     ```
     configuration.manager.migrate.configuration.objects=true
     ```

     This setting extracts more data than is supported by the Compare Environments tool. The Compare Environments tool ignores any data that is not supported.
   - To export all configuration data that **Compare Environments** supports, see "ObjectManager properties for comparing environments" on page 568.
   - To specify the configuration data that you want to export, look for the settings that begin with `configuration.manager.dump.*`

The `ObjectManager.properties` file contains over 45 settings of this type. For more information, see "Settings in the ObjectManager.properties file " on page 601.

To export data, change the value of a setting to true. For example, to export all fields and field groups, use the following setting:

```
configuration.manager.dump.bundle.type=true
```

For more information, see "Modifying the ObjectManager properties file" on page 601.

3. Save the `ObjectManager.properties` file.
4. Run the following command:

```
ObjectManager.sh d c <OP admin user> <OP admin user password>
   <output directory> <output file prefix>
```

The XML output file is created in the output directory that you specified and is named *<output file prefix>*`-op-config.xml`.

5. Repeat these steps in the target environment.

ObjectManager properties for comparing environments

If you want to export all of the configurations that Compare Environments supports, use the following settings in the *<OP_HOME>*`/bin/ObjectManager.properties` file.

```
configuration.manager.dump.modules=false
configuration.manager.dump.file.types=false
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=false
configuration.manager.dump.actors=false
configuration.manager.dump.actor.group.memberships=false
configuration.manager.dump.actor.object.profile.associations=false
configuration.manager.dump.admin.objectprofile.views=true
configuration.manager.dump.non.form.based.resources=false
configuration.manager.dump.form.based.content.types=true
configuration.manager.dump.form.based.resources=false
configuration.manager.dump.channels=false
configuration.manager.dump.resource.sets=false
configuration.manager.dump.associated.resources=false
configuration.manager.dump.rule.sets=false
configuration.manager.dump.rule.set.execute.sessions=false
configuration.manager.dump.registry=true
configuration.manager.dump.object.profiles=true
configuration.manager.dump.recursive.hierarchy=false
configuration.manager.dump.date.dimension.type=false
configuration.manager.dump.object.type.dimension=false
configuration.manager.dump.date.dimension.type.associations=false
configuration.manager.dump.locales=false
configuration.manager.dump.application.string.key.categories=true
configuration.manager.dump.application.string.keys=true
configuration.manager.dump.application.strings=true
configuration.manager.dump.recursive.hierarchy.strings=false
configuration.manager.dump.date.dimension.type.strings=false
configuration.manager.dump.object.type.dimension.strings=false
configuration.manager.dump.error.strings=false
configuration.manager.dump.object.strings=true
configuration.manager.dump.job.types=false
configuration.manager.dump.currency.exchange.rates=false
configuration.manager.dump.currencies=false
configuration.manager.dump.query.definitions=false
configuration.manager.dump.user.preferences=false
configuration.manager.dump.role.templates=false
configuration.manager.dump.role.administrators=false
configuration.manager.dump.role.assignments=false
configuration.manager.dump.field.dependency=false
configuration.manager.dump.field.dependency.picklist=false
configuration.manager.dump.subsystem.exclusion.fields=false
```

Comparing environments

You can compare environments to find differences between two environment configuration XML files.

Before you begin

You must have the **Compare Environments** application permission to see the **Compare Environments** menu item. The location of the permission in a role template is **All Permissions** > **SOX** > **Administration** > **Compare Environments**.

Prepare the XML files that you want to compare. For more information, see "Prepare the files to compare" on page 567.

Procedure

1. Log in as a user with the **Compare Environments** permission.
2. Click **Administration** > **Compare Environments**.
3. Select the XML file for the source environment.
4. Select the XML file for the target environment.
5. Choose the categories that you want to include.
6. Choose the severity levels that you want to include.
7. Select the types of changes you want to include:
   - **In Source, Not in Target**: Find items that exist in the source environment XML file and do not exist in the target.
   - **In Target, Not in Source**: Find items that exist in the target environment XML file and do not exist in the source.
   - **Validation Issue**: Find validation issues.
8. Click **Compare**.

   Depending on the size of the XML files, the options that you selected, and your upload connection speed, the process might take several minutes to complete.

   Important: Stay on the **Compare Environments** page until the process completes. If you leave the page, you will need to select the files again and re-run the comparison to get the results.
9. Click **Export Details**. Save or open the `.xlsx` file.
10. Analyze the results. For more information, see "Interpret results" on page 569.

Interpret results

When you export results from Compare Environments, you get a `.xlsx` file. The workbook provides details about the comparison, along with the results.

Context tab
Lists the options that you used to do the comparison.

Differences tab
Lists the differences that were found. Look for any errors or warnings.

Table 184: Descriptions of the columns on the Differences tab

Column	Description
Top Category	The overall category of the difference, error, or warning that was found.

Table 184: Descriptions of the columns on the Differences tab (continued)	
Column	**Description**
Severity	The severity of the issue. INFO: An information message only. No action is required. ERROR: An issue that must be fixed before you can use the XML files to migrate from the source to the target. WARNING: An issue that might impact migration. Investigate and make any changes that are needed.
Change Type	The type of issue that was found. ADD: An item exists in the source XML file but does not exist in the target XML file. When you migrate, the item will be added to the target environment. NOT PRESENT: An item exists in the target XML file but does not exist in the source XML file. UPDATE: An item exists in both the source and target, but a difference was found. When you migrate, the target environment will be updated with the value from the source XML file. REMOVE: An item exists in the target XML file but does not exist in the source XML file. When you migrate, the item will be removed from the target environment. CONFLICT: A validation issue was found in either the source or target XML file.
Context	The path to the XML element where the error, warning, or difference was found.
XML Element	The XML element that contains the error, warning, or difference.
Description	A description of the error, warning, or difference. You can find more information about errors and warnings on the **Validation_Rules** tab.
Source XML Line No.	The line number in the source XML file. If an element spans multiple lines, the tool reports the line number where the closing tag is located.
Target XML Line No.	The line number in the target XML file. If an element spans multiple lines, the tool reports the line number where the closing tag is located.
Attribute Changed	The name of the attribute that was changed.
Source Value	The value in the source XML file.
Target Value	The value in the target XML file.

Table 184: Descriptions of the columns on the Differences tab (continued)	
Column	**Description**
Context *n*	Details about where the error, warning, or difference was found. These columns parse the path in the Context column into individual elements. Each column contains an XML element and its value. For example, if an issue was found in a field, the **Context 1** column displays `bundleType: field_group_name` and the **Context 2** column displays `propertyType: field_name`.

Validation_Rules tab
Lists the rules that the tool uses to validate the source and target XML files.

Legend tab
Lists the configuration items that the tool compares and the name of the elements that represent them in the XML files.

If you want to migrate from the source environment to the target environment, fix any errors and review all warnings. Regenerate the XML files, and then run the Compare Environments tool again. Verify the results.

Errors, warnings, and how to fix them

When you run compare environments with the **Validation Issues** option selected, Compare Environments uses validation rules to check the XML files. If issues are found, it logs errors and warnings.

In many cases, an error or warning can be fixed in various ways. Analyze each error and warning to determine how to address it.

In some cases, you can resolve an issue by making a change in the source environment and then exporting a new XML file.

In other cases, the error or warning cannot be resolved by modifying the source environment. Instead, you can modify the source XML file to fix the error or warning manually.

- Edit the source XML file in a text editor to fix the error or warning.
- Run Compare Environments with the updated XML file to verify that the error or warning is fixed.

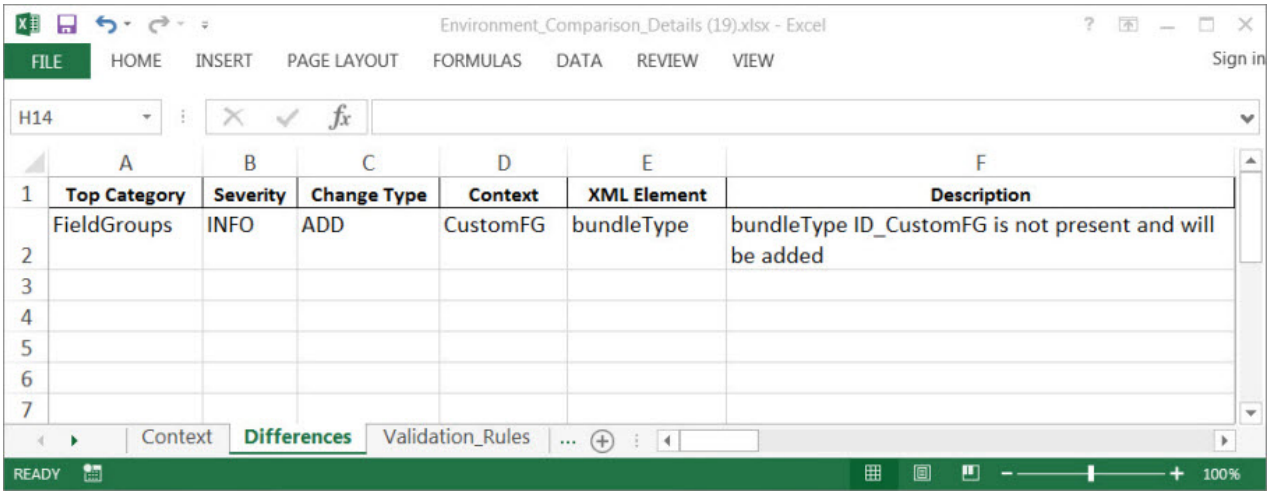
Important: The solutions that are described on the Validation_Rules tab for each error and warning are suggestions only.

Example: A field group exists in the source environment, but not in the target

Suppose that the source environment has a field group that is called `CustomFG`. The field group does not exist in the target environment.

You export field groups from each environment by using **Export Configuration**. You then compare the two XML files by using **Compare Environments**. You choose to compare all categories. You also choose to include errors, warnings, and information messages in the results.

In this case, the tool generates the following message:

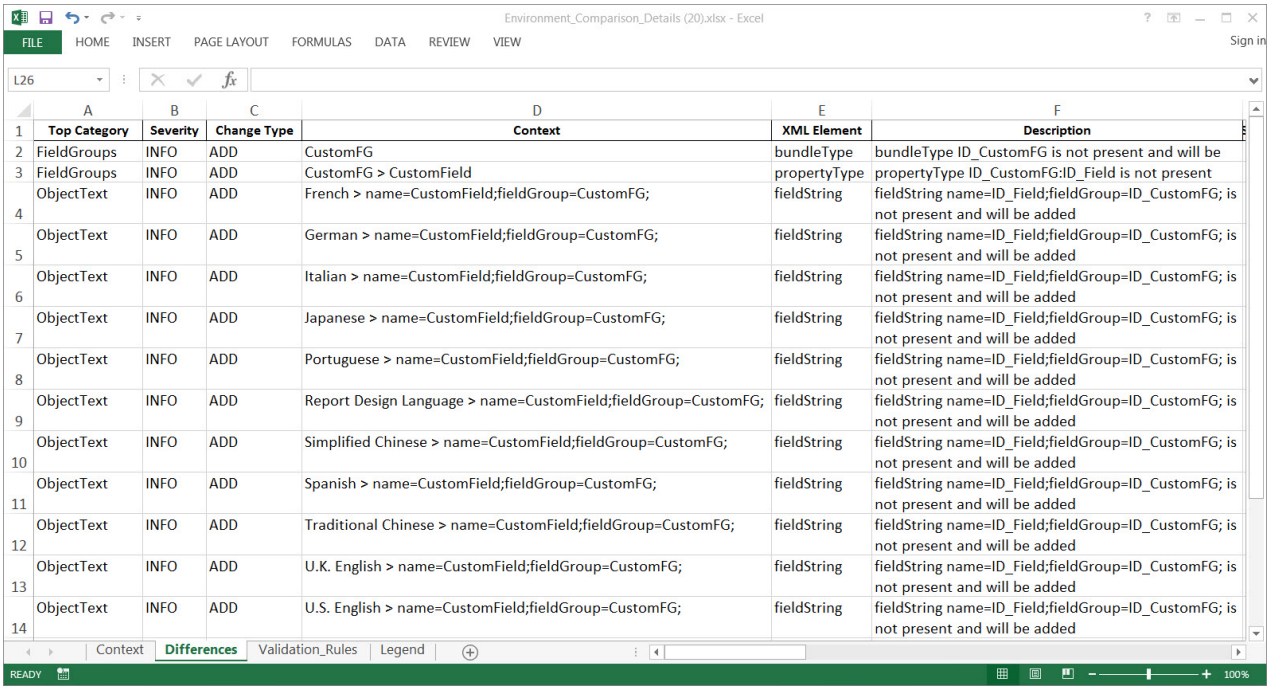


Top Category	Severity	Change Type	Context	XML Element	Description
FieldGroups	INFO	ADD	CustomFG	bundleType	bundleType ID_CustomFG is not present and will be added

Figure 21: Results of the export: A field group is not in the target environment

The `bundleType` message indicates that the field group that is called `CustomFG` is not in the target environment.

If you added fields to the `CustomFG` field group, you also see messages about the fields. For example, if the `CustomFG` field group has a field that is called `CustomField` and this field does not exist in the target, you see the following messages:



Top Category	Severity	Change Type	Context	XML Element	Description
FieldGroups	INFO	ADD	CustomFG	bundleType	bundleType ID_CustomFG is not present and will be
FieldGroups	INFO	ADD	CustomFG > CustomField	propertyType	propertyType ID_CustomFG:ID_Field is not present
ObjectText	INFO	ADD	French > name=CustomField;fieldGroup=CustomFG;	fieldString	fieldString name=ID_Field;fieldGroup=ID_CustomFG; is not present and will be added
ObjectText	INFO	ADD	German > name=CustomField;fieldGroup=CustomFG;	fieldString	fieldString name=ID_Field;fieldGroup=ID_CustomFG; is not present and will be added
ObjectText	INFO	ADD	Italian > name=CustomField;fieldGroup=CustomFG;	fieldString	fieldString name=ID_Field;fieldGroup=ID_CustomFG; is not present and will be added
ObjectText	INFO	ADD	Japanese > name=CustomField;fieldGroup=CustomFG;	fieldString	fieldString name=ID_Field;fieldGroup=ID_CustomFG; is not present and will be added
ObjectText	INFO	ADD	Portuguese > name=CustomField;fieldGroup=CustomFG;	fieldString	fieldString name=ID_Field;fieldGroup=ID_CustomFG; is not present and will be added
ObjectText	INFO	ADD	Report Design Language > name=CustomField;fieldGroup=CustomFG;	fieldString	fieldString name=ID_Field;fieldGroup=ID_CustomFG; is not present and will be added
ObjectText	INFO	ADD	Simplified Chinese > name=CustomField;fieldGroup=CustomFG;	fieldString	fieldString name=ID_Field;fieldGroup=ID_CustomFG; is not present and will be added
ObjectText	INFO	ADD	Spanish > name=CustomField;fieldGroup=CustomFG;	fieldString	fieldString name=ID_Field;fieldGroup=ID_CustomFG; is not present and will be added
ObjectText	INFO	ADD	Traditional Chinese > name=CustomField;fieldGroup=CustomFG;	fieldString	fieldString name=ID_Field;fieldGroup=ID_CustomFG; is not present and will be added
ObjectText	INFO	ADD	U.K. English > name=CustomField;fieldGroup=CustomFG;	fieldString	fieldString name=ID_Field;fieldGroup=ID_CustomFG; is not present and will be added
ObjectText	INFO	ADD	U.S. English > name=CustomField;fieldGroup=CustomFG;	fieldString	fieldString name=ID_Field;fieldGroup=ID_CustomFG; is not present and will be added

Figure 22: Results of the export: A field group and its fields are not in the target environment

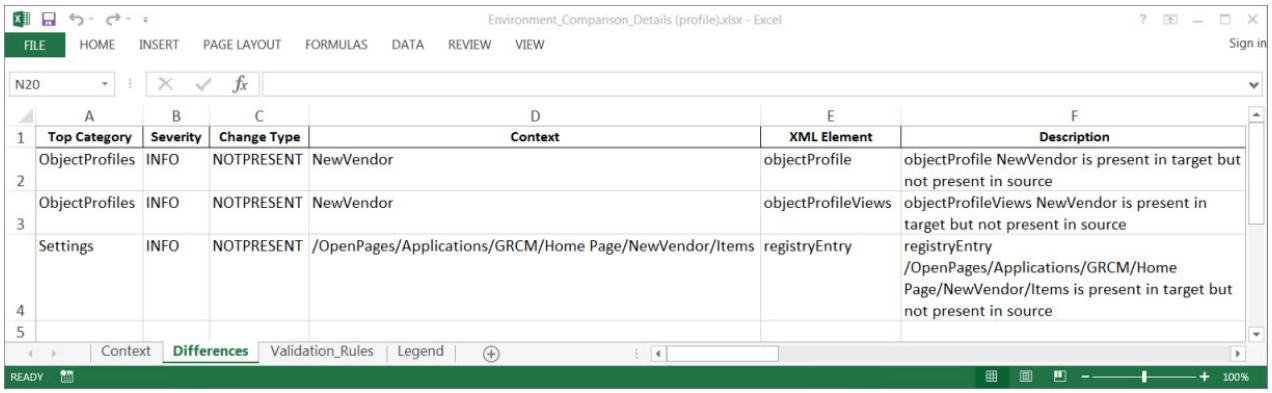
- The `bundleType` message indicates that the `CustomFG` field group is not in the target environment.
- The `propertyType` message indicates that the field that is called `CustomField` is not in the target environment.
- The `fieldString` messages are generated for each locale that is defined for the field called CustomField.

Example: A profile exists in the target environment, but not in the source

Suppose that the target environment has a profile that is called `NewVendor` that is based on the VRM Vendor profile. The NewVendor profile does not exist in the source environment.

You export object profiles from each environment by using **Export Configuration**. You then compare the two XML files by using **Compare Environments**. You choose to compare all categories. You also choose to include errors, warnings, and information messages in the results.

In this case, the tool generates the following messages:



	A	B	C	D	E	F
1	Top Category	Severity	Change Type	Context	XML Element	Description
2	ObjectProfiles	INFO	NOTPRESENT	NewVendor	objectProfile	objectProfile NewVendor is present in target but not present in source
3	ObjectProfiles	INFO	NOTPRESENT	NewVendor	objectProfileViews	objectProfileViews NewVendor is present in target but not present in source
4	Settings	INFO	NOTPRESENT	/OpenPages/Applications/GRCM/Home Page/NewVendor/Items	registryEntry	registryEntry /OpenPages/Applications/GRCM/Home Page/NewVendor/Items is present in target but not present in source
5						

Figure 23: Results of the export: A profile does not exist in the source environment

- The `objectProfile` message indicates that the profile that is called NewVendor does not exist in the source environment.
- When the NewVendor profile was created, a new view definition was created automatically. The `objectProfileViews` message indicates that this view definition does not exist in the source environment.
- When the NewVendor profile was created, a new registry setting was added automatically. The `registryEntry` message indicates that this setting does not exist in the source environment.

If the profile uses fields groups, fields, or other items that are not in the source environment, you see messages about these differences also.

Example: A custom object type exists in the target environment, but not in the source

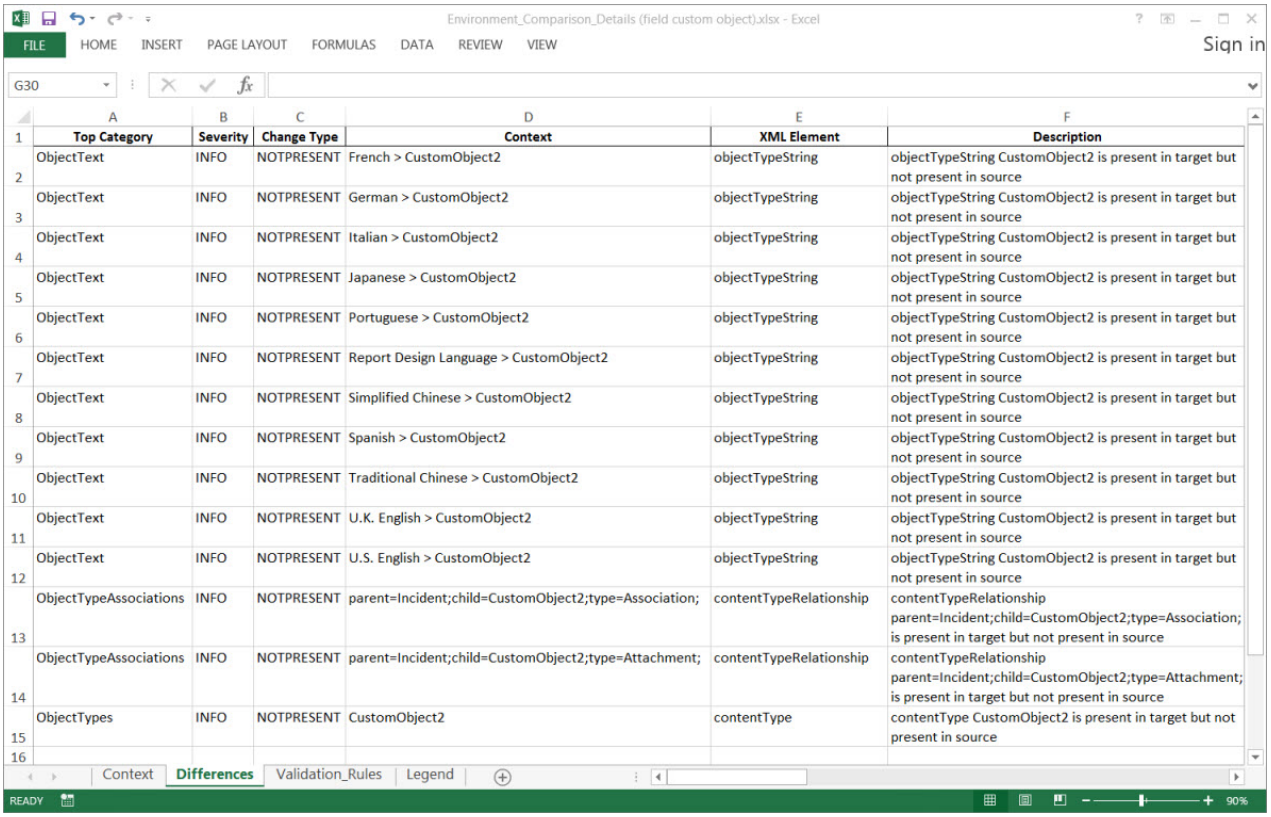
Suppose that the target environment has a custom object type that is not in the source environment.

The custom object has the following characteristics:

- Name: CustomObject2
- Parent: Incident
- Included field groups: OPSS-Inc-IT

You export object types from each environment by using **Export Configuration**. You then compare the two XML files by using **Compare Environments**. You choose to compare all categories. You also choose to include errors, warnings, and information messages in the results.

In this case, the tool generates the following messages:



	A	B	C	D	E	F
1	Top Category	Severity	Change Type	Context	XML Element	Description
2	ObjectText	INFO	NOTPRESENT	French > CustomObject2	objectTypeString	objectTypeString CustomObject2 is present in target but not present in source
3	ObjectText	INFO	NOTPRESENT	German > CustomObject2	objectTypeString	objectTypeString CustomObject2 is present in target but not present in source
4	ObjectText	INFO	NOTPRESENT	Italian > CustomObject2	objectTypeString	objectTypeString CustomObject2 is present in target but not present in source
5	ObjectText	INFO	NOTPRESENT	Japanese > CustomObject2	objectTypeString	objectTypeString CustomObject2 is present in target but not present in source
6	ObjectText	INFO	NOTPRESENT	Portuguese > CustomObject2	objectTypeString	objectTypeString CustomObject2 is present in target but not present in source
7	ObjectText	INFO	NOTPRESENT	Report Design Language > CustomObject2	objectTypeString	objectTypeString CustomObject2 is present in target but not present in source
8	ObjectText	INFO	NOTPRESENT	Simplified Chinese > CustomObject2	objectTypeString	objectTypeString CustomObject2 is present in target but not present in source
9	ObjectText	INFO	NOTPRESENT	Spanish > CustomObject2	objectTypeString	objectTypeString CustomObject2 is present in target but not present in source
10	ObjectText	INFO	NOTPRESENT	Traditional Chinese > CustomObject2	objectTypeString	objectTypeString CustomObject2 is present in target but not present in source
11	ObjectText	INFO	NOTPRESENT	U.K. English > CustomObject2	objectTypeString	objectTypeString CustomObject2 is present in target but not present in source
12	ObjectText	INFO	NOTPRESENT	U.S. English > CustomObject2	objectTypeString	objectTypeString CustomObject2 is present in target but not present in source
13	ObjectTypeAssociations	INFO	NOTPRESENT	parent=Incident;child=CustomObject2;type=Association;	contentTypeRelationship	contentTypeRelationship parent=Incident;child=CustomObject2;type=Association; is present in target but not present in source
14	ObjectTypeAssociations	INFO	NOTPRESENT	parent=Incident;child=CustomObject2;type=Attachment;	contentTypeRelationship	contentTypeRelationship parent=Incident;child=CustomObject2;type=Attachment; is present in target but not present in source
15	ObjectTypes	INFO	NOTPRESENT	CustomObject2	contentType	contentType CustomObject2 is present in target but not present in source
16						

Figure 24: Results of the export: A custom object does not exist in the source environment

- The `contentType` message indicates that the object type that is called `CustomObject2` does not exist in the source environment.
- When you created the CustomObject2 object type, you defined a parent relationship with the Incident object type. The `contentTypeRelationship` message in row 13 indicates that the parent association is not in the source environment.
- Although you did not define an attachment association when you created the CustomObject2 object type, the association was added by default when you created it. The `contentTypeRelationship` message in row 14 indicates that the association is not in the source environment.
- The `objectTypeString` messages are generated for each locale.

Log files for the Compare Environments tool

Each time that your run the Compare Environments tool, a log file is created.

The log files are located in the *<OP_HOME>*`/aurora/logs` directory.

The naming convention for the log files is *<openpages server instance name><unique session id>-<start java timestamp>*`-compareenvironments.log`.

Example:

```
opapp-OPNode1Server11982-1499351409947-compareenvironments.log
```

Delete old Compare Environments log files periodically to clean up the *<OP_HOME>*`/aurora/logs` directory.

The log files for the Compare Environments tool are included when you run the LogCollector tool. For more information, see “Collect log files and diagnostic data” on page 539.

Chapter 22. Migrating OpenPages GRC Platform environments

If your organization has multiple IBM OpenPages GRC Platform environments, you can migrate both the configuration information and the metadata from one environment to another. Migration means exporting from a source environment and importing into a target environment.

The term environment migration refers to using **Administration** > **Export Configuration** to create a JAR file that can be imported using **Administration** > **Import Configuration**. You can also use ObjectManager, a command line interface (CLI) tool, to migrate configuration changes. For more information, see "Importing configuration changes" on page 621. You can use **Import Configuration** to import files in XML format. Supplemental information types, including users and instance data, can be migrated in XML file format. For more information, see "Supported migration items" on page 577.

An OpenPages GRC Platform environment is a set of OpenPages GRC Platform servers that target a single database instance, inclusive of that database instance.

Many organizations use different OpenPages GRC Platform environments for specific purposes. For example, a company might use the following environments:

- Development environment - A specific set of servers where changes are made to the OpenPages GRC Platform 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

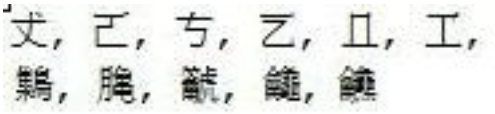
The environment migration settings are found in the **Applications** > **GRCM** > **Environment Migration** folder hierarchy.

For instructions on accessing the settings page, see Chapter 15, "Viewing the Configuration and Settings page," on page 307.

Tip: To author an XML settings path, add the `OpenPages` folder at the beginning of the path. For example: `/OpenPages/Applications/GRCM/Environment Migration/`

Table 185: Environment migration settings

Setting	Definition
Allow ObjectManager XML	Controls whether ObjectManager XML files can be imported through **Administration** > **Import Configuration**. The default is false.
Asynchronous Timeout	The timeout value (in seconds) for AJAX calls on environment migration pages. The default is 120.

Table 185: 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 in the Export File Name Prefix. The special characters to avoid are: 
Maximum String Items	Controls how many rows are displayed in the **Review selected items** box when exporting items with environment migration. Permissible values are any integer greater than zero. The default is 10000. Certain categories of items that can be exported with Environment Migration (such as Application Text) contain many tens of thousands of items. To reduce the page size and make Internet Explorer more responsive when reviewing these categories, you can now set a limit on the number of items that are shown. When a limit is set you can still use the search feature to find items beyond the row limit.
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 access environment migration for import and export. For details on these permissions, see “Types of application permissions” on page 32.

You must also have read and write permissions on the Migration Documents folder. You can see the folder by clicking **Administration** > **Manage System Files** > **Files**.

You might also need read and write permissions on other folders, depending on what you are importing and exporting.

For an overview of Environment Migration, see Chapter 22, “Migrating OpenPages GRC Platform environments,” on page 575.

Supported migration items

In any scenario, you can use the environment migration capability to move items between any two compatible IBM OpenPages GRC Platform environments.

The following information types are part of environment migration and, as such, are exported in JAR files by using **Export Configuration** and imported in JAR files by using **Import Configuration**. Alternatively, they can be imported in XML format files by using **Import Configuration**.

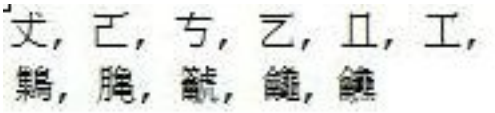
- Object Profiles
- Object Types
- Security Rules
- Field Groups
- Fields
- Application Text
- Object Text
- Error Text
- Filter Definitions
- Field Dependencies
- Dependency Picklists
- Object Type Relationships
- Rulesets
- Registry settings
- Object Type Dimensions
- Recursive Object Levels
- Date Dimension Types
- Date Dimension Type Associations

The following supplemental information types can be exported using the ObjectManager tool and imported in XML format files by using **Import Configuration**:

- System data (typically loaded during installation)
  - file types (for example, ppt, xls, doc)
  - application permissions
  - currencies
  - channels
  - locales
- User-related information
  - users and user groups
  - group memberships
  - user associations to profiles
  - user preferences
  - role templates
  - role assignments
  - delegated administrators
- Instance data
  - instance data (for example, risk and control objects and field values)

  - parent and child relationships
- Other
  - currency exchange rates

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:



For information on ObjectManager, see Chapter 23, “The ObjectManager tool,” on page 589.

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 575), 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`.

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 186: Dependent Items Exported

Item	These dependencies are exported
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
Application strings	Any corresponding string keys

Table 186: Dependent Items Exported (continued)	
Item	**These dependencies are exported**
Object type dimensions	Any recursive object levels, if associated
Date dimension type associations	Any corresponding date dimension types

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 GRC Platform 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 575).

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.

Important: Manually validate all data before importing the configuration items into the target environment.

The validation process provides feedback through a detailed Cognos-style report on the current status, the number of correctly validated items, and any inconsistencies or failed validations.

Items that are 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 GRC Platform Customer Support.

Configuration settings that are not migrated

The configuration settings listed in Table 187 on page 580, are not migrated by environment migration.

Important: Do not attempt to change the security model with the **Settings** > **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.

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

Note: The hidden settings will not be migrated if the **Show Hidden Settings** setting is set to false. For details, see "Show hidden settings" on page 311. To allow the migration of the hidden settings, set the **Show Hidden Settings** setting to true.

Table 187: Configuration settings that are not exported	
Setting description	**Location**
Mail server name	**Applications** > **Common** > **Email** > **Mail Server**
SMTP user name	**Applications** > **Common** > **Email** > **SMTP User Name**
SMTP password	**Applications** > **Common** > **Email** > **SMTP Password**
SOCKS Proxy private IP address	**Applications** > **Common** > **Email** > **SOCKS Proxy Private IP Address**
Guest password on server	**Platform** > **Application Server Guest Password**
JMS listener Urls for all paired servers	**Platform** > **Global Caches** > **JMS** > **Listener Urls**
Default OpenPages e-mail sender address	**Platform** > **Publishing** > **Mail** > **From Address**
Default OpenPages e-mail server	**Platform** > **Publishing** > **Mail** > **Host**
Default OpenPages e-mail username	**Platform** > **Publishing** > **Mail** > **Username**
OpenPages detail page name for reference by reporting tool	**Platform** > **Reporting Schema** > **Object URL Generator** > **Detail Page**
OpenPages server name for reference by reporting tool	**Platform** > **Reporting Schema** > **Object URL Generator** > **Host**
OpenPages server port for reference by reporting tool	**Platform** > **Reporting Schema** > **Object URL Generator** > **Port**
OpenPages application protocol for reference by reporting tool	**Platform** > **Reporting Schema** > **Object URL Generator** > **Protocol**
Export File Name Prefix	**Applications** > **GRCM** > **Environment Migration** > **Export File Name Prefix**
Index search server URL	**Platform** > **Search** > **Index** > **Search Server URL**
Request search server URL	**Platform** > **Search** > **Request** > **Search Server URL**
Search server administration URL	**Platform** > **Search** > **Admin** > **Search Server Administration URL**
Solr user ID	**Platform** > **Search** > **Solr User ID**
Solr password	**Platform** > **Search** > **Solr Password**

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
- custom query subjects
- JSPs
- Role Templates
- instance data

Although role templates and instance data are not part of the environment migration JAR files, you can import them into another environment using ObjectManager XML format files and **Import Configuration**.

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 OpenPages GRC Platform 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 "Configure user and group selectors display types for simple strings" on page 266.

Reports not migrated

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 OpenPages GRC Platform 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 items are 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, ensure that all namespaces upon which computed fields have a dependency are included in the export JAR.

- Objects, Field Groups, and Fields

  If a filter includes criteria that rely on an object, a field group, or a field that is not already in the target environment, the migration will fail. To avoid this scenario, ensure that all objects, field groups, and fields upon which filters 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.

- You must have imported the metadata and created reporting schema before you can import security rules.
- 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 GRC Platform 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 "The OPBackup utility" on page 387.
- Make modifications and additions to configuration items in a test or development environment. After the items are tested, migrate the items to the production environment.
- Before importing configuration items, validate the data using the OpenPages GRC Platform migration capabilities described in "Validating the migration file" on page 585.
- 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.
- If you migrate filters for large text fields, you must enable the Text search feature on your target machine so large text fields display correctly in the filters.

  For more information about enabling the IBM DB2 Text Search feature, see "Enable DB2 text search" on page 407.

  For more information about enabling the Oracle Text feature, see "Enabling Oracle Text" on page 453.

The environment migration process

From a single client system, you can use the IBM OpenPages GRC Platform application to select and export changed configuration items from one 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 188 on page 582 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 188: 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 583.
Target	Verify that all the configuration items are valid in the target environment. See "Validating the migration file" on page 585.
Target	Import the configuration items into the current environment. See "Importing configuration items to the target environment" on page 584.

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 Administration Mode" on page 17.
- The export will fail if you have invalid triggers. It's best to disable triggers prior to doing the export configuration.

Before you begin

You must be logged in as an OpenPages administrator who has the **ExportConfiguration**application permission. You must also have read and write access to the Migration Documents folder. For information, see "Settings that apply to environment migration" on page 575.

Determine whether you must preserve the SMTP configuration in the target environment. The following settings can be exported:

- **Applications** > **Common** > **Email** > **SMTP Port**
- **Applications** > **Common** > **Email** > **SMTP Security Type**

If you import the settings, you can overwrite existing values in the target environment. To preserve the SMTP configuration, you must clear them from the list of selected items in Step 6 in the following procedure.

Procedure

1. Log on to the source OpenPages application as an administrator.
2. Disable System Administration Mode, if enabled. For details, see "Enabling and disabling System Administration Mode" on page 17.
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** icon 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** icon.
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. Optional: 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** icon 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** icon.

    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 "Log summary migration report " on page 587 and "Log details migration report" on page 587.

11. Click the **Refresh** icon 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.

    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 GRC Platform 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 "Import validation" on page 579). 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 that are not migrated" on page 579.

You must be logged in as an OpenPages administrator who has the **ImportConfiguration** application permission. You must also have read and write access to the Migration Documents folder. For information, see "Settings that apply to environment migration" on page 575.

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 Administration Mode" on page 17). 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. 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 Chapter 15, "Viewing the Configuration and Settings page," on page 307).
2. Expand the **Administration** > **Settings** > **Applications** > **GRCM** > **Environment Migration** folder hierarchy.

   Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.
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 it is best 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 GRC Platform 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 file can be in either JAR or XML format.
   b) **Server repository** to import a migration file from the OpenPages GRC Platform repository. Click **Browse** to locate the migration file to import.
4. Click **Submit**.
5. To review the details of the selected items, click the links in the **Review items in the migration package** pane. If you are importing a JAR format file, all items of that type selected for import are displayed in the **Selected item details** pane. If you are importing an XML format file, supplemental information types are validated but not displayed in the **Selected item details** pane. For more information about, see "Supported migration items" on page 577.

   Click **Clear** 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 **Back** in the browser.
6. 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 **View Log**.
7. Click **Refresh** 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 "Log summary migration report " on page 587 and "Log details migration report" on page 587. 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 by using **Administration** > **Import Configuration**.

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. 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 **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 Chapter 15, "Viewing the Configuration and Settings page," on page 307.

Procedure

1. Log on to the target IBM OpenPages GRC Platform application as a user with the **ImportConfiguration** permission and access to the Migration Documents folder.
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 file can be in either JAR or XML format.
   b) **Server repository** to import a file from the OpenPages repository. Click **Browse** to locate the migration file to import.
4. Click **Submit**.
5. To review the details of the selected items, click the links in the **Review items in migration package** pane. If you are importing a JAR file, all items of that type selected for import are displayed in the **Selected item details** pane. If you are importing an XML file, supplemental information types are validated but not displayed in the **Selected item details** pane. For more information about, see "Supported migration items" on page 577.

   Click **Clear** 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 **Back** in the browser.
6. When you are satisfied with the data to import, click **Import**. 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 581.

   The **Import History** pane shows the progress of the import. You can view a detailed status, by clicking **View Log**.
7. Click **Refresh** 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 "Log summary migration report " on page 587 and "Log details migration report" on page 587.

The **Import Configuration** page returns to the initial state, allowing you to perform additional imports, as needed.

Results

- After a successful import, you can view detailed feedback by clicking **View Log** to download a 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 **Platform** > **Reporting Framework V6** > **Configuration** > **Supported Triangle Relationships** setting, you must update the Reporting Schema with the new triangle views. For instructions, see "Changes that require the reporting schema to be regenerated" on page 89.

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 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 GRC Platform 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 23. The ObjectManager tool

The ObjectManager tool provides a command-line interface (CLI) that you can use instead of the application graphical user interface to load data into the IBM OpenPages GRC Platform repository.

With the ObjectManager tool, you can perform the following tasks:

- Import (load) data, such as objects and configuration data, into the OpenPages GRC Platform repository.
- Export (dump) filtered or unfiltered data from the OpenPages GRC Platform repository. You can use this functionality, for example, to migrate environments and data from one computer to another one in a multi-deployment environment.
- Batch-load multiple loader files in a single session.

Only a Super Administrator has full access to ObjectManager operations.

An alternative to using the ObjectManager tool is to use **Administration** > **Import Configuration**. You can use it to load system data, user-related information, and instance data. The rules that apply to loader files that are imported with the ObjectManager tool apply also to **Import Configuration**.

The ability to import ObjectManager XML files through **Import Configuration** is controlled by the `/OpenPages/Applications/GRCM/Environment Migration/Allow ObjectManager XML` registry setting. It is disabled by default.

Working with loader files

The ObjectManager tool uses XML loader files to load (import) or dump (export or extract) data into IBM OpenPages GRC Platform.

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 OpenPages GRC Platform 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 OpenPages GRC Platform, 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 "Working with loader files" on page 589.

All element tags in a data loader file are nested within the root element <openpagesConfiguration xmlFormatVersion="1.31"> and </openpagesConfiguration> tags.

An ObjectManager data loader file has the following structure:

```
<?xml version="1.0" encoding="UTF-8"?>
<openpagesConfiguration xmlFormatVersion="1.31">
      <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.

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) and Mexican peso (MXN).

The exchangeRates element contains the exchangeRate child-element, which has attributes for the 3-letter ISO code for the country or region and the updated exchange rate for that currency.

```
<?xml version="1.0" encoding="UTF-8"?>
<openpagesConfiguration xmlFormatVersion="1.31">
   <exchangeRates>
      <exchangeRate isoCode="CAD"
                      startDate="2013-05-09 17:36:12"
                                      rate="0.8636"/>
      <exchangeRate isoCode="MXN"
                      startDate="2013-05-09 17:36:12"
                                      rate="0.0951"/>
   </exchangeRates>
</openpagesConfiguration>
```

Running ObjectManager commands

The ObjectManager command file is named `ObjectManager.cmd` on computers running a Microsoft Windows operating system. The command file is named `ObjectManager.sh` on computers running an AIX or Linux operating system.

The file is located in the *<OP_Home>*`\bin` directory of your IBM OpenPages GRC Platform installation.

Table 189: Installation location of the OpenPages GRC Platform application	
Operating system	**Installation location**
Windows	By default, *<OP_Home>* is `C:\OpenPages`
AIX and Linux	By default, *<OP_Home>* is `/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 OpenPages GRC Platform application services are running.

Interactive command line loader file syntax

The ObjectManager tool uses the following syntax for a loader file.

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>
```

ObjectManager command line parameters

You can use various commands and parameters with the ObjectManager tool.

`<command>`
Required.

Value can be one of the following:

`dump` or `d` - dumps or exports data.

`load` or `l` - loads or imports data from a single loader file.

`verify` or `v` - certifies or compares data.

You can use this command only if you are using IBM OpenPages GRC Platform version 7.1.

Starting with OpenPages GRC Platform version 7.1.0.1, the `verify` command has been deprecated. Instead, you must use the `validate` command instead which both verifies and validates the data.

`validate` or `v` - certifies or compares data.

You can use this command only if you are using OpenPages GRC Platform version 7.1.0.1 or a later version.

`<batch-mode>`
Places ObjectManager in batch processing mode loads multiple loader files in a single session.

Value is `batch` or `b`.

`<user>`
Required.

A user account. Some actions may require a Super Administrator account.

`<password>`
Required.

User account password.

`<loader-file-path>`
Optional.

The file path to a single XML loader file.

By default, this is the current directory if no file path is specified.

<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>
Optional.

The user-defined portion of the loader file name.

By default, the ObjectManager tool will attempt to load from or write to the file op-config.xml. if no prefix is specified.

<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.

Load command example

This Windows-based example shows 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 GRC Platform.

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:

```
ObjectManager l c OpenPagesAdministrator OpenPagesAdministrator
c:\import data1
```

Dump command example

This Windows-based example shows how to export or dump data from IBM OpenPages GRC Platform to a file with the config1 prefix 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 OpenPages GRC Platform into the config1-op-config.xml loader file:

```
ObjectManager d c OpenPagesAdministrator OpenPagesAdministrator
c:\export config1
```

The file named config1-op-config.xml will automatically be created in the c:\export folder.

Improving performance for small files in ObjectManager

There is startup overhead for ObjectManager that depends on the number of users. In environments with large numbers of users (10,000+), this can amount to 10 minutes. This overhead is onerous for small

transactions because it can result in an excessive amount of time to process ObjectManager files, no matter how small.

This issue arises because when ObjectManager connects to the server, it must initialize its environment. This initialization includes fixed costs in resources that depend on the total number of users that are registered with a system. If you have a system with a high number of registered users, this cost in resources can be large.

ObjectManager operations often take a long time. To distinguish if slow performance is due to this issue, create an XML file that does only a small operation, such as setting the value of a string. If this takes a long time (more than 2 minutes), then you might be experiencing the slowdown that is related to this issue.

To resolve this issue, an additional command line argument has been added to ObjectManager. This enables the processing to be completed on the server, rather than on the client. Because the server environment is already initialized, the per-user initialization cost is avoided.

Procedure

To use this mode, the argument -server must be added as the first argument on the command line. All other arguments remain the same, but are shifted by one position. The REST API must be enabled on the server. For example:

```
ObjectManager.cmd -server l c <username> <password> <file_path> <file_name
without op-config.xml>
```

```
ObjectManager.cmd -server load configuration <username> <password> <file_path>
<file_name without op-config.xml>
```

Additionally, in the Object Manager properties file, openpages.service.host must be set to the fully qualified host name of the admin server, and openpages.rest.port must be set to the port used for the REST API.

Because the program waits for the processing to be complete, a timeout might occur for large files with a long processing time. To resolve this issue, either run the job without the argument -server, or break the file into smaller files.

A warning message `Class path contains multiple SLF4J bindings` might occur. This warning can be safely ignored.

Attention: The `ObjectManager.log` is not updated when using the –server switch. A `Results.log` is generated under the logs subfolder where the output XML file is generated. Check server logs when ObjectManager errors occur.

Batch loader file syntax and sample

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.

The ObjectManager tool uses the following syntax for batch loading multiple loader files.

```
ObjectManager <batch-mode> config|c <user> <password>
<batch-loader-dir> <batch-loader-list-file>
```

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 (example`1-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
```

For example, you save this 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 GRC Platform. 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
   ```

Using ObjectManager to move objects

This example shows how an IBM OpenPages GRC Platform administrator can move a process object from the folder location /ENTITY02 to /ENTITY01.

Before you begin

This solution assumes that the administrator knows the following:

- The contents of TechNote # 1648075 that explains the difference between folder location and associations.
- The system-level folder name of the object.
- The target folder location already exists. Otherwise, the following validation will occur:

  ```
  VALIDATION ERROR (Line: 967 Column: 89): Target Folder Resource
  (/_op_sox/Project/Default/ICDocumentation/Processes/SampleFolder001)
  does not exist.
  ```

About this task

The following is the ObjectManager syntax for moving objects using the ObjectManager tool:

```
<openpagesConfiguration xmlFormatVersion="1.31">
     <moveResources>
        <targetFolder name="{fullpath of target folder}">
             <sourceResource name="{fullpath of the object to be moved}"/>
```

```
        </targetFolder>
     </moveResources>
</openpagesConfiguration>
```

Procedure

1. Log onto the application server.
2. Open a text editor.
3. Copy the previous syntax example.
4. Update the example to reflect the target folder location(s) and source folder location(s).

   For example:

```
<openpagesConfiguration xmlFormatVersion="1.31">
<moveResources>
<targetFolder name="/_op_sox/Project/Default/ICDocumentation/
    Processes/ENTITY01">
<sourceResource name="/_op_sox/Project/Default/ICDocumentation/
    Processes/ENTITY02/
PROC01.txt"/>
</targetFolder>
</moveResources>
</openpagesConfiguration>
```

5. Save the file using the an ObjectManager name (i.e.: samplemove-op-config.xml).
6. Open a command prompt or shell. Alternatively, you can use **Administration** > **Import Configuration** to import the XML file. For information, see "Performing the import for environment migration" on page 586.
7. Go to *OP_Home* | `bin` where *OP_Home* represents the installation location of the OpenPages GRC Platform application.

   On Microsoft Windows operating systems, the default location is `C:\OpenPages`. On AIX and Linux operating systems, the default location is `/opt/OpenPages`.
8. Run the command to load the ObjectManager file.

   The following is the sample output for the working example:

```
D:\OpenPages\bin>ObjectManager l c
OpenPagesAdministrator OpenPagesAdministrator
D:\temp samplemove

OpenPages V8.2.0.0 (Build: OP_6.2-56 2012/11/06 19:17:21) starting ...
OpenPages Global environment initialized.
==============================
Object Manager Admin Utility V6.2.0.0 (Build: OP_6.2-56 2012/11/06 19:27:49)
==============================

List of command line arguments:
        Arg 1: <l>
        Arg 2: <c>
        Arg 3: <OpenPagesAdministrator>
        Arg 4: <****>
        Arg 5: <D:\temp>
        Arg 6: <samplemove>
Total number of arguments: 6
OpenPages Server environment initialized.


Loading OpenPages Configuration (samplemove) from folder: 'D:\temp' ...

Processing started at Thu Apr 05 15:51:29 EDT 2013

Processing Move Resource Requests ...
      1 total


Move Resource requests processed: 1

Total Objects processed: 0

Total Requests processed: 1

Total Validation Errors: 0
```

```
Total Exceptions: 0

Processing finished at Thu Apr 05 15:51:29 EDT 2013
Elapsed time: 347 milliseconds
```

9. Restart the OpenPages services. For more information, see Chapter 20, “Starting and stopping servers,” on page 549.
10. If an administrator needs to move multiple objects via ObjectManager, the following is the sample syntax:

```
<openpagesConfiguration xmlFormatVersion="1.31">
  <moveResources>
     <targetFolder name="{target fullpath folder for object 1}">
     <sourceResource name="{fullpath of the object 1 to be moved}"/>
     </targetFolder>
     <targetFolder name="{target fullpath folder for object 2}">
     <sourceResource name="{fullpath of the object 2 to be moved}"/>
     </targetFolder>
     <targetFolder name="{target fullpath folder for object 3}">
     <sourceResource name="{fullpath of the object 3 to be moved}"/>
    </targetFolder>
  </moveResources>
</openpagesConfiguration>
```

Using ObjectManager to rename objects

This example shows how an IBM OpenPages GRC Platform administrator can rename an entity from ENTITY01 to ENTITY01A.

Before you begin

The following solution assumes that the administrator knows the system-level folder name of the object. Otherwise, the following message will be displayed:

```
VALIDATION ERROR (Line: 968 Column: 55): Resource to rename
(/_op_sox/Project/Default/BusinessEntity/ENTITY_oldname/ENTITY_oldname.txt)
does not exist.
```

About this task

The following is the ObjectManager syntax for renaming objects:

```
<openpagesConfiguration xmlFormatVersion="1.31">
     <renameResources>
          <renameResource oldFullName="{fullpath of the object to be renamed}"
                          newShortName="{name new of the object}.txt"/>
     </renameResources>
</openpagesConfiguration>
```

Procedure

1. Log onto the application server.
2. Open a text editor.
3. Copy the previous syntax example.
4. Update the example to reflect the target folder location(s) and source folder location(s).

   For example:

```
<openpagesConfiguration xmlFormatVersion="1.31">
     <renameResources>
          <renameResource oldFullName="/_op_sox/Project/Default/
                                                  BusinessEntity/ENTITY01/ENTITY01.txt"
                          newShortName="ENTITY01A.txt"/>
     </renameResources>
</openpagesConfiguration>
```

5. Save the file using the ObjectManager file name format, such as `samplerename-op-config.xml`.

6. Open a command prompt or shell. Alternatively, you can use **Administration** > **Import Configuration** to import the XML file. For information, see "Performing the import for environment migration" on page 586.
7. Go to *OP_Home* | `bin` where *OP_Home* represents the installation location of the OpenPages GRC Platform application.

   On Microsoft Windows operating systems, the default location is `C:\OpenPages`. On AIX and Linux operating systems, the default location is `/opt/OpenPages`.
8. Run the command to load the ObjectManager file.

   The following is the sample output for the working example:

```
D:\OpenPages\bin>ObjectManager l c OpenPagesAdministrator
OpenPagesAdministrator D:\temp samplerename

OpenPages V8.2.0.0 (Build: OP_6.2-56 2012/11/05 19:17:21) starting ...
OpenPages Global environment initialized.
============================
 Object Manager Admin Utility V6.2.0.0 (Build: OP_6.2-56 2012/11/05 19:27:49)
============================

List of command line arguments:
        Arg 1: <l>
        Arg 2: <c>
        Arg 3: <OpenPagesAdministrator>
        Arg 4: <****>
        Arg 5: <D:\temp>
        Arg 6: <samplerename>
Total number of arguments: 6
OpenPages Server environment initialized.


Loading OpenPages Configuration (samplerename) from folder: 'D:\temp' ...

Processing started at Fri Apr 05 08:48:21 EDT 2013

Processing Rename Resource Requests ...
      1 total


Rename Resource requests processed: 1

Total Objects processed: 0

Total Requests processed: 1

Total Validation Errors: 0

Total Exceptions: 0

Processing finished at Fri Apr 05 08:48:23 EDT 2013
Elapsed time: 2418 milliseconds
```

9. Restart the OpenPages services. For more information, see Chapter 20, "Starting and stopping servers," on page 549.

   If an administrator needs to rename multiple objects via ObjectManager, the following is the sample syntax:

```
<openpagesConfiguration xmlFormatVersion="1.31">
     <renameResources>
          <renameResource oldFullName="{fullpath of the object 1 to be renamed}"
                          newShortName="{name new of the object 1}.txt"/>
          <renameResource oldFullName="{fullpath of the object 2 to be renamed}"
                          newShortName="{name new of the object 2}.txt"/>
          <renameResource oldFullName="{fullpath of the object 3 to be renamed}"
                          newShortName="{name new of the object 3}.txt"/>
     </renameResources>
</openpagesConfiguration>
```

Using ObjectManager to assign or revoke role assignments

An IBM OpenPages GRC Platform administrator can assign or revoke role assignments using the ObjectManager tool.

Before you begin
This solution assumes that the administrator knows the following items:

- The system-level folder name of the security domain.
- The role assignment type of the role template.
- The role template name.
- The OpenPages GRC Platform user name.

About this task
The ObjectManager syntax for revoking or assigning a role assignment is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<openpagesConfiguration xmlFormatVersion="1.31">
   <roleAssignments>
      <roleAssignment type="{object type}" status="{assign/revoke}">
         <businessUnits>
            <businessUnit name="{path of the security domain}"/>
         </businessUnits>
         <roleActors>
            <roleActor name="{actorname}"/>
         </roleActors>
         <roles>
            <role name="{role template name}"/>
         </roles>
      </roleAssignment>
   </roleAssignments>
</openpagesConfiguration>
```

Using the following example, an administrator can revoke the user "johndoe" from the root level security domain.

Procedure

1. Log on to the application server.
2. Open a text editor.
3. Copy the syntax example.
4. Update the example to reflect the correct role assignment type: whether to assign or revoke the role; the security domain path; name of actor; and the role template name. For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<openpagesConfiguration xmlFormatVersion="1.31">
   <roleAssignments>
      <roleAssignment type="SOXBusEntity" status="revoke">
         <businessUnits>
            <businessUnit name="="/_op_sox/Project/Default/BusinessEntity"/>
         </businessUnits>
         <roleActors>
            <roleActor name="johndoe"/>
         </roleActors>
         <roles>
            <role name="OpenPages Modules 7.0 - All Data - No Admin"/>
         </roles>
      </roleAssignment>
   </roleAssignments>
</openpagesConfiguration>
```

5. Save the file using the ObjectManager file name format, such as `groupmem-revoke-op-config.xml`.
6. Open a command prompt or shell. Alternatively, you can use **Administration** > **Import Configuration** to import the XML file. For information, see “Performing the import for environment migration” on page 586.
7. Go to *OP_Home* `\bin` folder.
8. Run the command to load the ObjectManager file.

The following extract is the sample output for the working example:

```
OpenPages V9.0.0.2 (Build: OP_7.0.0.2-89 2014/06/10 14:20:23)
starting ...
OpenPages Global environment initialized.
==============================
Object Manager Admin Utility V7.0.0.2
(Build: OP_7.0.0.2-89 2014/06/10 14:20:23)
==============================

List of command line arguments:
    Arg 1: <load>
    Arg 2:  <config>
    Arg 3:  <OpenPagesAdministrator>
    Arg 4:  <****>
    Arg 5:  <C:\temp>
    Arg 6:  <groupmem-revoke>
Total number of arguments: 6
OpenPages Server environment initialized.


Loading OpenPages Configuration (groupmem-revoke) from folder:
    'C:\temp' ...

Processing started at Fri Jun 13 14:00:52 EDT 2014

Loading Role Assignments ...
      1 total

Role Assignments processed: 1
Business Units processed: 1
Role Actors processed: 1
Roles processed: 1

Total Objects processed: 4
Total Validation Errors: 0

Total Exceptions: 0
Processing finished at Fri Jun 13 14:00:58 EDT 2014
Elapsed time: 5703 milliseconds
```

9. Restart the OpenPages services. For more information, see Chapter 20, “Starting and stopping servers,” on page 549.

Using ObjectManager to create or load users

This example shows how an IBM OpenPages GRC Platform administrator can create or load users into the system.

Before you begin

This solution assumes that the OpenPages administrator has already created the groups that are referenced in the example.

About this task

The following is the syntax for creating or loading users using the ObjectManager tool:

```
<openpagesConfiguration xmlFormatVersion="1.31">
    <actors>
        <actor
                name="{username}"
                type="User"
                password="{password}"
                firstName="{firstname}"
                middleName=""
                lastName="{lastname}"
                canChangePassword="{true/false}"
                isTemporaryPassword="{true/false}"
                passwordExpiresInDays="0"
                description=""
                emailAddress="{email_address}"
                locale="{locale}"
                adminLevel="Default"
```

```
                enabled="true"
                hidden="false"
                editable="true">
        </actor>
    </actors>
    <actorGroupMemberships>
        <actorGroupMembership name="{username}" isEntityGroup="false">
            <group name="{existing_group_name}" isEntityGroup="false"/>
            <group name="OpenPages" isEntityGroup="false"/>
        </actorGroupMembership>
    </actorGroupMemberships>
</openpagesConfiguration>
```

Procedure

1. Log on to the application server.
2. Open a text editor.
3. Copy the syntax example that is included earlier in this topic into the text editor.
4. Modify the example to reflect the actual users and groups details. For example, you can modify the example in the following way:

```
<openpagesConfiguration xmlFormatVersion="1.31">
    <actors>
        <actor
                name="johndoe"
                type="User"
                password="openpages123"
                firstName="John"
                middleName=""
                lastName="Doe"
                canChangePassword="true"
                isTemporaryPassword="false"
                passwordExpiresInDays="0"
                description=""
                emailAddress="john.doe.user@company.com"
                locale="U.S. English"
                adminLevel="Default"
                enabled="true"
                hidden="false"
                editable="true">
        </actor>
    </actors>
    <actorGroupMemberships>
        <actorGroupMembership name="johndoe" isEntityGroup="false">
            <group name="All_Users" isEntityGroup="false"/>
            <group name="OpenPages" isEntityGroup="false"/>
        </actorGroupMembership>
    </actorGroupMemberships>
</openpagesConfiguration>
```

5. Save the file using the ObjectManager file name format, such as `loadusers-op-config.xml`.
6. Open a command prompt or a shell and follow the instructions below. Alternatively, you can use **Administration** > **Import Configuration** to import the XML file. For information, see "Performing the import for environment migration" on page 586.
7. Go to *OP_Home* | `bin` directory where *OP_Home* represents the installation location of the OpenPages GRC Platform application. On Microsoft Windows operating system, the default location is `C:\OpenPages`. On AIX and Linux operating systems, the default location is `/opt/OpenPages`.
8. Run the command to load the ObjectManager file. The following is the sample output for the example:

```
==================
 ObjectManager Admin Utility V7.0.0.2
==================
List of command line arguments:
        Arg 1: <l>
        Arg 2: <c>
        Arg 3: <OpenPagesAdministrator>
        Arg 4: <****>
        Arg 5: <C:\temp>
        Arg 6: <loadusers>
Total number of arguments: 6
OpenPages Server environment initialized.
```

```
Loading OpenPages Configuration (userz2) from folder: 'C:\temp' ...

Processing started at Mon Feb 23 14:00:00 EST 2015

Loading Actors ...
      1 total

Loading Actor Group Memberships ...
      1 total

Actors processed: 1 (1 updated)
Actor Group Memberships processed: 1

Total Objects processed: 2

Total Validation Errors: 0

Total Exceptions: 0

Processing finished at Mon Feb 23 14:00:59 EST 2015
Elapsed time: 454 milliseconds

C:\OpenPages\bin>
```

9. Restart the OpenPages services. For more information, see Chapter 20, "Starting and stopping servers," on page 549.

Modifying the ObjectManager properties file

The `ObjectManager.properties` file contains settings that control or limit the scope of exported (dumped) configuration and related data from the ObjectManager tool.

Depending on your export activity, modify the value of configuration or migration settings. Edit the `ObjectManager.properties` file in any text editor.

Note: Before you modify the `ObjectManager.properties` file, make a backup copy of the file.

For a list of settings and descriptions, see "Settings in the ObjectManager.properties file " on page 601.

To determine the settings in the file require modification, refer to the following topics:

- "Exporting all currency exchange rates" on page 611
- "Exporting currency field definitions" on page 613
- "Exporting computed field definitions" on page 614
- "Migrating configuration changes using the ObjectManager tool" on page 615

The `ObjectManager.properties` file is located in the *<OP_Home>*`\bin` directory of your IBM OpenPages GRC Platform installation.

Table 190: Installation location of the OpenPages GRC Platform application

Operating system	Installation location
Windows	By default, *<OP_Home>* is `C:\OpenPages`
AIX and Linux	By default, *<OP_Home>* is `/opt/OpenPages`

Settings in the ObjectManager.properties file

The `ObjectManager.properties` file contains several settings or properties that you can configure for exporting data.

Server parameters

openpages.service.host
Contains the name of the host server. This is a non-configurable system parameter.

openpages.service.port
Defines the server port number. Default is 10101.

The logger property

object.manager.logger.settings=./ObjectManagerLogging.properties

Defines the location of the `ObjectManagerLogging.properties` file relative to the bin directory. Do not change it.

The configuration.manager.migrate.configuration.objects property

The `configuration.manager.migrate.configuration.objects` property overwrites the following `configuration.manager.dump.*` properties and is the equivalent of setting these properties to `true`:

- `configuration.manager.dump.bundle.types`
- `configuration.manager.dump.file.upload.content.types`
- `configuration.manager.dump.jsp.based.content.types`
- `configuration.manager.dump.admin.objectprofile.views`
- `configuration.manager.dump.form.based.content.types`
- `configuration.manager.dump.object.profiles`
- `configuration.manager.dump.application.string.key.categories`
- `configuration.manager.dump.application.string.keys`
- `configuration.manager.dump.application.strings`
- `configuration.manager.dump.object.strings`
- `configuration.manager.dump.error.strings`
- `configuration.manager.dump.query.definitions`
- `configuration.manager.dump.field.dependency`
- `configuration.manager.dump.field.dependency.picklist`
- `configuration.manager.dump.recursive.hierarchy`
- `configuration.manager.dump.date.dimension.type`
- `configuration.manager.dump.object.type.dimension`
- `configuration.manager.dump.date.dimension.type.associations`
- `configuration.manager.dump.recursive.hierarchy.strings`
- `configuration.manager.dump.date.dimension.type.strings`
- `configuration.manager.dump.object.type.dimension.strings`
- `configuration.manager.dump.content.type.relationship.sets`
- `configuration.manager.dump.actor.object.profile.associations`
- `configuration.manager.dump.locales`
- `configuration.manager.dump.role.templates`
- `configuration.manager.dump.role.administrators`
- `configuration.manager.dump.role.assignments`
- `configuration.manager.dump.subsystem.exclusion.fields`
- `configuration.manager.dump.registry`

Additionally, the `configuration.manager.migrate.configuration.objects` property exports the following data:

- Any object folders referenced by:
  - `jsp.based.content.types`
  - `form.based.content.types`
- query definition (filter) strings
- reporting schema column definitions (which are used to keep framework labels consistent when you have duplicate field names).

The configuration.manager.dump.* export properties

The following list describes the behavior of the various export `configuration.manager.dump.*` properties when a property is enabled (the value is set to `true`).

configuration.manager.dump.modules
Exports a list of the modules (solutions) that are installed. It also controls the list of entries on the **About OpenPages GRC Platform** and **Build Information** pages.

configuration.manager.dump.file.types
Exports a list of valid file attachment types (such as `docx`, `pdf`, `jpg`).

configuration.manager.dump.bundle.type
Exports all field groups in the system, along with all of their fields.

configuration.manager.dump.file.upload.content.types
Exports all file upload object types, such as **SOXDocument**. It will also export any folders (`nonFormBasedResources`) that are referenced by these object types.

configuration.manager.dump.jsp.based.content.types
Exports all other object types, such as **SOXBusEntity**, **Mandate**, **Policy**, or any "Custom Forms". It will also export any folders (`nonFormBasedResources`) that are referenced by these object types.

configuration.manager.dump.content.type.relationship.sets
Exports a list of which objects types can be associated to what other object types.

configuration.manager.dump.app.permissions
Exports a list of application permissions that can be granted to groups or role templates.

configuration.manager.dump.actors
Exports all users, groups, and security domain groups.

configuration.manager.dump.actor.group.memberships
Exports all group memberships, such as: which users belong to what groups, which users belong to what security domains, and which security domains belong to what other security domains.

configuration.manager.dump.actor.object.profile.associations
Exports users and their assigned profiles.

configuration.manager.dump.admin.objectprofile.views
Exports object profiles. This property should be used with the `configuration.manager.dump.object.profiles` setting.

configuration.manager.dump.object.profiles
Exports object profiles. This property should be used with the `configuration.manager.dump.admin.objectprofile.views` setting.

configuration.manager.dump.non.form.based.resources
Exports all folders and object instances in the system. You can use the setting `configuration.manager.dump.resources.root.folder` to narrow the scope of objects that are exported. You will probably want to use this setting with the setting `configuration.manager.dump.resource.sets`.

As an alternative, you can use the `configuration.manager.dump.associated.resources` property.

configuration.manager.dump.form.based.content.types
Exports form-based object type definitions if these were used. By default (out of the box), the software does not use form-based object type definitions.

configuration.manager.dump.form.based.resources
Exports instances of form-based object types if these were used. This property is similar to the `configuration.manager.dump.non.form.based.content.types` property.

The `configuration.manager.dump.form.based.resources` property is generally not needed because of what is stated in the `configuration.manager.dump.form.based.content.types` property.

configuration.manager.dump.channels
Exports all reports that appear on the **Reporting** menu in the IBM OpenPages GRC Platform application, such as: all JSP reports and any Cognos reports that have been published to the OpenPages GRC Platform application. It does not export any report definitions from Cognos. If you want to export JSP report definitions, you will also want to set the `configuration.manager.dump.non.form.based.resources` property to `true`, and the `configuration.manager.dump.resources.root.folder` property to `/Reports`.

configuration.manager.dump.resource.sets
Exports object instance relationships. For example, if you had an entity called "Entity ABC" that had a child process called "Process A," you would set the following properties to `true`:

- `configuration.manager.dump.non.form.based.resources property` to get the definitions of "Entity ABC" and "Process A"
- `configuration.manager.dump.resource.sets` property to get the entry that says "Process A" is a child of "Entity ABC".

As an alternative, you can use the `configuration.manager.dump.associated.resources` property.

configuration.manager.dump.associated.resources
Exports objects and their relationships – you can use it instead of configuration.manager.dump.non.form.based.resources and configuration.manager.dump.resource.sets.

To filter the scope of the export, you can use the following settings:

configuration.manager.dump.associated.resources.set
The value of this setting, `SOX.ProjectDefault`, is a constant, do not change it.

configuration.manager.dump.associated.resources.label
Enter the name of the reporting period from which you want to export data. If you leave this value blank, it will default to the **Current Report Period**.

configuration.manager.dump.associated.resources.root.node.*[number]*
You can create multiple entries with this setting if you increment the *[number]* part of the name. Enter the full paths of the objects (one object per entry) that you want to use as the scope for the data export. To find the full path of the object, you may need to look at the object in OpenPages. The default value of `/_op_sox/Project/Default/Default.txt` will export all of the data in the system.

configuration.manager.dump.associated.resources.include.content.type.*[number]*
You can create multiple entries with this setting if you increment the *[number]* part of the name. Enter one object type name per entry that you want to include in the export. As the export process navigates the object tree structure in the system, when it encounters an object that is not of a type listed in these entries, it will not export that object or any of its children. In this way you can limit the scope of exported objects. A blank entry value will include all object types.

To filter export results, add entry values to one of the following settings. Adding entry values to both settings is redundant.

```
configuration.manager.dump.associated.resources.include.content.type.
[number]
```

```
configuration.manager.dump.associated.resources.exclude.content.type.
[number]
```

configuration.manager.dump.associated.resources.exclude.content.type.
[number]
You can create multiple entries with this setting if you increment the *[number]* part of the name. Enter one object type name per entry that you want to exclude in the export. As the export process navigates the object tree structure in the system, when it encounters an object that is not of a type listed in these entries, it will not export that object or any of its children. In this way you can limit the scope of exported objects. A blank entry value will include all object types.

configuration.manager.dump.rule.sets
Exports all object reset rule sets.

configuration.manager.dump.rule.set.execute.sessions
Exports the history of object reset executions.

configuration.manager.dump.registry
Exports all settings in the system.

To filter the scope of the export, you can use the following settings:

configuration.manager.migrate.configuration.exclude.registry.entry.
[number]
Excludes entries listed in this setting from export.

configuration.manager.dump.registry.root.entry.
[number]
Sets the scope of settings to be exported.

You can create multiple entries with this property by incrementing the *[number]* part of the name.

configuration.manager.dump.recursive.hierarchy
Exports recursive object levels.

configuration.manager.dump.date.dimension.type
Exports date dimension types.

configuration.manager.dump.object.type.dimension
Exports object type dimensions.

configuration.manager.dump.date.dimension.type.associations
Exports date dimension type associations (what date dimension types are enabled for what fields).

configuration.manager.dump.locales
Exports supported locales (languages). No translations are included.

configuration.manager.dump.application.string.key.categories
Exports the application text folders.

configuration.manager.dump.application.string.keys
Exports application text keys – the list of entries on the **Application Text** page – without translations.

configuration.manager.dump.application.strings
Exports translations for application text.

configuration.manager.dump.recursive.hierarchy.strings
Exports translations for recursive object levels.

configuration.manager.dump.date.dimension.type.strings
Exports translations for date dimension types.

configuration.manager.dump.object.type.dimension.strings
Exports translations for object type dimensions.

configuration.manager.dump.error.strings
Exports translations for error messages.

configuration.manager.dump.object.strings
Exports translations for: object type names, field names, field guidance, section names, and enumerated values.

configuration.manager.dump.currency.exchange.rates
Exports exchange rates.

configuration.manager.dump.currencies
Exports the list of valid currencies (enabled and disabled).

configuration.manager.dump.query.definitions
Exports public filters.

configuration.manager.dump.user.preferences
Exports **Alert Notification** settings for each user.

configuration.manager.dump.role.templates
Exports role templates.

configuration.manager.dump.role.administrators
Exports which users are assigned as administrators for what security domains.

configuration.manager.dump.role.assignments
Exports which users are assigned which role templates for what security domains.

configuration.manager.dump.field.dependency
Exports field dependencies.

configuration.manager.dump.field.dependency.picklist
Exports dependent picklists.

configuration.manager.dump.subsystem.exclusion.fields
Exports which fields are excluded from the workflow and/or reporting subsystems.

configuration.manager.dump.record.level.security.rulesets
Exports rule sets from record level security.

The configuration.manager.force.update.* properties

configuration.manager.force.update.object.strings

configuration.manager.force.update.application.strings
Overwrites existing object/application strings when set to true prior to load. The default is false. If you change this setting to true, it overwrites existing customized strings. Change it immediately back to false after the load is done to protect against inadvertently overwriting customized strings.

The invalid characters property

configuration.manager.property.name.illegal.characters=!@#$%^&*()<>+=[]\/{}|?
Defines characters that cannot be used in field names.

The disable triggers properties

configuration.manager.migrate.configuration.disable.all.triggers=/OpenPages/Applications/GRCM/Disable Triggers
Points to the registry setting that indicates whether triggers are disabled or not. Do not change it. It works with the `configuration.manager.disable.triggers` setting.

configuration.manager.disable.triggers
Disables triggers when importing or exporting data in order to not trigger excess processing as objects are created, modified, or associated. If set to true, triggers are disabled at the start of the import or export and re-enabled at the end. Default is false.

The resource load property

configuration.manager.load.resource.ignore.undefined.property.value
Controls behavior when loading objects. For more information, see "Controlling data load behavior" on page 609.

Filtering data for export

By using a filters file with predefined filters, you can narrow the scope of configuration and related data that is exported from the IBM OpenPages GRC Platform repository by the ObjectManager tool.

Before you begin

Before you can export selected data using a filters configuration file, you must verify that all dump configuration settings in the `ObjectManager.properties` file are correctly set.

Any settings in the `ObjectManager.properties` file that start with the following code must have its value set to `true`. If the value is set to `false`, then change the value to `true`.

```
configuration.manager.dump.<property>=true
```

For example, `configuration.manager.dump.object.profiles=true`

For details on modifying the `ObjectManager.properties` file, see "Modifying the ObjectManager properties file" on page 601.

About the filters configuration file

Filters are defined in an XML-based configuration file that must be named ObjectManagerExportFilters.xml and resides in the following path:

```
C:/OpenPages/ObjectManagerExportFilters.xml
```

The XML tags used for specifying the predefined filters are the same as the current ObjectManager configuration loader XML tags. Most filters are defined on the 'name' attribute of an object. Some filters have either additional or different filter attributes.

For a list of predefined filters, see Table 191 on page 608.

Example

The following sample filter code shows how you can use the ObjectManager tool to export only the Object Profile with the name "Default". No other type of objects or any other profile will be exported.

```
<objectProfiles>
        <!-- List of names of profiles to export -->
        <objectProfile name="Default"/>
</objectProfiles>
```

After defining the filters in the filters configuration file, you can use the ObjectManager dump command to export the objects.

ObjectManager predefined filters

The following predefined filters are supported in the ObjectManager tool.

Table 191 on page 608 lists the various element types with their corresponding element tag and filter attributes.

Table 191: ObjectManager predefined filters

Element type	Element tag	Filter attribute	Comment
Application Text	<application String>	name	The name of the application string.
Channels	<channel>	Any of the following: • name • channelFolder (name) • pageTemplate (name)	The name of the channel or path of the channel folder or page template.
Currencies	<currency>	isoCode	The 3-letter ISO currency code.
Exchange Rates	<exchangeRate>	isoCode	The 3-letter ISO currency code.
Field Groups	<bundleType>	name	The name of the field group.
File based resources	<resource>	name	The full path of the resource.
Filters	<queryDefinition>	name	The name of the Query definition.
Job Types	<jobType>	name + (the associated bundles)	The name of the job type.
Object Profiles	<objectProfile>	name	The name of the object profile.
Object Profile Views	<objectProfileView>	Any of the following: • type • name	Either the type only or the type and name of the Activity view.
Object Reset (SCOR) Rulesets	<ruleSet>	name	The name of the set.
Object Types	<contentType>	name	The name of the object type.
Object Type Pick List Dependencies	<dependencySet>	objectType	The object for which dependencies are defined.
Object Type Relationships	<contentType Relationship>	Any of the following: • parent • child	The parent and/or child object types.

Table 191: ObjectManager predefined filters (continued)			
Element type	**Element tag**	**Filter attribute**	**Comment**
Object Text	Any of the following: • <objectTypeString> • <fieldString> • <enumValueString> • <viewString> • <sectionString>	name	The data for the selected string.
Role Templates	<roleTemplate>	name	The name of the Role Template.
Settings	<registryEntry>	name	The name of the setting.
Sub-system Field Extensions	<subSystemExclusion ObjectType>	name	The name of the excluded object type.
User Group Memberships	<actorGroup Membership>	name	For all groups.
	<group>	name	For all group members.

Sample filter configuration file

The following sample ObjectManagerExportFilters.xml filter file exports configuration data for only the Object Profile named "Default" and its associated Detail and Activity Views.

```
<openpagesConfigurationFilters xmlFormatVersion="1.0">

    <objectProfiles>
        <!-- List of names of profiles to export -->
        <objectProfile name="Default"/>
    </objectProfiles>

    <objectProfileViewsSet>
        <!-- Specifiy the name of the profile  -->
        <objectProfileViews name="Default">
            <!-- Specifiy the name of the object type in the profile -->
            <objectProfileViewsForObjectType name="SOXProcess">
                <!-- Specifiy the views and their names -->
                <objectProfileView type="Detail"/>
                <objectProfileView type="Activity" name="Process AV"/>
            </objectProfileViewsForObjectType>
        </objectProfileViews>
    </objectProfileViewsSet>

</openpagesConfigurationFilters>
```

Controlling data load behavior

To control the behavior of the ObjectManager tool when loading objects, you can modify a setting in the `ObjectManager.properties` file.

By setting the `configuration.manager.load.resource.ignore.undefined.property.value` in the `ObjectManager.properties` file, you can control whether the ObjectManager tool creates objects with undefined values (such as an empty value or a value without a default). This setting applies only to non-required fields.

Note: If a field is required and has no default value defined, then the ObjectManager tool:

- Ignores the setting in the `configuration.manager.load.resource.ignore.undefined.property.value` property
- Does not create the object instance
- Reports validation errors.

Procedure

1. Open the `ObjectManager.properties` file in a text editor of your choice (see "Modifying the ObjectManager properties file" on page 601).
2. Set the value of the `configuration.manager.load.resource.ignore.undefined.property.value` property. If you set the value to:
   - true - then ObjectManager creates the object without validation errors. This value is the default.
   - false - then ObjectManager reports validation errors, does not create the object, and moves to the next object in the loader file.
3. Run the ObjectManager tool (see "Running ObjectManager commands" on page 590).

Managing currency exchange rates

You can use XML elements in Object Manager 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.

There are several methods for updating currency exchange rates:

- Upload a CSV file with currency exchange rates from:
  - The application user interface. For more information, see "Formatting and uploading a CSV file" on page 149.
  - An ObjectManager loader file. For more information, see "Importing exchange rates" on page 610
- Manually edit the rates in the application user interface. For more information, see "Editing exchange rates for an existing currency code" on page 149

Importing exchange rates

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 and uploading a CSV file" on page 149.

Before you begin

To use this function, the currency must have a standard three letter ISO code and exist in your system.

Procedure

1. Create an XML data loader file (see "Creating a data loader file" on page 590).
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 that are listed in the table:

Table 192: Element tags		
Element	**Attribute**	**Description**
exchangeRate	isoCode	A three letter ISO currency code
exchangeRate	rate	The currency exchange rate

The following example loads currency exchange rates for the Canadian dollar (CAD) and Mexican peso (MXN).

```
<?xml version="1.0" encoding="UTF-8"?>
<openpagesConfiguration xmlFormatVersion="1.31">
   <exchangeRates>
      <exchangeRate isoCode="CAD"
          startDate="2013-05-09 17:36:12"
          rate="0.8636"/>
      <exchangeRate isoCode="MXN"
          startDate="2013-05-09 17:36:12"
          rate="0.0951"/>
   </exchangeRates>
</openpagesConfiguration>
```

- 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. Substitute the value of the attribute that is listed in the table:

Table 193: Element tag to upload a .csv file		
Element	**Attribute**	**Description**
uploadFile	name	The file path and name of the CSV file

For 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 592.

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 601.

Before you begin

To use this function, the currency must have a standard 3-letter ISO code and exist in your system.

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 592.

Enabling and disabling currencies

You can enable one or more currencies to make it available to the appropriate processes, or you can disable one or more currencies from IBM OpenPages GRC Platform.

A disabled currency can be enabled later.

Before you begin

To use this function, the currency must have a standard three letter ISO code and exist in your system.

Procedure

1. Create an XML data loader file (see "Creating a data loader file" on page 590).
2. To enable or disable one or more currencies, use the element tags in the following example and substitute the values of the attributes that are listed in the table:

Table 194: Elements to enable or disable currencies

Element	Attribute	Description
`currency`	isoCode	A three letter ISO currency code
`currency`	enabled	If you set the value to: • `true` - the currency is enabled • `false` - the currency is disabled

The following example enables Euros and disables United Kingdom pounds.

```
<currencies>
   <currency isoCode="EUR"
             enabled="true"/>
   <currency isoCode="BBP"
             enabled="false"/>
</currencies>
```

3. Create an XML data loader file (see "Creating a data loader file" on page 590).

Importing currency field definitions

You can import currency field definitions.

Before you begin

In IBM DB2 environments, before you import an ObjectManager load that contains metadata definitions (such as fields, field groups, object type, object type associations), drop the reporting schema. Then, when the import completes, recreate the reporting schema.

Procedure

1. Create an XML data loader file (see "Creating a data loader file" on page 590).
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:

Table 195: Elements for importing currently field definitions

Element	Attribute	Description
`bundleType`	`name`	The name of a field group
`bundleType`	`description`	A brief description of the field group
`propertyType`	`name`	The name of a currency field within the specified field group

Table 195: Elements for importing currently field definitions (continued)		
Element	**Attribute**	**Description**
`propertyType`	`description`	A brief description of the currency field
`propertyType`	`required`	If you set the element to one of the following values: • `true` - the field is required • `false` - the field is not required
`propertyType`	`multiValued`	If you set the element to one of the following values:: • `true` - multiple values can be selected from the list • `false` - only one value can be selected from the list

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 592.

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 601.

Procedure

1. In the `ObjectManager.properties` file, set the values of the following properties as shown:

```
configuration.manager.migrate.configuration.objects=false
configuration.manager.dump.bundle.types=true
```

Tip: When you use ObjectManager to export all object instances and their relationships, and you have a large dataset, Object Manager will report an exception in ObjectManager.log. To avoid the exception, limit the size of the data that is exported by specifying a folder path or selecting the specific objects in the hierarchy. To specify a folder path, add the following property: configuration.manager.dump.resources.root.folder=folder_path. To specify multiple objects whose hierarchies are to be exported, add the following property, where number is a positive integer:

```
configuration.manager.dump.associated.resources.root.node.n=number
```

2. Use the ObjectManager dump command to export the data. See the “Dump command example” on page 592.

Importing computed field definitions

You can import computed field definitions.

For information on computed fields, see “Defining a computed field” on page 155.

Before you begin

In IBM DB2 environments, before you import an ObjectManager load that contains metadata definitions (such as fields, field groups, object type, object type associations), drop the reporting schema. Then, when the import completes, re-create the reporting schema.

Procedure

1. Create an XML data loader file (see “Creating a data loader file” on page 590).
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:

Table 196: Elements to import computed field definitions

Element	Attribute	Description
`computationHandler`	`name`	Do not change. A field definition attribute of the computed field.
`computationHandler`	`value`	A value that corresponds to a particular field definition attribute.

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 592.

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 601.

Procedure

1. In the `ObjectManager.properties` file, set the value of the following property as shown: `configuration.manager.migrate.configuration.objects=true`

   Tip: When you use ObjectManager to export all object instances and their relationships, and you have a large dataset, Object Manager will report an exception in ObjectManager.log. To avoid the exception,

limit the size of the data that is exported by specifying a folder path or selecting the specific objects in the hierarchy. To specify a folder path, add the following property: `configuration.manager.dump.resources.root.folder=`*`folder_path`*. To specify multiple objects whose hierarchies are to be exported, add the following property: `configuration.manager.dump.associated.resources.root.node.n=`*`number`*, where *number* is a positive integer.

2. Set the dump options for all other objects to `false`.
3. Use the ObjectManager dump command to export the data. See the "Dump command example" on page 592.

Migrating configuration changes using the ObjectManager tool

You can use the ObjectManager tool to migrate configuration changes from one deployment environment to another.

Multi-deployment environments

If you have a multi-deployment environment where changes to the IBM OpenPages GRC Platform 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 OpenPages GRC Platform 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 OpenPages GRC Platform 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.

The ObjectManager 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 GRC Platform repository)

To limit the scope of the changes to the previously mentioned configuration objects, you can edit settings in the ObjectManager.properties file. For details, see "Modifying ObjectManager settings" on page 616.

Table 197 on page 616 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 197 on page 616 to do an initial export of the configuration data from the "Development" system to the "Test" deployment system.

Table 197: Tasks for migrating configuration changes

Use this deployment...	To do this task...	Related Topic...
Test	1. 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 616 for step-by-step setup instructions before you export configuration data.
Test	2. Export the configuration changes into a file.	See "Exporting configuration changes" on page 619 for step-by-step instructions on how to export configuration metadata.
Production	3. Compare the configuration changes from the previous deployment (in task 2) against this deployment.	See "Validating or verifying configuration changes" on page 619 for step-by-step instructions on how to verify or validate configuration changes. **Note:** If you are using OpenPages GRC Platform version 7.1, you must verify configuration metadata. If you are using OpenPages GRC Platform version 7.1.0.1 or a later version, you must validate configuration changes.
Production	4. Import the configuration changes (from task 3) into the current deployment.	See "Importing configuration changes" on page 621 for step-by-step instructions on how to update configuration changes.
Production	5. To verify or validate that all the updates were applied, compare the configuration changes from the previous deployment (in task 2) against the newly updated deployment.	See "Validating or verifying configuration changes" on page 619 for step-by-step instructions on how to verify or validate 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.

Procedure

1. In a text editor of your choice, open the `ObjectManager.properties` file (see "Modifying the ObjectManager properties file" on page 601).
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 GRC Platform repository settings that are excluded, by default, from the migration process, follow the instructions in "Modifying excluded settings from export" on page 617.

Modifying excluded settings from export

If the value of some IBM OpenPages GRC Platform repository settings were changed to reflect a particular deployment environment, you can optionally 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, OpenPages GRC 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/Applications/Common/Email/SMTP User Name
3=/OpenPages/Applications/Common/Email/SMTP Password
4=/OpenPages/Applications/Common/Email/SOCKS Proxy Private IP Address
5=/OpenPages/Platform/Application Server Guest Password
6=/OpenPages/Platform/Publishing/Mail/From Address
7=/OpenPages/Platform/Publishing/Mail/Host
8=/OpenPages/Platform/Publishing/Mail/Username
9=/OpenPages/Platform/Reporting Schema/Object URL Generator/Host
10=/OpenPages/Platform/Reporting Schema/Object URL Generator/Port
11=/OpenPages/Platform/Global Caches/JMS/Listener Urls
12=/OpenPages/Platform/Reporting Schema/Object URL Generator/Detail Page
13=/OpenPages/Platform/Reporting Schema/Object URL Generator/Protocol
14=/OpenPages/Applications/GRCM/Environment Migration/Export File Name Prefix
15=/OpenPages/Platform/Search/Index/Search Server URL
16=/OpenPages/Platform/Search/Request/Search Server URL
17=/OpenPages/Platform/Search/Admin/Search Server Administration URL
18=/OpenPages/Platform/Search/Solr User ID
19=/OpenPages/Platform/Search/Solr Password
20=/OpenPages/Platform/Workflow Implementations/IBM BPM/Server URL
```

You can add additional settings to the list for exclusion or remove an existing setting from the list to include it in the export.

Note: To preserve the SMTP configuration in the target environment, you must add the following settings to the list of exclusions:

```
23=/OpenPages/Applications/Common/Email/SMTP Port
24=/OpenPages/Applications/Common/Email/SMTP Security Type
```

If you import the settings, you can overwrite existing values in the target environment. These settings are not, by default, in the list of exclusions.

Procedure

1. Open the ObjectManager.properties file (see "Modifying the ObjectManager properties file" on page 601).
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 21).
   b) Increment the number (for example, 22).
   c) Specify a full setting path and name.

      For example (do not wrap - use a single line):

```
configuration.manager.migrate.configuration.exclude.registry.entry.
22=/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. Use the ObjectManager dump command to export the data. See "Dump command example" on page 592. Not all items in the exclude list will be in the XML dump file.

   Note: Make changes to the exclusion list by editing the ObjectManager.properties file in ObjectManager. Changes to ObjectManager.properties are ignored if you use Environment Migration.

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. This procedure disables all triggers in the system.

Procedure

1. Access the **Settings** page (see Chapter 15, "Viewing the Configuration and Settings page," on page 307).
2. Expand the **Applications** > **GRCM** folder hierarchy.

   Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.
3. Click the **Disable Triggers** setting to open its detail page.
4. In the **Value** field, type `true`.
5. Click **Save**.

Migrating configuration changes

After you modify settings in the `ObjectManager.properties` file, you can begin the migration process.

Migrating configuration changes from one environment to another involves exporting, validating, and importing the changes.

Note: If you are using OpenPages GRC Platform version 7.1, you must verify configuration changes. If you are using OpenPages GRC Platform version 7.1.0.1 or a later version, you must validate configuration changes.

Exporting configuration changes

Exported data represents a snapshot of the configuration objects in the IBM OpenPages GRC Platform 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 OpenPages GRC Platform application is running.
2. Open a command or shell window and change to the *<OP_Home>* | `bin` directory of your OpenPages GRC Platform installation.
3. From the command or shell window, run an ObjectManager command on a single line.
   a) On a computer running a Microsoft Windows operating system:

   ```
   ObjectManager dump config <admin-user> <password>
    <config-folder-path> <prefix>
   ```

   b) On a computer running an AIX or Linux operating system:

   ```
   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.

   For example, on a Windows operating system:

   ```
   ObjectManager dump config OpenPagesAdministrator OpenPagesAdministrator
    c:\temp myconfig
   ```

4. To compare the exported configuration data against the configuration data in the OpenPages GRC Platform repository of the next deployment environment, see "Validating or verifying configuration changes" on page 619.

   Note: If you are using OpenPages GRC Platform version 7.1, you must verify configuration data. If you are using OpenPages GRC Platform version 7.1.0.1 or a later version, you must validate configuration data.

Validating or 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 GRC Platform repository of the current deployment environment.

If you are using OpenPages GRC Platform version 7.1, run the `verify` command.

Starting with OpenPages GRC Platform version 7.1.0.1, the `verify` command has been deprecated. Instead, you must use the `validate` command instead which both verifies and validates the data.

When you run this command using the ObjectManager tool:

- The results are displayed on the screen during the validation 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 *<OP_Home>*`\bin` 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 OpenPages GRC Platform installation, open a command or shell window.
3. From the command or shell window, run an ObjectManager command on a single line (optionally re-direct the output to a file):
   a) On a computer running a Microsoft Windows operating system:

      If you are using OpenPages GRC Platform version 7.1:

      ```
      ObjectManager verify  config <admin-user> <password>
       <config-folder-path> <prefix>
      ```

      If you are using OpenPages GRC Platform version 7.1.0.1 or a later version:

      ```
      ObjectManager validate  config <admin-user> <password>
       <config-folder-path> <prefix>
      ```

   b) On a computer running an AIX or Linux operating system:

      If you are using OpenPages GRC Platform version 7.1:

      ```
      ObjectManager.sh verify config <admin-user> <password>
       <config-folder-path> <prefix>
      ```

      If you are using OpenPages GRC Platform version 7.1.0.1 or a later version:

      ```
      ObjectManager.sh validate 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.

   On a Windows operating system and using OpenPages GRC Platform version 7.1.0.1 or a later version, 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 current deployment, and redirects the display output (from a Windows server) to a text file called `config_log.txt` also located in the `c:\temp` folder:

   ```
   ObjectManager validate  config OpenPagesAdministrator OpenPagesAdministrator
    c:\temp myconfig >c:\temp\config_log.txt
   ```

4. Review the output for any errors (see the sample output following these steps for more information).
5. To import the configuration changes and update the repository of the current deployment environment with these changes, see the topic "Importing configuration changes" on page 621.
6. To verify or validate that the updated repository of the current deployment matches the configuration changes from the export file, repeat Steps 2-4.

Results

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.
```

Verification errors indicate differences in the content of the configuration data between the export file and the OpenPages GRC Platform 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 OpenPages GRC Platform 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.

After the repository is updated with the configuration changes from the export file and the verification or validation process is repeated, the data in the export file and in the repository should match and no errors should be displayed.

Importing configuration changes

After comparing and verifying or validating the configuration metadata and changes, you can migrate the changes to the current deployment environment or system.

Note: If you are using OpenPages GRC Platform version 7.1, you must verify configuration data. If you are using version 7.1.0.1 or a later version, you must validate configuration data.

When you import the configuration changes from the previous deployment, the configuration objects in the IBM OpenPages GRC Platform repository of the current deployment are upgraded with those changes.

An alternative to using the command line interface (CLI) tool in ObjectManager is to use **Administration** > **Import Configuration** to import the XML file. For information, see "Performing the import for environment migration" on page 586.

Procedure

1. Verify that the OpenPages GRC Platform application is running.
2. Open a command or shell window and change to the *<OP_Home>*|`bin` directory of your OpenPages GRC Platform installation.
3. From the command or shell window, run an ObjectManager command on a single line:
   a) On a computer running a Microsoft Windows operating system:

   ```
   ObjectManager load config <admin-user> <password>
    <config-folder-path> <prefix>
   ```

   b) On a computer running an AIX or Linux operating system:

   ```
   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.

For example, on a Windows operating system:

```
ObjectManager load config OpenPagesAdministrator OpenPagesAdministrator
 c:\temp myconfig
```

4. To see the configuration changes in the application, stop and then restart the OpenPages GRC Platform application service (`OpenPagesAdminServer`).
5. To validate that the newly updated OpenPages GRC Platform repository matches the configuration changes from the export file, see the topic “Validating or verifying configuration changes” on page 619.
6. To export the configuration data to a file, see the topic “Exporting configuration changes” on page 619.

Chapter 24. Using FastMap

FastMap is a productivity tool that works with the IBM OpenPages GRC Platform export feature, and automates the importing and batch processing of object data into OpenPages GRC Platform.

The FastMap tool uses a data load template (a Microsoft Excel workbook in .xls or xlsx format) to capture data for import. When you import data into OpenPages GRC Platform, 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 OpenPages GRC Platform application interface, you use a FastMap data load template to capture the data for batch processing.

After the data is captured, log on to the OpenPages GRC Platform application and import the template (in .xls or .xlsx 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. After processing is complete, the objects become available for reports and updating by users.

Attention: When you import an object using FastMap, the imported object settings are determined by the **Detail** view settings within the profile.

For example, you are using the Default profile and you want to import SOXControl objects. If the **Detail** view for SOXControl has the **Description** field set to **Read-only**, you cannot update the **Description** field after importing the object via FastMap. In addition, administrators should be aware that field dependency rules are not evaluated for FastMap loads. This allows FastMap users to stage data, requiring users to enter required data during subsequent updates.

This video demonstrates how to use FastMap to bulk load data:

https://youtu.be/DTwGUDBeBOY

FastMap overview

FastMap Task Flow provides an overview of the tasks using FastMap to import data into IBM OpenPages GRC Platform.

Note: FastMap import is not supported for File and Signature objects or for the system Comment field.

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)

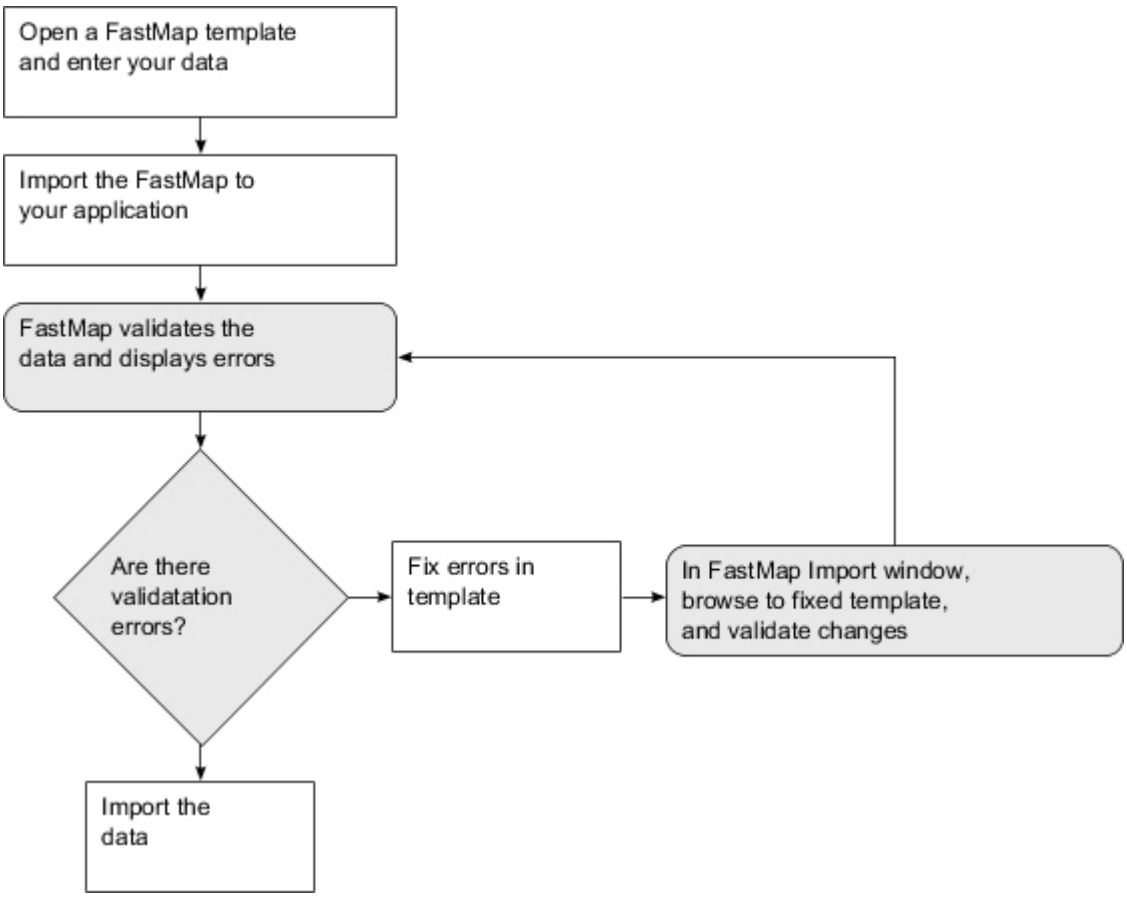


Figure 25: FastMap task flow

FastMap templates

A FastMap template is a Microsoft Excel workbook with 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 or xlsx 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

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 or .xlsx format in Microsoft Office 2010.
- User access is based on the Role Template assigned to a user or group. For details about Role Templates, see "Role templates" on page 51.
- For Long String data types, the medium text sub type is the only sub type supported for FastMap uploads. Fields with a large sub type are ignored by Excel and FastMap as these fields might be too large for Excel to store in a cell (the maximum storage for a cell is 32 KB).
- Fields that cannot be modified, such as the system **Creation Date**, **Created By**, or **Last Modified By** fields, also cannot be edited by using the FastMap process. For example, if you are migrating data, you cannot preserve the creation date information by using FastMap. FastMap import is not supported for the system Comment field.

The FastMap data validation process

When a FastMap template is imported into the IBM OpenPages GRC Platform 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 FastMap validation errors" on page 626.

FastMap 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.

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 FastMap Definition worksheet" on page 641.

When you export object type data from the IBM OpenPages GRC Platform 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.

Accessing FastMap to import data and view status

You can access FastMap in multiple ways from the **Reporting** menu on the IBM OpenPages GRC Platform 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 OpenPages GRC Platform 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 198 on page 626.

Table 198: 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 198 on page 626).

   A separate browser window opens with the selected report.

Importing a FastMap data load template

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" on page 625).
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 FastMap validation errors" on page 626.
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** icon to view the current status of the import (see "Understanding import status messages" on page 633 for more details).

Resolving FastMap validation errors

Before FastMap can import data into the IBM OpenPages GRC Platform 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. After all validation errors are resolved, FastMap is ready to import the data into the OpenPages GRC Platform application.

Understanding FastMap 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 199 on page 627 lists some of the most common messages that may be displayed in a FastMap Import window.

Table 199: 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 "Troubleshooting FastMap validation messages" on page 627.
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.

For example, 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 FastMap conflict with recent updates warning message

If you are unable to import changes and this 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: 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 following this procedure.

Procedure

1. Open the FastMap template in Excel.
   a) If necessary, unhide the Definition worksheet (see "Unhiding a FastMap Definition worksheet" on page 642).
   b) Remove the `exportDate` parameter.
   c) Save the change.
2. Resubmit the template for import.

Troubleshooting FastMap validation messages

FastMap Validation Messages 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.

In the following two tables, Table 200 on page 628 and Table 201 on page 631, messages are listed in alphabetical order.

Table 200: FastMap validation error messages

Message	Cause	Resolution
`Currency field is missing currency code.`	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.`	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.`	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.`	Signature objects are not supported for import.	Remove Signature objects from the worksheet.
`Invalid boolean format. Value must be either true or false.`	An invalid Boolean value is specified.	Ensure the Boolean value is set to either `true` or `false`.
`Invalid classifier format.`	Values in classifier fields or classifier target fields were exported, edited, and re-imported.	Remove the value from the spreadsheet or re-export and import the data. Do not edit classifier fields or classifier target fields after exporting them.
`Invalid currency code.`	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.`	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.`	A non-numeric value was entered for a decimal field.	Make sure that decimal fields have a numeric value.
`Invalid decimal range.`	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.`	Exchange rate is 0 or negative.	Make sure the exchange rate value is greater than 0 (zero).

Table 200: FastMap validation error messages (continued)

Message	Cause	Resolution
`Invalid group.`	An invalid value was entered for a Group field.	Ensure the name of the group is spelled correctly and is valid.
`Invalid Integer format`	A non-numeric value was entered for a numeric value.	Make sure the field has a numeric value.
`Invalid Integer range.`	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.`	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.`	The value of the `parentResource` parameter is invalid.	Make sure the full path of the specified parent object is correct.
`Invalid Property Type.`	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 Reader provided.`	The value of the reader parameter is not valid.	Ensure the reader parameter is spelled correctly and is valid. [Hidden - for future use]
`Invalid URL.`	An invalid URL was entered for a URL field.	Ensure the URL is correct and fully qualified.
`Invalid user.`	An invalid value was entered for a User field.	Ensure the name of the user is spelled correctly and is valid.
`Invalid user/ group.`	An invalid value was entered for a User/Group selector.	Ensure the name of the user or group is spelled correctly and is valid.
`Invalid Writer provided.`	The value of the writer parameter is not valid.	Ensure the writer parameter is spelled correctly and is valid. [Hidden - for future use]
`Locale is invalid.`	The locale value specified is not recognized.	Ensure the value of the locale is spelled correctly and is valid.
`Missing currency code column.`	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.`	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.

Table 200: FastMap validation error messages (continued)		
Message	**Cause**	**Resolution**
`Multiple resources found with the same key value.`	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.`	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.
`Name contains illegal characters.`	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).`	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.`	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.`	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.`	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.`	A parent is specified in your spreadsheet, but FastMap cannot find it in the IBM OpenPages GRC Platform 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.`	A text field contains more characters than is allowed in the OpenPages GRC Platform application.	Modify the text field so it does not exceed the character or byte limit.

Table 200: FastMap validation error messages (continued)		
Message	**Cause**	**Resolution**
`Required property is missing value.`	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.
`System 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.`	A text property value is formatted as a number or a date in the spreadsheet. A `Text` field in OpenPages GRC Platform is formatted in the worksheet cell as `Number` or `Date`. The field cannot be read in by OpenPages GRC Platform 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.`	The total number of rows in the workbook is greater than the value set in the `Maximum Workbook Rows` setting (see “Limiting the rows for import to optimize FastMap performance” on page 653).	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.`	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.`	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.

Table 201: FastMap validation warning messages		
Message	**Cause**	**Resolution**
`Full import will result in objects being deleted.`	When setting `fullImport` to 'true', FastMap identifies objects to be deleted.	Informational message, no action required.

Table 201: FastMap validation warning messages (continued)		
Message	**Cause**	**Resolution**
`Invalid Content Type`	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. • In an English locale the data was exported from a Filtered List View to Excel. Then the locale in the Excel worksheet was change to something other than en_US. An error is issued when the data is imported with FastMap.	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.`	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.`	A record's last modified date is more recent than the value from the `exportDate` parameter.	See "Troubleshooting FastMap conflict with recent updates warning message" on page 627 for details.

Viewing FastMap import status

After all validation errors are resolved, FastMap displays a status message indicating the number of objects to be imported.

After 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.

To understand the various status messages that may be displayed, see "Understanding import status messages" on page 633.

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 625.
2. To view the current status of an import, click **Refresh** on the report.

Understanding import status messages

The FastMap Import Status report window displays a progress meter showing the percentage completed.

The information is listed in Table 202 on page 633.

Table 202: 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
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>

Table 202: FastMap Import Status Information (continued)		
This column...	**Displays this...**	**Possible values...**
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 FastMap import status" on page 632.

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 GRC Platform application.

The data exported to a workbook by FastMap

When you export object data from a Filtered List View page, the resulting Microsoft Excel workbook has the following characteristics:

- You can export either all object fields that are displayed on an object's Detail View page or object fields that are currently displayed in the view you have open. The fields are exported to a corresponding worksheet in the workbook.
- Each object field is represented by a column on the worksheet.
- The header row in the worksheet contains labels for each object field. However, if the `useSystemNames` export template parameter is set to TRUE or if duplicate labels exist in the current locale, there are two header rows. The first header row contains full system names in the format, `<Field Group>.<Field Name>`, and the second header row contains labels for each object field.

  For information about the `useSystemNames` export template parameter, see "FastMap parameters for importing and exporting data" on page 644.
- 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:

  ```
  /   \   ?   *   :   [   ]
  ```

  For 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 GRC Platform export template the special `Delete` column and the three `Parent` columns are hidden on the object type worksheet.

  See Table 203 on page 635 for details.
- The Definition worksheet is included in the workbook and populated, by default, with the `profileName`, `locale`, `exportDate`, and `ignoreReadOnlyWarnings` parameters.

  See "Using the FastMap Definition worksheet" on page 641 for details.

FastMap exported spreadsheet file name characters
When you export object data from a Filtered List View page for an object type, the file name of the exported spreadsheet is derived from the plural label of the object type. If the plural label of the object type contains special characters, these special characters may be removed from the spreadsheet file name by the operating system causing a mismatch between the object type label and the file name. Special characters in a file name are constrained to characters allowed by the operating system.

See the help topic "Rules for Naming Folders, Objects, and Files" for more information about special characters in names. To access the online Help system, log on to the IBM OpenPages GRC Platform application, then click the **Help** link. In the **Help** window, click **Getting Started** to expand the folder, then click **Rules for Naming Folders, Objects, and Files** to display the topic.

For additional information about special characters in the exported spreadsheet, see "The data exported to a workbook by FastMap" on page 634.

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, select the object type you want and click the **Export** icon (to export in .xls or .xlsx 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. Optional: Add or modify parameters on the Definition worksheet as needed.
4. Save the file.
5. Import the workbook using the FastMap tool (see "Accessing FastMap to import data and view status" on page 625).

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 GRC Platform application.

Defining paths for objects

Sample Worksheet for Process Objects lists the various worksheet columns that you use to define the path of an object.

- The path columns in Figure 29 on page 640 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 29 on page 640 are optional.

Table 203: Columns that define the path of an object

This column...	Contains...
Folder Path	The path of an object.
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 Processes worksheet” on page 639.

Using special column headings

You can add special column headings to a FastMap data load worksheet to:

- Delete objects from the IBM OpenPages GRC Platform repository (see “Deleting objects with FastMap” on page 636)
- Move objects to another location (see) [hidden topic]
- Rename objects (see) [hidden topic]
- Disassociate objects (see “Disassociating objects with FastMap” on page 636)

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 with FastMap

To delete objects from the IBM OpenPages GRC Platform application, add a `Delete` column to the data load worksheet.

To delete objects by using FastMap, first ensure that the **Common** > **Cascade Delete** > **Include Object Types** setting specifies at least one object type.

By default, the `Delete` column is present on the worksheet when data is exported from the OpenPages GRC Platform application. To see how the `Delete` column is used in an example, see Figure 27 on page 640.

Table 204: Delete Column Values

If the value is set to...	Then...
Y	Objects that are specified for deletion (that is, have a Y in their row under the `Delete` column) will be deleted from the OpenPages GRC Platform repository. Any objects associated with the specified object using the **Cascade Delete** > **Include Object Types** setting will also be deleted from the repository.
`N` or "blank" (no value specified)	The object will not be deleted. This value is set by default.

Table 204 on page 636 shows the values for the Delete column.

Moving objects with FastMap

To move objects to a different folder location within the IBM OpenPages GRC Platform application, add a `New Folder Path` column to the data load worksheet.

For each object you want moved to a different folder location, specify the new path for the object in the corresponding row under the `New Folder Path` column. See Figure 27 on page 640 for an example.

Disassociating objects with FastMap

To disassociate objects within the IBM OpenPages GRC Platform application, add a `Remove Association` column to the data load worksheet.

See Figure 27 on page 640 for an example.

Table 205: 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 205 on page 637 shows the values for the Remove Association column.

Defining property fields for objects in FastMap templates

The number and type of object field columns in a FastMap 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 203 on page 635.

For more information about working with object fields, see “Guidelines for entering object data into FastMap templates” on page 637.

Guidelines for entering object data into FastMap 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

FastMap can override auto-naming. If auto-naming is enabled for an object and the Name column is excluded or left blank, the system assigns a name. If auto-naming is enabled for an object and a value exists in the `Name` column, that value is imported as the name.

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 206 on page 638 represents the name of a currency field for a specified object.

Table 206: 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 is a derived value)

`Base Code` (this value is set globally)

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.

For example, you have a multivalued enumerated field called "Domain" with the following selection values: Compliance, Operational, Technology, Financial Management, Internal Audit. Figure 26 on page 639 shows how data containing multiple values for the "Domain" field might look in the worksheet.

M	N	O
	Domain	
	Compliance	
	Compliance Internal Audit	
	Operational Technology Financial Management	
	Internal Audit	
	Compliance Operational Technology Financial Management	
	Technology	

Figure 26: Sample Multivalued Selection Column with Values

Adding custom columns and worksheets to FastMap templates

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 “Using the FastMap Definition worksheet” on page 641 for a sample Definition worksheet, and “FastMap parameters for importing and exporting data” on page 644 for additional parameters.

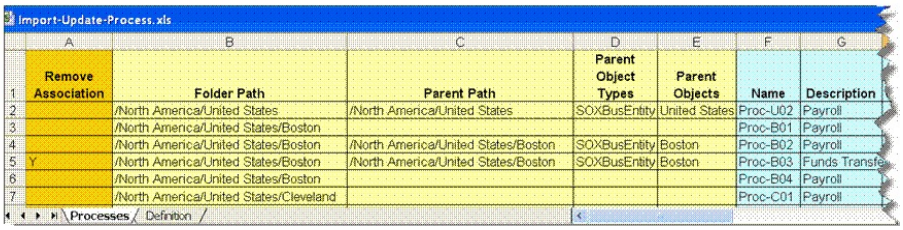
Sample Object worksheet for updating and creating objects

The sample Processes worksheet in Figure 27 on page 640 and Risks worksheet in Figure 28 on page 640 contain a combination of existing objects for update and the creation of new objects.

Sample Processes worksheet

The sample Processes worksheet in Sample Processes Worksheet shows the following:

- Column A, row 5 contains an existing Process object (`Proc-B03`) that will be disassociated from the `Boston` entity.
- Columns B through E 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 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

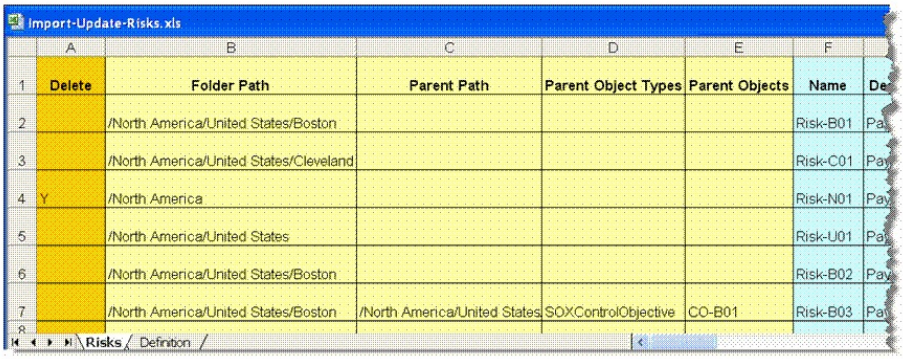
Processes / Definition /

Figure 27: Sample Processes Worksheet

Sample Risks worksheet

The sample Risks worksheet in the Sample Risks Worksheet shows the following:

- Column A, 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 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 represent object-specific fields.



Import-Update-Risks.xls

	A	B	C	D	E	F	De
1	Delete	Folder Path	Parent Path	Parent Object Types	Parent Objects	Name	
2		/North America/United States/Boston				Risk-B01	Pa
3		/North America/United States/Cleveland				Risk-C01	Pay
4	Y	/North America				Risk-N01	Pay
5		/North America/United States				Risk-U01	Pa
6		/North America/United States/Boston				Risk-B02	Pay
7		/North America/United States/Boston	/North America/United States	SOXControlObjective	CO-B01	Risk-B03	Pa
8							

Risks / Definition /

Figure 28: Sample Risks Worksheet

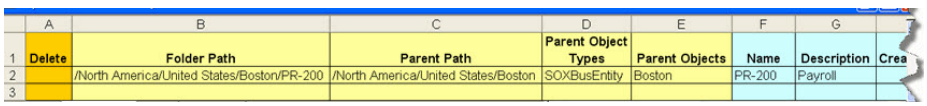
Sample self-contained object worksheet

If you are adding 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 name.

Important: You must specify the container folder for a self-contained object.

Table 203 on page 635 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 PR-200 Process folder.



	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 29: Sample Worksheet for Process Objects (Process Security Model)

Figure 30 on page 641 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
2		/North America/United States/Boston/PR-200	/North America/United States/Boston/PR-200	SOXProcess	PR-200	Risk-200

Figure 30: Sample Worksheet for Risk Objects (Process Security Model)

Sample Business Entity worksheet for creating a new business entity structure

The sample business structure in Sample Business Entity Structure shows three levels of business entities.

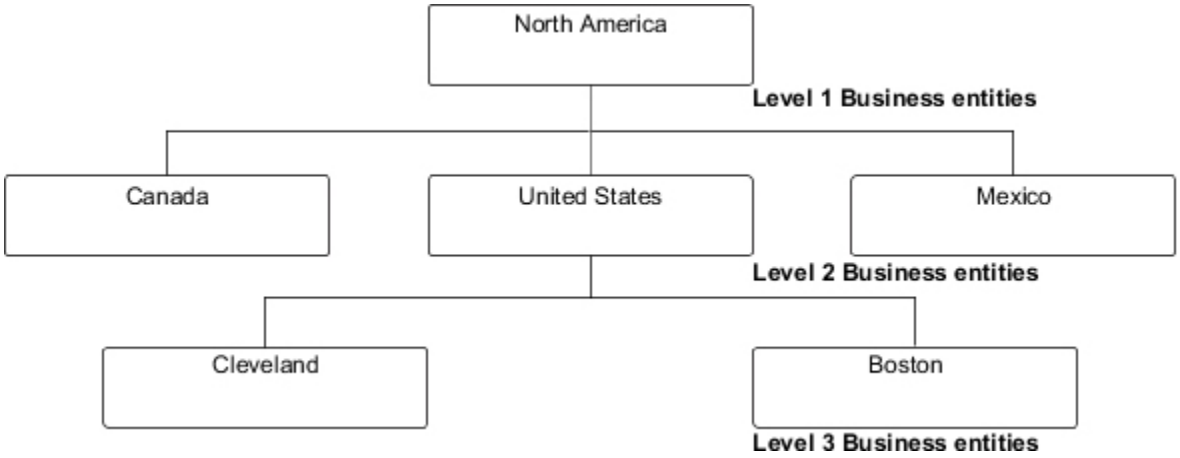


Figure 31: Sample Business Entity Structure

To create new Business Entity objects that map to the structure in Figure 31 on page 641, you would create a Business Entities object worksheet in Microsoft Excel similar to the one shown in Figure 32 on page 641.

The sample Business Entities worksheet in Figure 32 on page 641 creates new entities and shows the following:

- Column A is an optional field that can be used 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 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 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 32: Sample Business Entity Worksheet

Using the FastMap Definition worksheet

You can include a Definition worksheet in a workbook to configure FastMap behavior.

When you export data from IBM OpenPages GRC Platform, by default the Definition worksheet is not hidden from users in the workbook, and does not have column headings.

By default, the following parameter values are set:

Table 207: 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

Parameters that are listed in a Definition worksheet will override settings from other sources, such as JSP report parameters.

For more information, see "FastMap parameters for importing and exporting data" on page 644.

Unhiding a FastMap 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, 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. Save the file.

FastMap parameters

You can use FastMap parameters to customize how data is imported (uploaded) to and exported from the IBM OpenPages GRC Platform 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

FastMap 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 GRC Platform application uses `DefaultTemplate.xls` as the default export template.

Modifying parameters in the default FastMap export template

To add or modify parameters in this file, use the following instructions.

By default, the Definition worksheet in the `DefaultTemplate.xls` file has only the `ignoreReadOnlyWarnings` parameter set to TRUE.

Before you begin

To perform this procedure, you must have the **OpenPages Platform 3** profile associated with your username.

Procedure

1. From the menu bar, click **Administration** > **Manage System Files** > **Files**.
2. Click the **View** drop-down arrow, and select **Folder View** from the list.
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 209 on page 644.

Specifying a FastMap export template

The IBM OpenPages GRC Platform application supports multiple export templates.

You can specify export templates based on one or more of the following criteria:

- ContentType
- Locale
- Profile

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 system selects templates based on the following precedence: ContentType -> Locale -> Profile.

For example, `SOXRisk.xls` will be selected before `DefaultTemplate-en_US-FCM Module.xls`, and `SOXRisk-All-FCM Module.xls` will be selected before `SOXRisk.xls`

Note: If no match is found, the `DefaultTemplate.xls` export template is used.

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 OpenPages GRC Platform application.

For purposes of illustration, the examples listed in Table 208 on page 644 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 208: 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.

FastMap parameters for importing and exporting data

FastMap Definition Worksheet Import-only Parameters lists the various FastMap parameters that you can use on a Definition worksheet to configure FastMap behavior.

Table 209: FastMap Definition worksheet import-only parameters		
Import-only Parameter Name	**Default Value**	**Description**
`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

Table 209: FastMap Definition worksheet import-only parameters (continued)

Import-only Parameter Name	Default Value	Description
`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 GRC Platform, 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.
`fullLoad`	FALSE	Used when the data in your worksheet is a complete representation of what should be in the OpenPages GRC Platform 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 empty fields are blanked out during updates. If the value is set to: • TRUE - empty fields are ignored and not modified during an update. To explicitly clear a field, set its value to `*blank*`. • FALSE - empty fields will be blanked out during an update.

Table 209: FastMap Definition worksheet import-only parameters (continued)

Import-only Parameter Name	Default Value	Description
ignoreHiddenEnumWarnings	TRUE	Determines whether warning messages are displayed when values are submitted for hidden enumerated strings on a field in the OpenPages GRC Platform 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.
ignoreReadOnlyWarnings	FALSE	If data is being uploaded into fields that are defined as read-only, OpenPages GRC Platform 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 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 OpenPages GRC Platform. • 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.
reader	FastMap Reader	Use to specify a custom Java class for handling the validation of objects in FastMap. [Hidden - for future use]
shouldDefaultNotRequiredFields	TRUE	Determines whether 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.

Table 209: FastMap Definition worksheet import-only parameters (continued)

Import-only Parameter Name	Default Value	Description
shouldDefaultRequiredFields	TRUE	Determines whether 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.
shouldValidateBESelector	TRUE	Determines whether Business Entity Selector display fields are validated during import. If the value is set to: • TRUE - a warning will be displayed for any business entity that does not exist. • FALSE - no validation will be done on Business Entity Selector fields. Warnings are displayed for incorrect or invalid values. For example, a warning is shown for a wrong value, such as a typographical error. In this case, you might not want to load the data. Warnings are also displayed in cases where a value changed making it currently invalid. For example, you exported data from OpenPages and then reimported the data later by using FastMap. The data can be flagged as invalid because a field value moved, was renamed, or been deleted. In this case, you might want to load the data because it was accurate in its original state.
shouldValidateRequiredFields	TRUE	Determines whether fields configured as required in the Profile are validated during import. If the value is set to: • TRUE - required fields will be validated. • FALSE - required fields will not be validated.
suppressWarnings	FALSE	Determines whether 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 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 209: FastMap Definition worksheet import-only parameters (continued)		
Import-only Parameter Name	**Default Value**	**Description**
writer	FastMap Writer	Use to specify a custom Java class for handling the import of objects into FastMap. [Hidden - for future use]

Table 210: FastMap Definition worksheet import and export parameters		
Import and Export Parameter Name	**Default Value**	**Description**
exportDate	null	When exporting data from OpenPages GRC Platform, 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.
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. The useSystemNames parameter has no effect on enumerated values or their localized labels.

Table 210: FastMap Definition worksheet import and export parameters (continued)		
Import and Export Parameter Name	**Default Value**	**Description**
viewName	null	Specifies the view definition that is used by FastMap to validate fields. Any fields that are loaded that are not in this view are reported as invalid. The value can be set to the name of a Navigational View or Object View. The name is case sensitive. If the value is null or invalid, or if an object type is missing from the view, the Detail View is used to validate fields instead.

This video demonstrates how to enable System Names as a header in all FastMap exports to prevent conflicts and errors during imports:

https://youtu.be/M_CW-kXXmJY

Table 211: FastMap Definition worksheet export-only parameters		
Export-only Parameter Name	**Default Value**	**Description**
`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 OpenPages GRC Platform, this parameter determines whether 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.
`exportBaseCode`	TRUE	When exporting currency field data from OpenPages GRC Platform, this parameter determines whether 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 OpenPages GRC Platform, this parameter determines whether to include a column for the Exchange Rate. If the value is set to TRUE, the Exchange Rate field is included. If the value is set to FALSE, the Exchange Rate field is excluded.

Table 211: FastMap Definition worksheet export-only parameters (continued)		
Export-only Parameter Name	**Default Value**	**Description**
exportParentInfo	PRIMARY	This optional parameter specifies whether the object parent information is included or excluded from the export. You can specify the value of TRUE, FALSE, or PRIMARY for this parameter. When this parameter is set to TRUE, the parent information is included in the export. The **Parent Path**, **Parent Object Types**, and **Parent Objects** columns are filled out in the target object worksheet. If an object in the worksheet has multiple parents, one row with the unique parent\folder information is included for each parent, and the object field information is repeated in each row for that object. The resulting FastMap format worksheet can be used to load the objects and their associations to another system that does not contain these object and association instances, but has the same configured object types and associations, fields, and profiles. The data on the loaded target system will be the same as on the source system from which the content was exported. However, the export performance is slower when this parameter is set to TRUE. When this parameter is set to FALSE, data for **Parent Path**, **Parent Object Types**, and **Parent Objects** columns is not exported. When this parameter is set to PRIMARY, is not specified, or has an invalid value on the Definitions worksheet, the **Parent Path**, **Parent Object Types**, and **Parent Objects** columns in the target worksheet are filled out only for the primary parent. If an object has multiple parents, the non-primary parents are not exported.

Table 211: FastMap Definition worksheet export-only parameters (continued)

Export-only Parameter Name	Default Value	Description
highlightDuplicates	TRUE	For objects with multiple parents, this parameter is used to display the duplicated parent information by using the light-gray, italicized font to de-emphasize this information. The values are TRUE or FALSE. This parameter is dependent on the useFirstInstance import parameter. When this parameter is set to TRUE, and the useFirstInstance parameter is also set to TRUE, the first instance of the object parent information is displayed using the standard font style, and the subsequent, duplicated information is de-emphasized. If useFirstInstance is set to FALSE, the last instance of the object parent information is displayed using the standard style, and the previous, duplicate information is styled based on the highlightDuplicates parameter. Styles that are inherited from the export template are maintained. When this parameter is set to FALSE, the style of the information for objects with multiple parents is unchanged. The files exported with the highlightDuplicates and useFirstInstance parameters can be imported through FastMap without changes if the user does not make any changes to the data in the worksheet. If there are multiple records for an object in the worksheet because multiple parents are exported, the only object from which updates are recognized by FastMap is based on the useFirstInstance parameter (default value TRUE).
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 GRC Platform 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 212 on page 652 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 OpenPages GRC Platform.

Note: You can only use object fields with the data type of Simple String, Integer, or Enumerated String as lookup keys.

For example, you want to import risk data from an external system into the OpenPages GRC Platform repository. Data from the external system has a unique ID field that you want to keep and use as a lookup key within OpenPages GRC Platform.

You would create a custom field group and field definition within OpenPages GRC Platform 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. After 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.

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 9, “Fields and field groups,” on page 137).
2. Configure the key fields settings for FastMap as follows:
   a) Access the **Settings** page (see Chapter 15, “Viewing the Configuration and Settings page,” on page 307).
   b) Expand the **Applications** > **GRCM** > **FastMap** > **Key Fields** folder hierarchy.

      Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.
   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 212: 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`

Table 212: Lookup key settings (continued)	
Setting Name	**Description**
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.

Modifying export settings to optimize FastMap performance

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 "Maximum number of objects to export to Microsoft Excel on the Filtered List View" on page 338.
- Concurrent Exports - for details, see "Maximum concurrent export requests in the Filtered List View" on page 339.

Limiting the rows for import to optimize FastMap performance

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 to optimize FastMap performance" on page 654 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.

For example, if the Maximum Workbook Rows setting has a value of 2500 and a user wants to import data into IBM OpenPages GRC Platform 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 Chapter 15, “Viewing the Configuration and Settings page,” on page 307).
2. Expand the **Applications** > **GRCM** > **FastMap** folder hierarchy.

   Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.
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 to optimize FastMap performance

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 Chapter 15, “Viewing the Configuration and Settings page,” on page 307).
2. Expand the **Applications** > **GRCM** > **FastMap** folder hierarchy.

   Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.
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 optimize FastMap performance

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 Chapter 15, “Viewing the Configuration and Settings page,” on page 307).
2. Expand the **Applications** > **GRCM** > **FastMap** folder hierarchy.

Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.

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**.

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 625). 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 Chapter 15, "Viewing the Configuration and Settings page," on page 307).
2. Expand the **Applications** > **GRCM** > **FastMap** folder hierarchy.

   Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.
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 Chapter 15, "Viewing the Configuration and Settings page," on page 307).

2. Expand the **Applications** > **GRCM** > **FastMap** folder hierarchy.

   Tip: In the user interface, the `OpenPages` folder is hidden in the `Administration Settings` folder hierarchy. To author an XML settings path, include the `OpenPages` folder after the `Settings` folder in the path.
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

You can use a IBM OpenPages GRC Platform Professional Services AFCON-generated FastMap template (in .xls or .xlsx format) to import data into the FastMap tool. If you use this template, you must add a Definition worksheet to the template for compatibility.

The Definition worksheet 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 OpenPages GRC Platform Professional Services AFCON-generated FastMap template uses 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 FastMap Definition worksheet" on page 641).

A missing Definition worksheet in an OpenPages GRC Platform 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)`

Using FastMap with questionnaire template and assessment objects

You can use FastMap to import and export questionnaire template objects and the content in sections, subsections, and questions. You can also use it to import and export the standard fields for questionnaire assessment instances. However, you cannot use it import or export content, for example, question answers, comments, and attachments, on questionnaire assessment instances.

About this task

You can import and export content for the following objects:

- Questionnaire templates
- Section template

- Subsection template
- Question template
- Questionnaire assessments (standard fields only)

The `Enumerated Answers` field in the questionnaire template stores single and multi choice answers in JSON format. You cannot add this field to the object profile views, for example, filtered list view and detail view. You can, however, import and export it.

Every question in a questionnaire template has an internal identifier that is stored in the `ReportID` field. You can import a questionnaire template and leave the `ReportID` fields empty. You should then launch a program that uses the questionnaire template so that the system can assign `ReportID` values. The `ReportID` values are required for questionnaire templates and assessments to work correctly. In particular, when you copy answers from one questionnaire assessment to another, the systems requires the `ReportID` values to identify questions and their answers. For more information, see *Launching a program and copying answers* in the *IBM OpenPages GRC User Guide*.

Example

A question has three possible answers: Yes, No, and N/A, without descriptions and scores:

```
[{"value":"Yes"},{"value":"No"},{"value":"NA"}]
```

A question has two answers, Yes and No, where both answers have descriptions and scores:

```
[{"value":"Yes","score":20,"description":"description for Yes"},
{"value":"No","score":30,"description":"description for Yes"}]
```

A question has three answers, Yes, No, and N/A, where Yes requires a comment, No requires an attachment, and N/A requires both:

```
[{"value":"Yes","score":20,"requires":["comment"]},{"value":"No",
"score":30,"requires":["attachment"]},{"value":"NA","score":40,
"requires":["comment","attachment"]}]
```

Chapter 25. Configuring and generating the reporting framework

You can configure IBM OpenPages GRC Platform to use Cognos Analytics for your organization's reporting requirements.

The reporting framework

The reporting framework consists of Cognos framework models that are configured and generated in OpenPages. They support both relational and dimensional data used for creating reports in Cognos Analytics.

When you generate the reporting framework, packages for selected framework models are published to the Cognos server. Using the query subjects and query items in these namespaces, report authors can create reports from within IBM OpenPages GRC Platform.

For more information about the relational and dimensional data models, see the *IBM OpenPages GRC Report Author's Guide*.

For information about the Legacy Reporting Framework, see “Configure the reporting framework for upgraded legacy systems” on page 668.

Note: In reference to Reporting Framework V6, V6 refers to the latest framework version, not to any specific OpenPages release number.

Framework models

Framework models are based on the OpenPages object model and define subsets of objects and relationships necessary for your reporting requirements.

Framework models include the following components:

- Metadata
- Labels
- Facts and dimensions (standard models only)
- Custom query subjects

The reporting framework contains one pre-defined framework model named OPENPAGES_FRAMEWORK_V6, which is used for the pre-defined reports that are supplied with OpenPages. In addition to the OPENPAGES_FRAMEWORK_V6 framework model, you can create your own framework models. The ability to use multiple framework models allows you to target a framework model to specific solutions, user roles, or object profiles.

There are two types of framework models that you can create:

- Standard
- Basic

Both types support profile filtering and allow you to define the package name.

Standard framework models

Standard framework models are intended for advanced report writers with extensive knowledge of Cognos Analytics. Use this type of model for reports that require the more complex functionality that Cognos offers. The OPENPAGES_FRAMEWORK_V6 framework model is a standard model.

Standard framework models have the following characteristics:

- Support facts and dimensions.
- Nest relationship and dimensional subnamespaces.
- Use the following namespace hierarchy:
  - **[package label]** > **[namespace]** > **[namespace]_REL**
  - **[package label]** > **[namespace]** > **[namespace]_DIM**

  .
- Use extensive foldering for query subjects and data items.
- Contain query subjects for ancillary objects such as Enumerations and Relationships.
- Use complex field representations, for example, currencies have multiple data items for local and base amount.
- Represent recursive objects as multiple query subjects using recursive object levels.
- Provide secondary compliance objects, such as Files or Issues, as Stand Alone objects. Relationships to them must be built in reports.

Basic framework models

Basic models are intended for end users who do not have extensive knowledge of Cognos Analytics. Use this type of model for more simple reports that you want to allow your end users to create as they require.

Basic framework models have the following characteristics:

- Do not support facts and dimensions. The [namespace]_DIM sub-namespace is not created.
- Use the following namespace hierarchy:
  - **[package label]** > **[namespace]**

  Query subjects are created in the root namespace. The [namespace]_REL sub-namespace is not created.
- Do not create ancillary query subjects for Enumerations, relationships, and so on.
- Generate recursive objects, for example, Business Entity, SubMandate, and SubProcess, as single query subjects.
- Generate recursive object Levels only for Business Entity objects.
- Remove system-level data items, for example, IS_PRIMARY, LATEST_VERSION, and so on.
- Use simplified field representations, for example, single data items for Currencies and Enumerations as Local Amount and Localized Value, respectively.

More information

To configure framework models, see the following topics:

- “Configuring settings that apply to all framework models” on page 665
- “Configuring framework models ” on page 669
- “Configure reporting framework namespaces” on page 671

Namespaces

A namespace uniquely identifies a collection of query subjects, their relationships, and other objects (such as calculations) that you can use for authoring reports.

The framework generator uses the definition of a namespace (which is defined in the IBM OpenPages GRC Platform user interface) to create a corresponding namespace in the framework model.

The namespaces in the OPENPAGES_FRAMEWORK_V6 framework model are used by the pre-defined reports that are supplied with OpenPages. If you make changes to the namespaces, it can affect the functionality of the reports and may cause them to fail to run. You can add your own namespaces to the OPENPAGES_FRAMEWORK_V6 framework model to uniquely identify a collection of query subjects and other objects (such as calculations) for satisfying your reporting requirements

If you define your own standard and basic framework models, you must define namespaces for them.

When you generate the Reporting Framework V6, the packages for selected standard framework models are published to the Cognos server with relationship and dimensional subnamespaces:

- `[namespace]_REL` — this relational namespace enables report authors to report on objects based upon their defined relationships. This type of model is often used in list reports that use mixed data (numeric, data, and string).
- `[namespace]_DIM` — this dimensional namespace is organized into facts and dimensions, and gives report authors access to the online analytical processing (OLAP) features that are available in Cognos.

When you generate the Reporting Framework V6, the packages for selected basic framework models are published to the Cognos server. Query subjects are created in the root namespace. Sub-namespaces are not created.

To configure namespaces, see "Configure reporting framework namespaces" on page 671.

For more information about namespaces and the framework model, see the *IBM OpenPages GRC Report Author's Guide*.

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. It globally controls the types of aggregations that can be created for each configured fact field (see "Configuring reporting framework fact types" on page 665).

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.

To configure facts and dimensions, see "Configuring facts and dimensions" on page 674.

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. 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.

For more information about the dimensional data model, see the *IBM OpenPages GRC Report Author's Guide* on your documentation media.

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 GRC Platform application:

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

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 213 on page 662).

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, you can also specify which recursive object level sets you want available in a given namespace (see "Configure reporting framework namespaces" on page 671).

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.

To configure recursive object levels, see "Configuring business entity recursive object levels" on page 679.

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 213 on page 662.

Table 213: 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 is created in the `OpenPages_Reports_V6` package under the `GRC Objects` > `Business Entity` folder for report authors to use when they create Cognos reports.

Rules for defining sets of recursive object levels
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.

Triangle object relationships

A triangle object relationship exists when one child has two parents that are related to each other. To enhance report authoring capability, use the **Supported Triangle Relationships** setting to configure object types with triangle relationships in the Reporting Framework V6 relational data model. V6 refers to the latest framework version, not to any specific OpenPages release number.

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.

For example, a report author has a requirement to create a Risk report that allows business users to assess 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 33 on page 663.

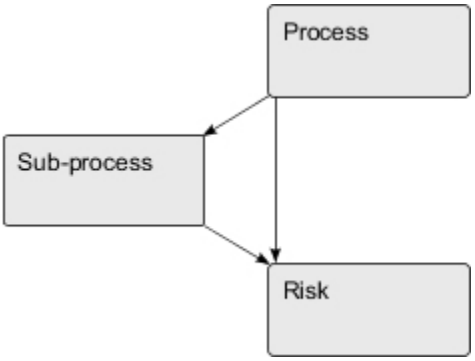


Figure 33: Triangle relationship between objects

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 Figure 33 on page 663, 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

Without the configured triangle, the report author would have to use advanced techniques that may not perform as well to accomplish this task.

To configure triangle object relationships, see “Setting the triangle reporting framework object relationships” on page 667.

Object type dimensions

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

To configure object type dimensions, see “Configuring object type dimensions” on page 681.

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 213 on page 662), you could use the Division recursive object type level as a filter for the starting object type followed by the Control object type.

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.

Selecting a starting object type for a dimension

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 679).

Planning the configuration

You can configure numerous aspects of the Reporting Framework V6.

Before you begin

Coordinate the configuration with your organization's Cognos report writers. Working together, you can ensure that the reports you are able to produce meet the needs of your organization. You can find detailed information about designing reports in the *IBM OpenPages GRC Report Author's Guide.*

About this task

To configure the Reporting Framework V6, complete the following tasks:

Procedure

1. Review the OPENPAGES_FRAMEWORK_V6 framework model and namespaces. You may need to update the namespaces delivered with the system or create new ones to meet your requirements.
2. Review the registry settings that apply to all framework models. For information, see “Configuring settings that apply to all framework models” on page 665.
3. Configure your own framework models and namespaces. For information, see “Configuring framework models ” on page 669.

4. Configure facts and dimensions. For information, see “Configuring facts and dimensions” on page 674.
5. Configure recursive object levels. For information, see “Configuring business entity recursive object levels” on page 679.
6. Configure object type dimensions. For information, see “Configuring object type dimensions” on page 681.
7. Generate the Reporting Framework V6. For information, see “Generating the reporting framework ” on page 683
8. Make reports available to end users by adding them to the home page tabs. For information, see “Displaying Cognos reports on home page tabs” on page 800.
9. Configure Cognos dashboards and stories and make it available to end users by adding it to the home page (optional). For information, see “Creating a dashboard or story page” on page 122.

Configuring settings that apply to all framework models

The settings in the **Administration** > **Settings** > **Platform** > **Reporting Framework V6** > **Configuration** folder apply to all framework models.

Configuring the number of models that can be concurrently generated

The Concurrent Models setting controls how many framework models can be concurrently generated.

Generating multiple models concurrently can improve the performance of the generation process. During generation each concurrent model uses memory and CPU resources on the Cognos Analytics server. Validate the impact and use caution before you increase this setting.

Administration > Settings > Platform > Reporting Framework V6 > Configuration > Concurrent Models

Default: 2

Values: In the **Value** field, type a number.

Configuring reporting framework fact types

A fact is a numeric field that can be aggregated.

For each fact that is selected for inclusion in the dimensional model (see “Facts and dimensions” on page 661 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 214 on page 665 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`.

Administration > Settings > Platform > Reporting Framework V6 > Configuration > Fact Types

Default: none.

Values: In the **Value** field, 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 214: Valid Fact Type Values

Fact Type	Action
SUM	Totals the value of objects in the set.

Table 214: Valid Fact Type Values (continued)	
Fact Type	**Action**
MIN	Returns the smallest existing value of an object in the set.
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.

Adding locale codes to the reporting framework

You can add locale codes to the IBM OpenPages GRC Platform Reporting Framework V6 so that they can be applied to localized reporting and reports.

Administration > Settings > Platform > Reporting Framework V6 > Configuration > Locales

Default: en_US

Values: In the **Value** field, type the following locale code values. Multiple values must be separated by a comma.

- en_US (U.S. English)
- de_DE (German)
- en_GB (U.K. 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)

Defining the sort order locale

The Sort Order Locale setting controls the language in which query subjects and data items are sorted.

Multiple locales can be loaded into the reporting framework but the reporting framework has a static sort order based on the Sort Order Locale setting.

Administration > Settings > Platform > Reporting Framework V6 > Configuration > Sort Order Locale

Default: en_US

Values: In the **Value** field, type one of the following locale code values:

- en_US (U.S. English)
- de_DE (German)
- en_GB (U.K. 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)

Setting the triangle reporting framework object relationships

To enhance report authoring capability, use the **Supported Triangle Relationships** setting to configure object types with triangle relationships in the Reporting Framework V6 relational data model.

For more information, see “Triangle object relationships” on page 663.

Administration > Settings > Platform > Reporting Framework V6 > Configuration > Supported Triangle Relationships

Default: none.

Values:

Important: The spelling and case of the object type name must exactly match its system name. For example, you would type S0XBusEntity for the Business Entity object type. Using the wrong case for letters or using the label text will result in an error message.

In the **Value** box, use the following syntax to configure the three objects in a triangle relationship:

```
Parent1|Parent2|Child
```

For example:

```
SOXProcess|SOXSubprocess|SOXRisk
```

Note: To enter multiple sets of triangle relationships, separate each triangle set with a comma as in:

```
SOXProcess|SOXSubprocess|SOXRisk,Mandate|Submandate|Requirement
```

Update the reporting schema to include the triangle relationship

After you've edited the triangle objects relationships, the reporting schema must be updated. You can either run the SQL script described in this procedure. This method incrementally updates the reporting schema with the triangle relationship configuration. Or you can create the report schema using the application user interface method.

Tip: Run the following SQL script to incrementally update the reporting schema. This method 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;
/
```

What to do next

Regenerate the framework model. For details, see “Updating the reporting framework” on page 686.

Enabling the reporting framework for custom forms

To run 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, use Z<n> as a prefix for custom forms to avoid conflicts with future IBM OpenPages GRC Platform 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).

Administration > Settings > Platform > Reporting Framework V6 > Configuration > Object Prefix

Default: none

Values: Add the new object type and prefix to the end of the current setting with a comma. The prefix must be entered as two uppercase letters, and must be unique; no other content type in the list can have the same prefix.

In the following example, the new object type (in bold) is called CustomSurvey and the prefix is 'ZA'.

```
...PROJECTACTIONITEM=PA,SOXSIGNATURE=SI,CUSTOMSURVEY=ZA
```

After you set these values, update the reporting framework model. For more information, see "Updating the reporting framework" on page 686

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 Reporting Framework V6 and Legacy Reporting Framework systems, then you must also add the new prefix to the **Object Prefix** setting in the **Platform** > **Reporting** > **Framework** > **Generation** folder hierarchy for the Legacy Reporting Framework.

Defining the transaction timeout for reporting framework generation

The Transaction Timeout setting defines the processing timeout for the reporting framework generation process.

Administration > Settings > Platform > Reporting Framework V6 > Configuration > Transaction Timeout

Default: 21600

Values: The value is in seconds.

Configure the reporting framework for upgraded legacy systems

Upgraded systems can generate two reporting frameworks. These must be configured.

- OPENPAGES_REPORTS - this is the legacy reporting framework and is available for backward compatibility for Cognos reports that have not been migrated to OPENPAGES_REPORTS_V6
- OPENPAGES_REPORTS_V6 - this is the reporting framework that is designed for faster execution of Cognos reports

Note: These settings are only available for OpenPages systems that have been upgraded from version 5.x or earlier.

Enable a legacy reporting framework

You can control whether or not to generate the legacy reporting framework through the **Enable Legacy Framework** setting.

Administration > Settings > Platform > Reporting Framework V6 > Configuration > Legacy > Enable Legacy Framework

Default: true.

Values:

- `true` - to enable the Legacy Reporting Framework
- `false` - to disable the Legacy Reporting Framework

Enable computed fields for legacy reporting frameworks
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 OPENPAGES_REPORTS_V6 reporting framework for computed field calculations. V6 refers to the latest framework version, not to any specific OpenPages release number.

Administration > Settings > Platform > Reporting Framework V6 > Configuration > Legacy > Object Types Using New Framework For Computed Fields

Default: blank.

Values: 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.

For example, `SOXBusEntity,SOXProcess,SOXIssue`

Configuring framework models

Settings in an **Administration** > **Settings** > **Platform** > **Reporting Framework V6** > **Models** > **[model name]** folder define one framework model. You can have multiple framework model folders.

For information about framework models, see "Framework models" on page 659.

Creating a framework model and namespace using a template

You can use the Template_Model framework model to quickly create new framework models and namespaces. The template model contains default values for settings and one namespace, TEMPLATE_NAMESPACE. To use it, you make a copy of the Template_Model folder and modify the settings to meet your needs.

Before you begin
Verify that the **Allow Create and Delete Settings** setting is enabled. See "Custom settings" on page 340.

Procedure

1. Click **Administration** > **Settings** > **Platform** > **Reporting Framework V6** > **Models**.
2. Select the **Template_Model** folder.
3. Click **Copy To**.
4. Select the **Models** folder so that the new framework model will be positioned in the **Models** folder.
5. Scroll down and enter the name of the new model in **New Folder Name**. Follow the naming guidelines in "Naming framework models" on page 670.
6. Click **OK**. The new folder is created.
7. Open the new framework model folder and change the **Package Label**. Review the other registry settings and change them to meet your requirements.
8. Build the namespaces for the new framework model.
   a) Select the **TEMPLATE_NAMESPACE** namespace folder or a namespace in another framework model and click **Copy To**.
   b) Select the new framework model's **Namespaces** folder so that the new namespace will be positioned in the **Namespaces** folder.
   c) Scroll down and enter the name of the new namespace in **New Folder Name**. Follow the naming guidelines described in "Naming namespaces" on page 672.

d) Open the new namespace folder and review the registry settings. Change them to meet your requirements.

e) Delete the **TEMPLATE_NAMESPACE** folder (optional).

Defining a name for a framework model

Each folder under **Administration** > **Settings** > **Platform** > **Reporting Framework V6** > **Models** defines one framework model. The name of the folder is the name of the framework model.

The name of the OPENPAGES_FRAMEWORK_V6 framework model folder cannot be changed.

Administration > Settings > Platform > Reporting Framework V6 > Models > [model name]

Default: none

Values: the name for the new framework model.

The newly created framework model is represented by a folder icon under the **Models** folder.

Naming framework models

The following list contains best practices to keep in mind when naming framework models:

- Framework model names are not translated in application text.
- Use the following characters when naming framework models:
  - Lowercase letters
  - Uppercase letters
  - Numbers
  - Underscores (_)

  Examples : `Audit_Model` and `RiskAssessment_Model`
- Do not use spaces.

Defining the format for a framework model

The Format setting controls whether a framework model uses the standard or basic format.

For information about framework models, see "Framework models" on page 659.

The Format setting of the OPENPAGES_FRAMEWORK_V6 framework model is standard. It cannot be changed.

Administration > Settings > Platform > Reporting Framework V6 > Models > [model name] > Format

Default: standard

Values:

- `standard` - the framework model uses the standard format
- `basic` - the framework model uses the basic format

Enabling a framework model

The Is Enabled setting controls whether a framework model is available for selection when you generate the reporting framework.

Administration > Settings > Platform > Reporting Framework V6 > Models > [model name] > Is Enabled

Default: true

Values:

- `true` - the framework model is available for selection when you generate the reporting framework.

- `false` - the framework model is not available for selection when you generate the reporting framework.

Defining the query mode for a framework model

The Mode setting controls whether a framework model is published in Cognos using Compatible Query Mode or Dynamic Query Mode.

The Mode setting for the OPENPAGES_FRAMEWORK_V6 framework model is cqm.

Administration > Settings > Platform > Reporting Framework V6 > Models > [model name] > Mode

Default: cqm

Values:

- `cqm` - the framework model is published in Cognos using Compatible Query Mode.
- `dqm` - the framework model is published in Cognos using Dynamic Query Mode.

Defining the package label for a framework model

The Package Label setting defines the package label name under which a framework model is published.

The Package Label setting for the OPENPAGES_FRAMEWORK_V6 framework model is OPENPAGES_REPORTS_V6. It cannot be changed.

Administration > Settings > Platform > Reporting Framework V6 > Models > [model name] > Package Label

Default:

Values: Type a name for the package label

Make package labels names meaningful to report writers.

Defining whether a framework model uses profile filtering

The Profile setting allows you to apply the filtering functionality of profiles to the data included in the reporting framework.

If an object type in the namespace is also in the profile given in the Profile setting, only fields listed for that object type in the profile definition are included in the framework. The ResourceId, Parent Folder Id, Reporting Period Id, and Detail Page URL fields are exceptions. They are always included.

If an object type in the namespace is not in the profile, all fields are included in the reporting framework.

If the Profile setting is empty, all fields are included in the reporting framework.

Administration > Settings > Platform > Reporting Framework V6 > Models > [model name] > [profile name]

Default:

Values: Type the name of a profile. Values are case sensitive.

Configure reporting framework namespaces

Settings in a **Administration** > **Settings** > **Platform** > **Reporting Framework V6** > **Models** > **[model name]** > **Namespaces** > **[namespace name]** folder define one namespace. A framework model can have multiple namespace folders. You can copy namespace folders from one framework model folder to another framework model folder. The same namespace folder name can be used in multiple framework models.

For information about namespaces, see “Namespaces ” on page 660.

The easiest way to create a new namespace is with the Template_Model framework model. For information, see “Creating a framework model and namespace using a template” on page 669.

Note: For systems that have been upgraded from versions of OpenPages 5.x or earlier, see Appendix D, "Legacy Reporting Framework Generation settings," on page 771 for information on configuring namespaces in the Legacy Reporting Framework.

Defining a name for a reporting framework namespace

Each folder under **Administration** > **Settings** > **Platform** > **Reporting Framework V6** > **Models** > **[model name]** > **Namespaces** defines one reporting framework namespace. The name of the folder is the name of the namespace.

The names of the system-supplied namespaces in the OPENPAGES_FRAMEWORK_V6 framework model folder cannot be changed.

Administration > Settings > Platform > Reporting Framework V6 > Models > [model name] > Namespaces > [namespace name]

Default: none.

Values: name for the new namespace. For example, `MYCOMPANY_NAMESPACE`.

The newly created namespace is represented by a folder icon under the **Namespaces** folder.

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`
- Do not use spaces.

Defining the object model for a namespace

The Object Model setting is required and contains the relationship path used for reporting in a namespace. A namespace cannot contain ambiguous paths.

The OpenPages GRC Platform Reporting Framework V6 generator uses the value pairs in this entry to define the parent-child relationships in the generated framework model.

Administration > Settings > Platform > Reporting Framework V6 > Models > [model name] > Namespaces > [namespace name] > Object Model

Default:

Values: In the **Value** field, enter value pairs to reflect parent-child object relationships. All parent-child paths must start with SOXBusEntity. The syntax is:

```
<parent object>|<child object>,<parent object>|<child object>
```

For example:

```
SOXBusEntity|SOXProcess,SOXProcess|SOXRisk,SOXRisk|SOXControl
```

System-supplied namespaces

If you change the **Object Model** setting in the system-supplied namespaces in the OPENPAGES_FRAMEWORK_V6 folder, it can affect the functionality of the pre-defined reports that are supplied with OpenPages.

Supported triangle relationships

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** setting of a namespace. The namespace can be either new or existing. For details on configuring the **Supported Triangle Relationships** setting, see "Triangle object relationships" on page 663.

Configuring secondary compliance objects for basic framework models

If the namespace is used in a basic framework model, you must define allowed relationships between primary and secondary compliance objects in the **Object Model** setting.

- Secondary compliance objects relationships must be added to the Object Model registry entry for the namespace, for example, SOXBusEntity|SOXIssue.
- Multiple relationships can be defined for a secondary compliance object, for example, SOXBusEntity|SOXIssue,SOXProcess|SOXIssue.
- Relationships between secondary compliance objects must be explicitly defined, for example, SOXIssue|SOXTask.

When the reporting framework is generated:

- Secondary compliance objects are generated like other objects but will have a hyphenated name including their parent object, for example, Business Entity - Issue.
- A query subject is created for each relationship defined, for example, Business Entity - Issue, Process - Issue.
- Relationships between two secondary compliance objects are generated within the context of a primary compliance object. For example, SOXBusEntity|SOXIssue,SOXIssue|SOXTask generates as Business Entity - Issue and Business Entity - Issue - Action Item.

Setting a namespace as the default

The Is Default setting defines whether a namespace will be used as the default namespace in the OpenPages GRC Platform data model.

A framework model can have only one default namespace. In the OPENPAGES_FRAMEWORK_V6 framework model, the Is Default setting in the DEFAULT namespace is set to `true`.

Administration > Settings > Platform > Reporting Framework V6 > Models > [model name] > Namespaces > [namespace name] > Is Default

Default:

Values: In the **Value** field,

- `true` - the namespace is set as the default namespace for use by generation logic, and is created first.
- `false` - the namespace is set as a non-default namespace.

Enabling a namespace

The Is Enabled setting controls whether a namespace is generated when you generate the reporting framework.

Administration > Settings > Platform > Reporting Framework V6 > Models > [model name] > Namespaces > [namespace name] > Is Enabled

Default: true

Values:

- `true` - the namespace will be generated when the framework model is updated.
- `false` - the namespace will not be generated and any previously existing namespace will be removed.

Defining entity recursive object levels for a namespace

If one or more sets of recursive object levels are defined in the OpenPages GRC Platform application, the Entity Recursive Object Levels setting provides the ability to specify which recursive object level set you want available in a given namespace.

Administration > Settings > Platform > Reporting Framework V6 > Models > [model name] > Namespaces > [namespace name] > Entity Recursive Object Levels

Default:

Values: Multiple recursive object level sets must be separated by a comma. For example:

```
ROL-1,ROL-2,ROL-3
```

For information on defining recursive object levels, see "Recursive object levels" on page 661.

Defining whether facts and dimensions are enabled for a namespace

The Is Facts and Dimensions Enabled setting controls whether facts and dimensions are enabled for a namespace.

Administration > Settings > Platform > Reporting Framework V6 > Models > [model name] > Namespaces > [namespace name] > Is Facts and Dimensions Enabled

Default: true

Values:

- `true` - facts and dimensions are enabled for the namespace.
- `false` - facts and dimensions are not enabled for the namespace.

Configuring facts and dimensions

You configure facts and dimensions using the **Administration** > **Reporting Framework** > **Configuration** task.

For more information, see "Facts and dimensions" on page 661.

Basic framework models do not support facts and dimensions. For more information, see "Framework models" on page 659.

The following table provides an overview of the configuration tasks for setting up facts and dimensions and a reference to the related information.

Table 215: Overview of configuration tasks for setting up facts and dimensions	
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” on page 675
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 675
You can configure the types of date dimensions you want available for reports in the dimensional namespace.	“Using date dimension types” on page 677
You can control whether facts and dimensions are enabled for individual namespaces.	“Defining whether facts and dimensions are enabled for a namespace ” on page 674
Update the Reporting Framework V6 to effect changes to facts and dimensions.	“Updating the reporting framework” on page 686

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 apply the changes made to fact fields, you can choose the "Dimensions and Facts" option. It regenerates and updates that portion of the reporting framework that changed.

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

Procedure

1. Complete one of the following steps to access facts and dimensions for an object type:
   - Click **Administration > Reporting Framework** > **Configuration**. From the **Facts and Dimensions** pane, click the name of the object type to select.
   - Click **Administration > Object Type**. Click the object type to select. From the **Facts and Dimensions** pane, click Edit.
2. Under the **Facts** table, do one of the following:
   - To enable a fact, select the each fact to include in the reporting framework.
   - To disable a fact, disable each fact you want excluded from the reporting framework.
3. Click **Save**.

What to do next

Update the reporting framework to effect the changes (see “Updating the reporting framework” on page 686).

Enabling and disabling enumeration and dependent picklist dimensions

You can enable and disable enumerated fields and dependent picklists as 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. Complete one of the following steps to access facts and dimensions for an object type:
   - Click **Administration > Reporting Framework** > **Configuration**. From the **Facts and Dimensions** pane, click the name of the object type to select.
   - Click **Administration > Object Type**. Click the object type to select. From the **Facts and Dimensions** pane, click Edit.
2. Under the **Enumeration and Dependent Picklist Dimensions** table, complete one of the following tasks:

Table 216: Enumeration and Dependent Picklists tasks

Task	Steps
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	a. Under the **Dependent Picklists** column, select the box next to the picklist you want included as a dimension in the reporting framework. b. 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.

Table 216: Enumeration and Dependent Picklists tasks (continued)	
Task	**Steps**
Disable a dependent picklist as a dimension	a. Under the **Dependent Picklists** column, clear the box next to the picklist you want excluded as a dimension from the reporting framework. b. 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. Click **Save**.
4. Update the reporting framework to effect the changes (see "Updating the reporting framework" on page 686).

Using date dimension types

When date fields are used as dimensions in reports, users can 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.

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

Notice: 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.

For more information, see Table 217 on page 678.

Complete the following steps to add a data dimension type:

Procedure

1. Click **Administration** > **Reporting Framework** > **Configuration**.
2. On the **Date Dimensions Type** table, click **Add**.
3. In the **Name** field, type a name for this date dimension.
4. Optional: Localize the text of the **Name** field for display in the reporting framework as follows. 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. Select a value next to each dimension you want for this date type. Only one value can be selected for each type of date dimension.

Table 217: 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.

6. Click **Save**.
   Map the date dimension to an object type date fields. See “Mapping date dimension types to date fields” on page 678.

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. Complete one of the following steps to access facts and dimensions for an object type:
   - Click **Administration > Reporting Framework** > **Configuration**. From the **Facts and Dimensions** pane, click the name of the object type to select.
   - Click **Administration > Object Type**. Click the object type to select. From the **Facts and Dimensions** pane, click Edit.
2. On the **Date Dimensions** pane, select date dimension types, for each date field in a row.
3. Click **Save**.

What to do next

Update the reporting framework to effect the changes (see “Updating the reporting framework” on page 686).

Enabling, disabling, modifying, and deleting 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. You can modify a date dimension type after you create it. 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 disable, modify, or delete a date dimension type, any reports that used that date dimension type will no longer run.

Procedure

1. Click **Administration** > **Reporting Framework** > **Configuration**.
2. In the **Date Dimension Types** pane, 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, click **Disable**, **Enable** or **Delete**. Or, make modifications and click **Save**.

What to do next
Update the reporting framework to effect the changes (see "Updating the reporting framework" on page 686).

Configuring 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 administrator interface in IBM OpenPages GRC Platform when configuring object type dimensions (see "Object type dimensions" on page 664).

For more information, see "Recursive object levels" on page 661.

Defining business entity recursive object levels

You can create multiple sets of recursive object levels for generation in the Reporting Framework V6. V6 refers to the latest framework version, not to any specific OpenPages GRC Platform release number.

Procedure

1. Access the **Object Types** page. Log on to the IBM OpenPages GRC Platform as a user with the Object Types application permission set.
   a) With the Object Types application permission set, select the **Administration** menu and click **Object Types**.
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 218: 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.

Table 218: Recursive Object Levels Definition Boxes (continued)	
In this box...	**Do this...**
Starting Entity	Type the full path, beginning with a slash, to the starting Business Entity. **Note:** Optionally, 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) icon 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) icon.
6. Optional: Localize the text for the names of the set and the text for 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) Click **Apply**.
7. To add another set, click **Add** and repeat Steps 4 - 6.
8. Click **Save**.
9. To specify which recursive object level set you want available in a given namespace, configure the `Entity Recursive Object Levels` setting (see "Configure reporting framework namespaces" on page 671).
10. Update the reporting framework to effect the changes (see "Updating the reporting framework" on page 686).

Deleting business entity sets of recursive object levels

You can delete a set of recursive object levels for a Business Entity

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. Log on to the IBM OpenPages GRC Platform as a user with the Object Types application permission set.

   a) With the Object Types application permission set, select the **Administration** menu and click **Object Types**.
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 click the **Delete** link.
5. Click **Save**.
6. Update the reporting framework to effect the changes (see "Updating the reporting framework" on page 686).

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. Log on to the IBM OpenPages GRC Platform as a user with the Object Types application permission set.
   a) With the Object Types application permission set, select the **Administration** menu and click **Object Types**.
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, complete one of the following tasks:

Table 219: Add or remove levels	
Task	**Steps**
Add another level to the set	Click the ⊞ (plus symbol) icon and type a unique name for this level.
Remove a level that was added	Click the ⊟ (minus symbol) icon.

5. Click **Save**.

What to do next
Update the reporting framework to effect the changes (see "Updating the reporting framework" on page 686).

Configuring object type dimensions

You configure object type dimensions using the **Administration** > **Reporting Framework** > **Configuration** task.

For more information, see "Object type dimensions" on page 664.

Adding object type dimensions

Use the following instructions to define object type dimensions for generation in the Reporting Framework V6. V6 refers to the latest framework version, not to any specific OpenPages GRC Platform release number.

Procedure

1. Click **Administration** > **Reporting Framework** > **Configuration**.
2. On the **Object Type Dimensions** table, click **Add**.
3. In the **Name** box, type a name for this object type dimension.
4. Optional: 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. Click **Create**.

What to do next

Update the reporting framework to effect the changes (see "Updating the reporting framework" on page 686).

Modifying object type dimensions

You have the option to 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. Click **Administration** > **Reporting Framework** > **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 220 on page 682).

Table 220: Modifying an Object Type Dimension

If you want to...	Then do this...
Change an object type	Click the **Choose Object Type** link for 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 for 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. Click **Save**.
5. Update the reporting framework to effect the changes (see "Updating the reporting framework" on page 686).

Enabling, disabling, and deleting object type dimensions

You can disable and then re-enable an object type dimension at a later time. When you delete an object type dimension, that object type dimension is permanently removed from the system and cannot be retrieved.

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

Procedure

1. Click **Administration** > **Reporting Framework** > **Configuration**.

2. In the **Object Type Dimensions** table, navigate to the row containing the object type dimension you want to disable, re-enable, or delete.
3. Under the **Actions** column in the same row for that object type dimension, do one of the following:
   - Click **Enable** or **Disable** (the link toggles between "Disable" and "Enable" depending on the selected action).
   - Click **Delete**.

What to do next
Update the reporting framework to effect the changes (see “Updating the reporting framework” on page 686).

Generating the reporting framework

When you generate the Reporting Framework V6, the packages for all or selected framework models are published to the Cognos server with relationship and dimensional subnamespaces.

Note: You should not use IBM Cognos Framework Manager to modify the packages. The packages are dynamically created and recreated when you launch the OpenPages Reporting Framework Generator. If you made changes using IBM Cognos Framework Manager, those changes are lost when you launch the OpenPages Reporting Framework Generator. If you would like to create a custom Cognos package, see your OpenPages Managing Consultant.

Regenerating the reporting framework

The following table lists the changes that require you to regenerate the reporting schema and the reporting framework:

Table 221: Regenerating the reporting schema and the reporting framework.

This type of change...	**Requires this to be regenerated...**	
	Reporting schema	**Reporting framework**
Adding a new field to a field group.	No	Yes
Adding a new object type.	No	Yes
Adding a new association between object types.	No	Yes
Removing object types or attributes. For information, see “Deleting a custom object type” on page 189.	Yes	Yes
Encrypting a long string (CLOB) field.	No	Yes
Enabling facts or dimensions.	No	Yes
Defining, modifying, or deleting business entity recursive object levels.	No	Yes
Removing a field from a field group.	No	Yes
Disabling an association between object types.	No	Yes
Disabling facts or dimensions.	No	Yes

Table 221: Regenerating the reporting schema and the reporting framework. (continued)		
This type of change...	**Requires this to be regenerated...**	
	Reporting schema	**Reporting framework**
Switching the security model. **Note:** Switching the security model after data is loaded or migrated into the system is not recommended and requires assistance from the OpenPages Professional Services team.	Yes	Yes
Changing the value of the **Populate past periods** setting. For information, see "Populating past reporting periods" on page 91.	Yes	No
Changing any setting used to compose URL links in the reporting schema, for example, the Host, Port, and Protocol settings. For information about updating the reporting schema, see "Updating URL host pointers for reports" on page 478 if you want to run the `RPS_Update` SQL script or "Creating or recreating the reporting schema" on page 91 if you are update manually.	Yes	No
Adding an index to an RT_column by using the **Settings** > **Platform** > **Reporting Schema** > **Create Index on Fields** setting.	Yes	No
Configuring the triangles setting. For information, see "Triangle object relationships" on page 663.	Yes	No
Changing an enumerated field from single-valued to multivalued and there is data in the field (DB2 only).	Yes	No

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

Reporting framework permissions

Before performing any actions on a reporting framework, you must have specific application permissions set on your account.

For more information, see "Types of application permissions" on page 32).

Table 222: Reporting framework permissions	
This application permission...	**Is used to...**
Reporting Framework	Update all or selected components of the reporting framework.
Reporting Framework Configuration	Configure facts and dimensions

Accessing the reporting framework

To update components of the reporting framework or to configure facts and dimensions, you must access the reporting framework.

Before you begin

To update or configure the reporting framework, you disable System Administration Mode (for more information, see "Enabling and disabling System Administration Mode" on page 17).

Make sure the following application permissions are set on the user account. For information, see "Reporting framework permissions" on page 684.

Procedure

1. Log on to IBM OpenPages GRC Platform as a user with the correct application permission set.
2. Click **Administration** > **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 for all or selected framework models.
   - **Configuration** — to configure facts and dimensions, object type dimensions, and date dimension types.

Choosing update options in the reporting framework

When you generate the Reporting Framework V6 or a Legacy Reporting Framework, you can choose to update all or particular components of the reporting framework.

If you want to continue using the Legacy Reporting Framework for certain reports with systems that were upgraded from version 5.x or earlier, you can specify the Legacy Framework Generation options.

Table 223 on page 685 lists the various options for updating the reporting framework.

Table 223: 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 model in the relational model.
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. For information about custom query subjects, see the *IBM OpenPages GRC Report Author's Guide* on your documentation media.
All Models	Reporting Framework V6	Generates the component you select (Framework Model, Labels, Facts and Dimensions, or Custom Query Subjects) for all framework models that are enabled.
Selected Models	Reporting Framework V6	Generates the component you select (Framework Model, Labels, Facts and Dimensions, or Custom Query Subjects) for selected framework models. The framework models must be enabled.

When you update the reporting framework, any changes to the reporting schema are reflected in Cognos. After the reporting framework model in Cognos is updated, report authors can create and modify reports based on these changes. If the reporting framework is not updated, external reports such as those built with Cognos will not be able to access the updated reporting schema.

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 Cognos tool, you would update the reporting framework through the administrative application interface.

After the Cognos reporting framework is updated, a report author could then create new (or modify existing) reports that contained the new fields or relationships. For more information about the Cognos reporting framework, see the *IBM OpenPages Report Author's Guide*.

Updating the reporting framework

After the reporting schema has been updated, the reporting framework must be updated as well to propagate the changes to the Cognos reports. Whenever you update the reporting framework, you need to revalidate reports. Failing to do so may result in reporting errors.

Note: This procedure assumes that you have created a new reporting schema.

Procedure

1. Access the **Reporting Framework Operations** page (see "Accessing the reporting framework" on page 684).
2. Disable System Administration Mode if it is enabled (for details, see "Enabling and disabling System Administration Mode" on page 17).
3. On the **Reporting Framework Operations** page, click **Update**.
4. In the **Reporting Framework Generation** window, complete the following steps:
   a) Under **Framework Generation**, select the **Framework Model**, **Labels**, **All Models** or **Selected Models** options and any additional options 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**.

      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 updates the percentage of completion.

Viewing reporting framework details

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

Before you begin

Complete the following steps to view reporting framework details:

Procedure

1. Access the Reporting Schema. Log on to the IBM OpenPages GRC Platform application user interface as a user with the **Reporting Schema** application permission set.
   a) From the menu bar, select **Administration** and click **Reporting Schema**.
2. On the **Reporting Framework Operations** tab, click the name of the operation.
3. On the **Operation Detail** pane, click **View Log**.

The log message detail page appears.

4. If a sub-operation exists, it is listed in on the **Sub Operations** pane.
   a) To view sub-operation details, click the name of the sub-operation.
   b) To view log details, click **View Log**.

Chapter 26. IBM OpenPages GRC Platform connectors

You can leverage information from across the business by using connectors to collect information from third-party solutions.

IBM OpenPages GRC Platform connectors use IBM Tivoli Directory Integrator to pull data into OpenPages

IBM Tivoli Directory Integrator is a general-purpose integration tool that you can use to build integrations between multiple data sources and targets. Connectors must be imported into an IBM Tivoli Directory Integrator workspace. (IBM Security Directory Integrator is the latest name for IBM Tivoli Directory Integrator. You might see TDI and SDI used interchangeably in the documentation.)

The version included with IBM OpenPages GRC Platform is IBM Tivoli Directory Integrator 7.1.1.4. This version is supported by the QRadar integration package and by IBM OpenPages GRC SDI Connector for UCF Common Controls Hub.

Attention: TDI must be at the 7.1.1.4 level.

IBM QRadar integration

IBM OpenPages GRC Platform includes an IBM QRadar integration package. QRadar is a separate stand-alone enterprise-level application. It is not included with IBM OpenPages GRC Platform.

IBM QRadar is a SIEM (Security Information and Event Management) system that contains relevant data for the Incident object type in OpenPages. In QRadar, this data is called an Offense.

Data can be pulled from QRadar, initiated by IBM Tivoli Directory Integrator (TDI), then mapped one-to-one to Incidents in IBM OpenPages GRC Platform.

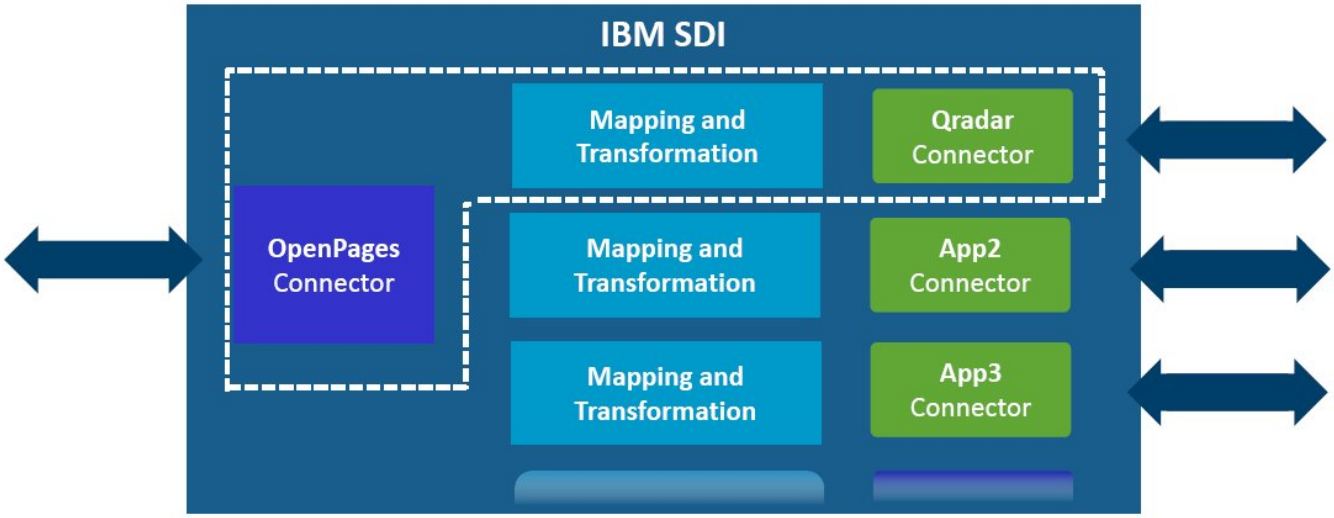


Figure 34: How OpenPages and QRadar work together

Using the QRadar integration project

The IBM QRadar integration project is an optional project that you can install to import Offenses from QRadar and create them as Incidents in the IBM OpenPages GRC Platform.

Before you begin

You must complete the following steps to install and configure the QRadar integration project before you begin. For more information, see "Installing QRadar integration" in the *IBM OpenPages GRC Installation and Deployment Guide*.

About this task

Connectors are plug-ins for TDI that are reusable components. OpenPages GRC Platform has one connector developed for OpenPages GRC Platform functionality. The connector is generic to any OpenPages GRC Platform object type and field type.

You can use QRadar filtering so that the relevant subset of Offenses can be managed in the context of the impact on your business. For example, you can configure the connector to import only Offenses that are open, or based on the date.

The SIEM API documentation is available in the QRadar Console. This can provide guidance on what to specify for the filter and the fields, (specified by the qradarFilter and qradarFields properties in the `connector.properties` file).

Procedure

1. Ensure IBM QRadar is installed. IBM QRadar is a separate enterprise-level application. It is not included with OpenPages GRC Platform.
2. Install IBM Tivoli Directory Integrator 7.1.1, followed by the IBM Tivoli Directory Integrator 7.1.1.4 fix pack 4, from the OpenPages GRC Platform installation media.
3. Configure Tivoli Directory Integrator to connect to QRadar.
4. Configure the property files.
5. Deploy the assembly line.

   Attention: The assembly line will not run when the OpenPages GRC Platform user that is configured to run the assembly line has left System Admin Mode enabled in OpenPages GRC Platform. You must ensure that System Admin Mode is disabled to run the assembly line.
6. The results of running the assembly line show up as new or updated Incident objects, as viewed from the OpenPages GRC Platform **Events** > **Incidents** menu option.

Configuring email notifications to be sent from the QRadar assembly line connector components

Both of the `QRadarOffensesToIncidents` assembly line connector components are able to send email notifications to alert people such as the IBM Tivoli Directory Integrator (TDI) administrator when errors or exceptions occur during the execution of the `QRadarOffensesToIncidents` assembly line.

About this task

To enable this capability, the three SMTP properties in the `connector.properties` file must be configured. Then, when an error or exception occurs, in addition to the error-level message getting logged to the TDI log file or to the TDI console, an email with the log message is also sent to the email addresses configured in the SMTP mailTo property of the `connector.properties` file.

Email messages can be sent from either the QRadar API connector component or the IBM OpenPages GRC Platform connector component of the `QRadarOffensesToIncidents` assembly line. Also, the IBM OpenPages GRC Platform connector automatically sends warn-level messages if there are issues with the validity of the primary parent ID supplied to the IBM OpenPages GRC Platform connector when

attempting to create a new IBM OpenPages GRC Platform object. Updating an existing IBM OpenPages GRC Platform object does not require a primary parent ID to be specified.

Procedure

1. Configure the mailTo property of the `connector.properties` file.

   The email address to use for sending email notifications about errors and exceptions that occur in the assembly line connectors. One or more email addresses can be specified as a comma-separated list. For example, `mailTo=user1@acme.com,user2@acme.com`.
2. Configure the smtpPort property of the `connector.properties` file.

   The SMTP port to use for sending email notifications about errors and exceptions that occur in the assembly line connectors. The default port to use for an SMTP server is 25.
3. Configure the smtpHost property of the `connector.properties` file.

   The SMTP host to use for sending email notifications about errors and exceptions that occur in the assembly line connectors. Specify either an IP name or IP address. For example, `smtpHost=mySmtpHost.acme.com` or `smtpHost=192.168.10.20`.

Specifying a primary parent ID to the IBM OpenPages GRC Platform connector

IBM OpenPages GRC Platform objects that are created by the IBM OpenPages GRC Platform connector must have a primary parent ID.

Procedure

There are three ways to supply a primary parent ID to the IBM OpenPages GRC Platform connector component, described in the order in which they are searched for:

- Provide the object resource ID of an existing suitable parent object as a string value in the work.primary_parent_id property in the output mapping:

  The following graphic shows the work.primary_parent_id property in the output mapping:

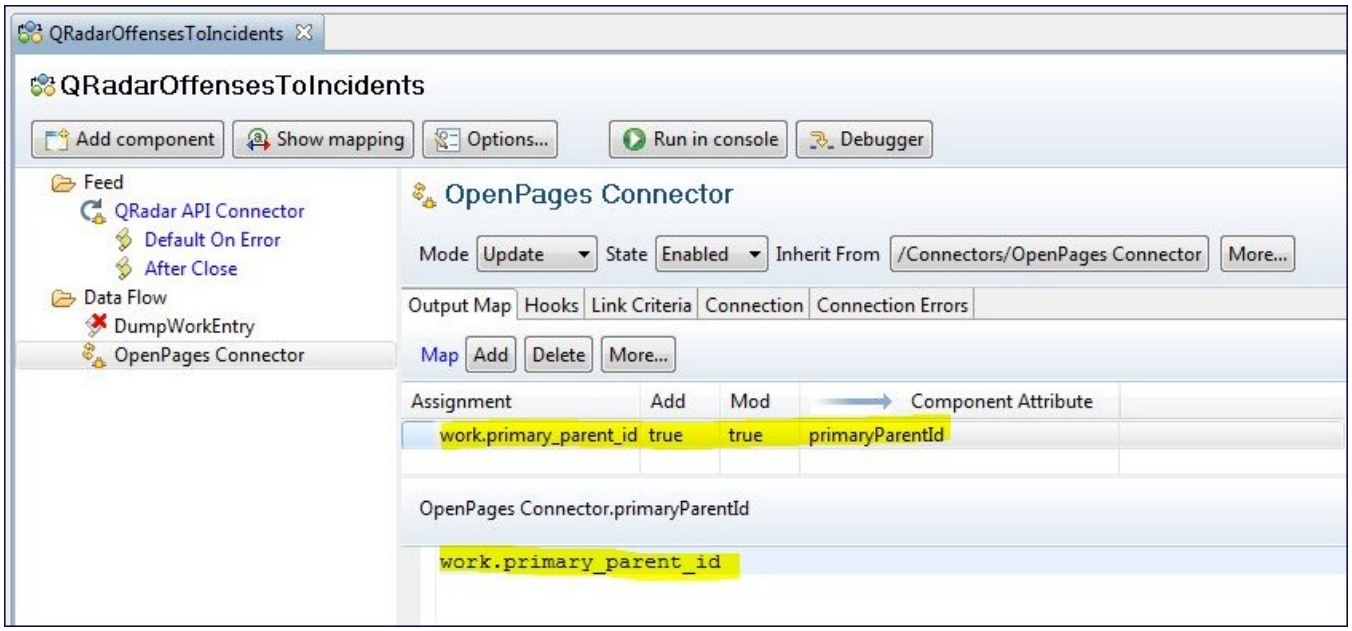


Figure 35: The work.primary_parent_id property in the output mapping:

The value must be a number, enclosed in double quotes, and should be the object resource ID of a suitable IBM OpenPages GRC Platform parent object. A null or empty value is ignored. This technique enables the use of a different primary parent ID for each object being created.

- If a work.primary_parent_id property value is not supplied in the IBM OpenPages GRC Platform connector output mapping from the preceding technique, then the IBM OpenPages GRC Platform connector looks for non-null values of the following two properties in the output mapping to derive the primary parent ID of a parent object for the new object being created:
  - work.parent_type: the GRC object type of the parent object
  - work.parent_location: the relative location of the GRC parent object instance

  The following graphic shows the primary parent ID derived from the non-null values of the two properties work.parent_type and work.parent_location in the output mapping.

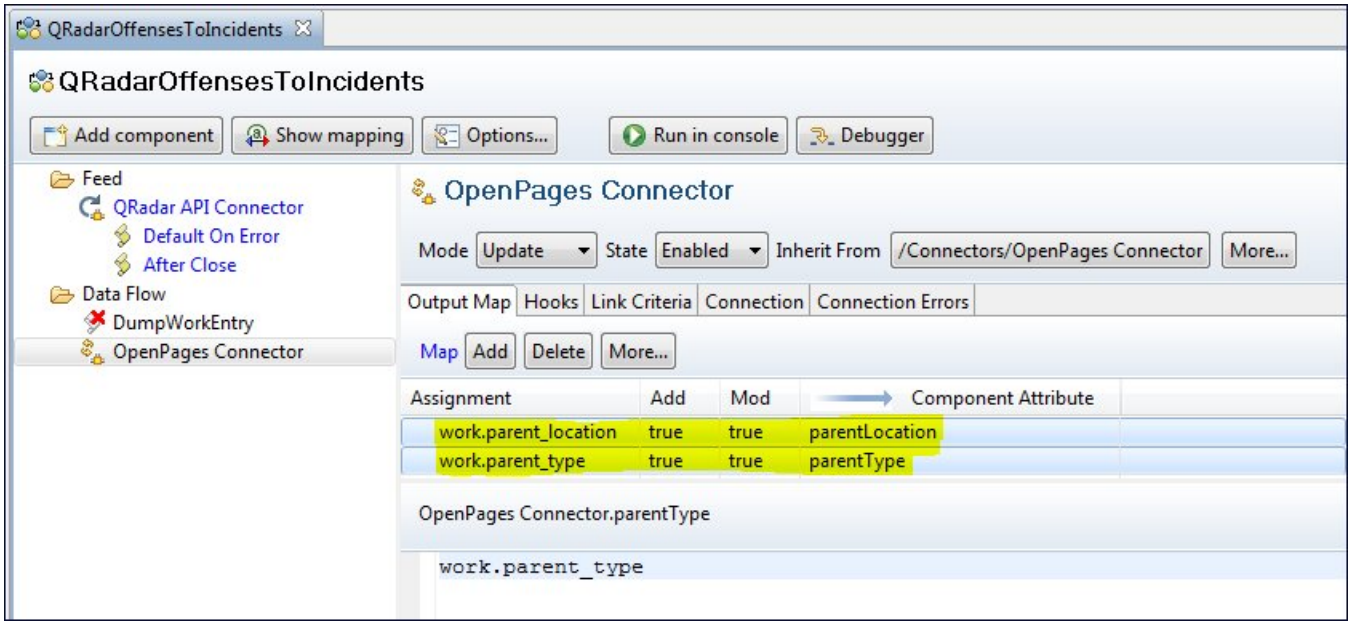


Figure 36: Primary parent ID derived from the non-null values of the two properties work.parent_type and work.parent_location in the output mapping

See the detailed descriptions and example values provided for the op_parentType and op_parentLocation properties in the `connector.properties` file, located in the `Runtime-qradar_integration` folder of the TDI `qradar_integration` project. If the values for these properties do not derive to a valid parent object, then they are ignored.

The following graphic shows a detail from the `connector.properties` file:

```
# op_parentType
#
# The GRC object type of the parent object to use for all newly created objects.
#
# Example:    op_parentType=SOXBusEntity
op_parentType=SOXBusEntity

# op_parentLoc
#
# The relative location of the GRC parent object instance to use as the parent for all
# newly created objects. For Business Entity parents, specify all of the segments of the
# Folder location except for the root.  For non-Business Entity parents, specify all of
# the segments of the folder location except for the root and append the name of the parent
# object as the last segment of the location. The op_parentLoc property should start with
# a leading '/' character; do not include any spaces around the '/' characters.
#
# Example 1: If a business entity object named 'Audits' has a Folder value of
#    BusinessEntity / Library / Audits
# then specify the relative location, that is, just the segments of the pathname under the
# root folder (in this case the root folder is 'BusinessEntity'), as follows:
#    opParentLoc=/Library/Audits
#
# Example 2: If a business entity object named 'Asia Pacific' has a Folder value of
#    BusinessEntity / Global Financial Services / Asia Pacific
# (where 'BusinessEntity' is the root in the Folder property) then specify the property as:
#    op_parentLoc=/Global Financial Services/Asia Pacific
#
# Example 3: If a non-business entity Risk object named 'Risk1' has a Folder value of
#    Risks/test1
# (where 'Risks' is the root in the Folder property) then specify the property as
# follows, being sure to append the parent object's name (in this example the parent
# object's name is 'Risk1'):
#    op_parentLoc=/test1/Risk1
#
op_parentLoc=/Library/Audits
```

Figure 37: A detail from the `connector.properties` file

This technique enables the use of a different primary parent ID for each object being created.

- If the properties in the preceding two techniques are not provided, then the IBM OpenPages GRC Platform connector uses the default primary parent ID derived from the op_parentType and op_parentLocation properties defined in the `connector.properties` file, located in the `Runtime-qradar_integration` folder of the TDI `qradar_integration` project. The values in the `connector.properties` file are processed once per assembly line execution, and the resulting derived value serves as the default primary parent ID to use if the properties in the two preceding sections are not provided.

If the values for these properties do not derive to a valid parent object, then there will be no default value available for the duration of the assembly line execution. See the detailed descriptions and example values provided for each of these properties in the `connector.properties` file, located in the `Runtime-qradar_integration` folder of the TDI `qradar_integration` project.

Specifying currency values to the IBM OpenPages GRC Platform connector by the output mapping

You can specify currency values in the IBM OpenPages GRC Platform connector output mapping as strings (enclosed with quotation marks) by using a standard format.

About this task

The amount is specified first, followed by a vertical bar, followed by the ISO code. White space is allowed. The entire string must be enclosed in quotation marks.

Procedure

Supply the currency values in the IBM OpenPages GRC Platform connector output mapping as strings, that is, enclosed with quotation marks, by using the following format: "*<amount>*|*<isoCode>*"

- Examples of valid currency values in the output mapping: "123.45|AUD" or "321 | USD"
- Example of an invalid currency value in the output mapping because the enclosing quotation marks are missing: 123.45|AUD
- Example of an incomplete currency value in the output mapping because the ISO code is missing; when this situation occurs, the default currency that is configured in IBM OpenPages GRC Platform is used: "123 | "

Specifying date values to the IBM OpenPages GRC Platform connector via the output mapping

Date values should be specified as **java.util.Date** objects in the IBM OpenPages GRC Platform connector output mapping.

IBM OpenPages GRC SDI Connector for UCF Common Controls Hub integration

IBM OpenPages GRC Platform includes IBM OpenPages GRC SDI Connector for UCF Common Controls Hub. UCF Common Controls Hub is a separate stand-alone web application. It is not included with IBM OpenPages GRC Platform.

UCF is a database of regulatory compliance documents. The regulatory documents are divided into parts, which can then be used by APIs. UCF Common Controls Hub is the web portal to the UCF data.

Data can be pulled from UCF (initiated by IBM Tivoli Directory Integrator), then mapped one-to-one to object types in IBM OpenPages GRC Platform.

Note: IBM Security Directory Integrator is the latest name for IBM Tivoli Directory Integrator. You might see TDI and SDI used interchangeably in the documentation.

Table 224: UCF object type mappings

Object type in UCF	Object type in OpenPages
Authority documents	Mandates
Citations	Submandates
Controls	Requirements

A mandate can have one or submandates. A submandate can have zero or more requirements. A requirement can be related to multiple submandates from different mandates.

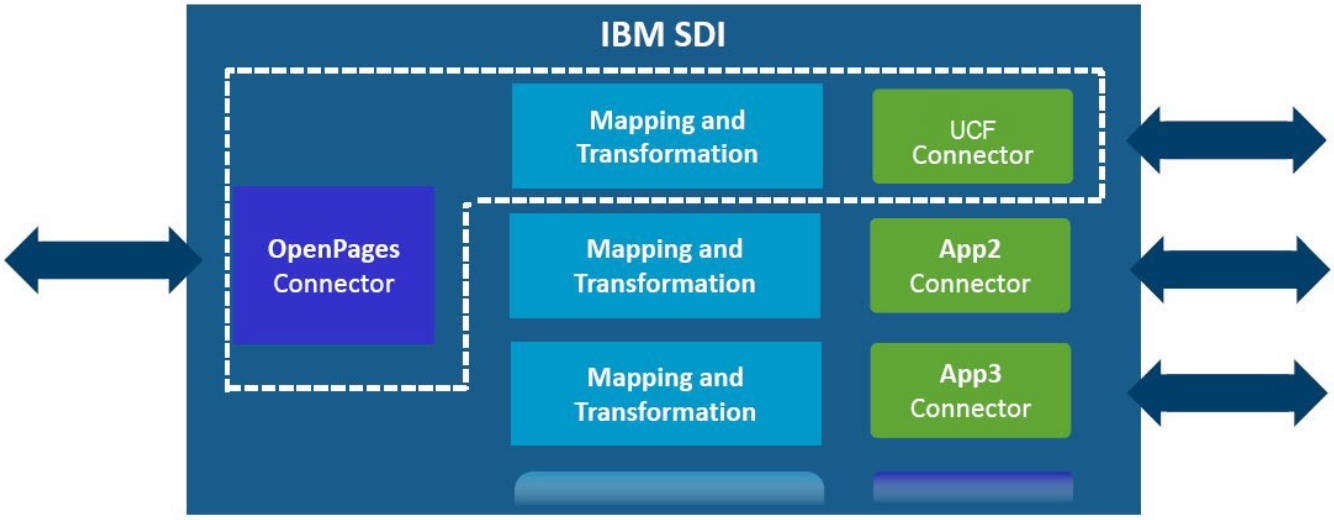


Figure 38: How OpenPages and UCF work together

Run the UCF assembly lines

Run the UCF assembly lines to import objects from UCF Common Controls Hub into OpenPages GRC Platform.

You must install and configure the UCF connector before you begin. For more information, see "Installing UCF integration" in the *IBM OpenPages GRC Installation and Deployment Guide*.

Run the assembly lines in the following order. Wait for each assembly line to finish before you run the next assembly line:

- UCF Authority Documents to OP Mandates
- UCF Citations to OP Submandates
- UCF Controls to OP Requirements

To run an assembly line, right-click it in the TDI Configuration Editor and click **Run AssemblyLine**. To view the log, click  .

Note: The UCF connector assembly lines do not support Delta mode.

You can schedule the assembly lines to run by using the IBM Tivoli Directory Integrator scheduler. Set up the scheduler so that each assembly line completes before the next begins.

Attention: The assembly lines will not run when System Admin Mode (SAM) is enabled in OpenPages GRC Platform. The assembly lines write data to the OpenPages database, and System Admin Mode prevents write operations. Ensure that System Admin Mode is disabled before you run the assembly lines.

If you encounter errors about missing impact zones or guidance areas, see “Update business entities, fields, and field groups” on page 697.

To view the UCF objects in OpenPages GRC Platform, go to **Compliance** > **Mandate Overview**. Expand **Library** > **UCF**.

Changing the connection information

You can change the connection information that the UCF connector uses to connect to IBM OpenPages GRC Platform and to UCF Common Controls Hub. You configure the connection information by updating property files and by entering passwords in the Tivoli Directory Integrator Configuration Editor.

About this task

The UCF connector includes two text files that contain the assembly line properties.

The property files are in the **Runtime-ucf_integration** folder of the **ucf_integration** project.

op_client.properties
The `op_client.properties` file stores the connection information for OpenPages.

passwords.properties
The `passwords.properties` file contains the OpenPages password and your UCF token. The values are encrypted.

Note: Do not edit this file. Set the values by using the Tivoli Directory Integrator Configuration Editor.

Procedure

1. From the Tivoli Directory Integrator Configuration Editor, open the **ucf_integration** project.
2. In the Navigator pane, expand **Runtime-ucf_integration**.
3. Right-click the `op_client.properties` file and click **Text Editor**.
4. Set or change the property values.

Table 225: Properties in the `op_client.properties` file

Property	Description
`op_api_root`	The OpenPages REST API root The default (typical) value is `/grc/api`. The `op_api_root` is appended to the `op_url` to form the full URL to access the OpenPages REST API.
`op_url`	The OpenPages URL Use the format `https://<host>:<port>`
`op_user`	The OpenPages user name that the UCF connector uses to log in to OpenPages Use an account with administrative privileges. The user account must have security permissions to create and update the mandate, submandate, and requirements object types.

For example:

```
op_api_root=/grc/api
op_url=https://op_server:10111
op_user=ucf
```

5. Save the changes and exit the text editor.
6. Right-click the `password.properties` file and click **Text Editor**.
7. Type the password of the OpenPages user that you used in the `op_client.properties` file.
8. Enter your UCF Common Controls Hub token in the `ucf_api_token` parameter.

To get your token, log in to UCF Common Controls Hub. Click **Settings** > **API Manager** > **API Keys**. Click **Create Credentials**.

If you are unable to create a token, contact UCF Common Controls Hub.

9. Save the changes and exit the text editor.

   The values in the `password.properties` file are automatically encrypted.

10. Refresh the property files and the connectors with the updated connection information.
    a) In the Navigator pane, expand **Resources** > **Properties**.
    b) Right-click **op_client**, and then click **Open**.
    c) Click **Read properties from Server**, and then click **Send properties to Server**.
    d) Click **Save**, and then close the window.
    e) Right-click **passwords**, and then click **Open**.
    f) Click **Read properties from Server**, and then click **Send properties to Server**.
    g) Click **Save**, and then close the window.

Update business entities, fields, and field groups

If UCF Common Controls Hub adds new control impact zones or adds new authority document guidance areas, you need to update IBM OpenPages GRC Platform.

You need to update OpenPages in the following cases:

- The assembly line reports that an impact zone is missing.

  In this case, you need to add a business entity with the same name as the missing control impact zone. The parent of the new business entity must be `/Library/UCF/Harmonized Controls`.

  For example: `/Library/UCF/Harmonized Controls/<Impact Zone Name>`

- The assembly line reports that a mandate cannot be created because an authority document's guidance area could not be found.

  In this case, you need to add a business entity with the same name as the authority document's guidance area. The parent of the new business entity must be `/Library/UCF/Authority Documents`.

  For example: `/Library/UCF/Authority Documents/<Guidance Area Name>`

  Next, add the new business entity name as an enumerated string value to the fields UCF-Mand:UCF Category, UCF-SubMand:UCF Guidance Area, and UCF-Req:UCF Guidance Areas.

You can add new business entities in OpenPages. Alternatively, you can use FastMap to import them.

IBM Tivoli Directory Integrator (TDI) techniques

If you use the IBM OpenPages GRC Platform connectors, there are TDI techniques that might help you.

Scheduling IBM Tivoli Directory Integrator

IBM Tivoli Directory Integrator (TDI) has a built-in capability for scheduling. Each assembly line can have one or more schedules. TDI can run in a daemon mode between runs, or shut down completely. Assembly lines can also be run on demand by the command line.

In the TDI Configuration Editor, right-click an assembly line and select **Create Schedule**.

If you are using the UCF connector, schedule the assembly lines in the following order. Schedule the assembly lines so that each completes before the next begins.

- UCF Authority Documents to OP Mandates
- UCF Citations to OP Submandates
- UCF Controls to OP Requirements

For more information about scheduling assembly lines, see the IBM Tivoli® Directory Integrator Knowledge Center topic Scheduling AssemblyLines(http://www-01.ibm.com/support/knowledgecenter/SSCQGF_7.1.1/com.ibm.IBMDI.doc_7.1.1/SchedulingassemblyLines.htm).

TDI command line tips

You can run the assembly lines on your local or remote server where IBM Tivoli Directory Integrator (TDI) is installed.

To run commands on a remote TDI server, you must have TDI 7.1.1.4 installed on your local system. When entering TDI commands on the local server to execute on a remote TDI server, be sure to include the -h <hostname> command switch.

Attention:

- If changes are made to any of the properties files used by the connector components and you are running the `tdisrv` service, the `tdisrv` service must be stopped and restarted for those changes to take effect.
- Logging for TDI running as a service is written to the `ibmdi.log` file in the installed TDI area where the service lives. For example, on a Windows-based system, this is *<TDI-install-root>*`/win32_service/logs/ibmdi.log` by default.
- When you run an assembly line by using the TDI Configuration Editor, the log entries are put into the *<TDI-solutions-root>*`/logs/ibmdi.log` by default.

Here are some examples of commands that you can run against your imported configuration. Note the use of the -h <hostname> switch when the command is intended to run on a remote TDI server configuration. Also, the use of the `ibmdisrv` command is not typically used, but is included here as an example of how it can be used:

- `tdisrvctl -v -op start -c C:\TDI_Solutions\workspace\qradar_integration \Runtime-qradar_integration\qradar_integration.xml -r QRadarOffensesToIncidents`
- `tdisrvctl -v -h <hostname> -op start -c C:\TDI_Solutions\workspace \qradar_integration\Runtime-qradar_integration\qradar_integration.xml -r QRadarOffensesToIncidents`
- `ibmdisrv -c "C:\TDI_Solutions\workspace\qradar_integration\Runtime-qradar_integration\qradar_integration.xml" -r "QRadarOffensesToIncidents"`

Troubleshooting the assembly line "Connection refused" error

When you start the IBM Tivoli Directory Integrator (TDI) Configuration Editor, or when you run TDI commands from a command line, you might encounter an error that says the connection to your TDI server is refused.

About this task

This error can be caused by running more than one instance of either the TDI Configuration Editor or the `tdisrv` service at the same time on the same server.

Procedure

1. Check for any program that is using port 1099 already by using the following commands:
   - Windows: `netstat -an | findstr 1099`
   - UNIX: `netstat -an | grep 1099`
2. If the output of this command is not empty, determine which process is already using port 1099 and stop that process. If the process is already stopped, reenter the command after a minute or two to ensure that the ports are no longer in use. You might need to repeat the `netstat` command a few times before the output is empty.

Chapter 27. Configuring questionnaire assessments

You can use the questionnaire assessments to assess risk and compliance or to collect information for specific processes and asset risks. This capability streamlines, standardizes, and centralizes the collection of questionnaire-based assessment information.

Configuring questionnaire assessments

To use questionnaire assessments, you set up user permissions for users. You can also configure the email server so that lifecycle triggers send emails to lifecycle assignees. You can customize two visual elements on questionnaire assessments: the logo in the header and the introduction text on the landing page. These elements are displayed on all questionnaire assessments regardless of the questionnaire template and program that is used to create the questionnaire assessments.

Procedure

1. Configure the email server that is used to route mails to lifecycle assignees. For information see "Set the mail server address" on page 322.
2. Verify that users who create and launch programs have the following permissions:
   - Read/write/associate access to Questionnaire Template objects.
   - Read/write access to the objects used by Questionnaire Templates: Section Templates, SubSection Templates, and Question Templates.
   - Read/write/associate access to Program objects.
   - Read/write/associate access to Questionnaire Assessment objects.
   - Read/associate access to assets.
3. Verify that users who complete and review questionnaire assessments have the following permissions:
   - Read access to the objects used by questionnaire templates: Questionnaire Templates, Section Templates, SubSection Templates, and Question Templates.
   - Read access to Program objects. Required for four-stage lifecycle because the program owner is at one point the lifecycle assignee for questionnaire assessments.
   - Read/write/associate access to Questionnaire Assessment objects. You can do this with Record Level Security (RLS), where the current lifecycle assignee has the questionnaire assessment, or with the role template.
   - Read/write/associate/delete access to SOXDocument for attachments.
   - Read access to assets.
4. Customize the logo on the questionnaire assessment to be your company logo. File specifications are as follows:
   - Size: 133 pixels wide by 40 pixels high
   - Type: png
   - Name: `logo.png`
   - Folder location: `../sosa.war/image/questionnaire/`

     Changes to the logo file can be overwritten in subsequent upgrades.

   Copy the file to the folder location. No further setup is necessary. If you do not customize the logo, the system displays the product name in the header rather than a logo.
5. Customize the introduction text that is displayed on the landing page when a respondent opens a questionnaire assessment. Write the text and save it in the

`questionnaire.intro.label.informationDetails` token under **Administration** > **Application Text** > **Labels**.

Chapter 28. Configuring the approval app

The approval app is an optional feature that leverages the power of IBM OpenPages GRC Platform and provides an easy-to-use interface for quickly taking action on a review, approval, or attestation request with confidence and full knowledge of the context surrounding the request. The approval app works with objects that are set up for the configurable lifecycle.

By using the approval app, a casual or infrequent user of IBM OpenPages GRC Platform is now able to make well-informed decisions for GRC tasks guided by information from the system quickly and easily, without the need for extensive training in OpenPages. If you want to see all of the items sent to you in the approval app, you can go to your To Do list by clicking the IBM OpenPages GRC Platform logo. You simply make the decision (or respond to certification language or questions), with your comments if necessary, and click the relevant button to submit. You can use this feature on tablets and mobile devices as well, for increased flexibility.

Configuring the JSON file for the approval app

You use the `deck_config.json` file as a place to configure object types, fields, and so on, for the approval app.

About this task

The `deck_config.json` is preconfigured to be ready for use. If you want, there are other changes that you can make. For more information, see “Customizing the JSON file for the approval app ” on page 707.

The following table contains the property list and instructions for the `deck_config.json` file properties.

Table 226: Properties in `deck_config.json`

Property	Needed	Parent Property	Description	Value (example)
profile	exactly 1	root property	Name of the OpenPages profile used by the approval app	approval app
objectTypes	1 to many	root property	List of the approval app supported object types (system names)	SOXControl
objects	1 per objectType	root property	List of properties for each object type	[{}]
type	1	objects	Type of the OpenPages object system name	SOXControl
fieldTitle	1	objects	Field to be used as the name of the object	Name
fieldDesc	1	objects	Field to be used as the description of the object	Description
lifecycle	1	objects	List of lifecycle properties for object	{}
enabled	1	lifecycle	Boolean to enable object for the approval app	true

Table 226: Properties in `deck_config.json` (continued)

Property	Needed	Parent Property	Description	Value (example)
stageMap	1	lifecycle	List of the approval app enabled lifecycle stages	{}
"Attestation"	1 to many	stageMap	List of properties for the approval app enabled lifecycle stage	{}
showInList	1	"Attestation"	Boolean to display stage in the approval app	true
questionFieldLists	1	"Attestation"	List of question field properties for certification	[{}]
rule	1 to many	questionFieldLists	Rule to determine whether a question is used	default
fields	1 per rule	questionFieldLists	List of question fields for certification	[{}]
systemName	1 to many	fields	OpenPages system name of certification question field	OPSS-Ctl-Cert:DesEff
displayType	1 per systemName	fields	the approval app-specific display type for the certification field	Text Area
widgetList	1	objects	List of properties for the controlling views in OpenPages	[{}]
attachmentList	0 or 1	widgetList	Controls the display of the **Files** list under the **Related Content** section in the approval app. • `show`: Always display the **Files** list. • `hide`: Always hide the **Files** list. If you want to show files or links, you must add them to the profile view of the object. • `auto`: Shows the **Files** list. But if the profile view includes files or links, hides the **Files** list. Default: `auto`	show

Table 226: Properties in `deck_config.json` (continued)

Property	Needed	Parent Property	Description	Value (example)
name	1	widgetList	Name of the approval app section controlled by a view	details
type	1	widgetList	Type of the OpenPages view controlling the approval app section	ActivityView
activityView	1	widgetList	Name of the OpenPages view controlling the approval app section	OP-Deck-Control
parentViews	0 to 1	widgetList	List of OpenPages views displayed in the approval app Related Content section	[{}]
type	1 to many	parentViews	Type of the OpenPages parent object system name	SOXRisk
activityView	1 per type	parentViews	Name of the OpenPages view controlling the approval app section	OP-Deck-LE-Risk
dueDateGroup	1	root property	List of properties for grouping the items in the approval app	{}
defaultField	1	dueDateGroup	Field to be used as the Due Date field	OPLC-Std:LCDueDate
group	0 to 1	defaultField	List of properties controlling the date ranges for grouping in the approval app	[{}]
number	1 to many	group	Date range for grouped items	14
unit	1 per number	group	Unit of measurement for group date range (day, month, or year)	day
maxTodoObjects	1	root property	Number of items to be displayed in the approval app	25

Debugging the `deck_config.json` file

You can debug the `deck_config.json` file by logging into OpenPages as an administrator and pasting a URL (`http://<yourIP>:<port>/openpages/app/deck/reloadConfig`) in the browser. If there is an error in the `deck_config.json` file, a message displays that shows details about the error, such as the error number, exception type, line number, and error description. The error is logged in the aurora log as well. You can then locate and fix the error in the `deck_config.json` file.

To perform this procedure, you must have the **OpenPages Platform 3** profile associated with your user name.

Procedure

1. Click **Administration** > **Manage System Files** > **SysXMLDocument**.
2. Open the `End User Applications Config` folder to find the `deck_config.json` file.
3. Configure the `deck_config.json` file according to the preceding table.

   The following example shows a typical `deck_config.json` file.

```
{
    "profile": "Deck",
    "objectTypes" : ["SOXControl","SOXIssue","LossEvent","Incident"],
    "objects" : [
        {
            "type" : "SOXControl",
            "fieldTitle" : "Name",
            "fieldDesc" : "Description",
            "lifecycle" : {
                "enabled" : true,
                "stageMap" : {
                    "Attestation" : {
                        "showInList": true,
                        "questionFieldLists" : [
                            {
                                "rule" : "default",
                                "fields" : [{
                                        "systemName":"OPSS-Ctl-Cert:DesEff",
                                        "displayType":"Radio Button/Checkbox"
                                    },
                                    {
                                        "systemName":"OPSS-Ctl-Cert:DesEffExplain",
                                        "displayType":"Text Area"
                                    },
                                    {
                                        "systemName":"OPSS-Ctl-Cert:DocAccurate",
                                        "displayType":"Radio Button/Checkbox"
                                    },
                                    {
                                        "systemName":"OPSS-Ctl-Cert:DocAccurateExplain",
                                        "displayType":"Text Area"
                                    },
                                    {
                                        "systemName":"OPSS-Ctl-Cert:OpEff",
                                        "displayType":"Radio Button/Checkbox"
                                    },
                                    {
                                        "systemName":"OPSS-Ctl-Cert:OpEffExplain",
                                        "displayType":"Text Area"
                                    },
                                    {
                                        "systemName":"OPSS-Ctl-Cert:Change",
                                        "displayType":"Radio Button/Checkbox"
                                    },
                                    {
                                        "systemName":"OPSS-Ctl-Cert:ChangeExplain",
                                        "displayType":"Text Area"
                                    }]
                            }
                        ]
                    }
                }
            },
            "widgetList" : [
                {
                    "name" : "details",
                    "type" : "activityView",
                    "activityView" : "OP-Deck-Control",
                    "parentViews" : [
                        {
                        "type" : "SOXRisk",
                        "activityView" : "OP-Deck-Control-Risk"
                        }
                    ]
                }
            ]
        },
        {
            "type" : "SOXIssue",
            "fieldTitle" : "Name",
            "fieldDesc" : "Description",
```

```
            "lifecycle" : {
                "enabled" : true,
                "stageMap" : {
                    "Close Request" : {"showInList": true},
                    "Due Date Change Request" : {"showInList": true}
                }
            },
            "widgetList" : [
                {
                    "name" : "details",
                    "type" : "activityView",
                    "activityView" : "OP-Deck-Issue"
                }
            ]
        },
        {
            "type" : "LossEvent",
            "fieldTitle" : "Name",
            "fieldDesc" : "Description",
            "lifecycle" : {
                "enabled" : true,
                "stageMap" : {
                    "Awaiting Approval" : {"showInList": true},
                    "Awaiting Approval L1" : {"showInList": true},
                    "Awaiting Approval L2" : {"showInList": true}
                }
            },
            "widgetList" : [
                {
                    "name" : "details",
                    "type" : "activityView",
                    "activityView" : "OP-Deck-LE",
                    "parentViews" : [
                        {
                        "type" : "SOXRisk",
                        "activityView" : "OP-Deck-LE-Risk"
                        }
                    ]
                }
            ]
        },
        {
            "type" : "Incident",
            "fieldTitle" : "Name",
            "fieldDesc" : "Description",
            "widgetList" : [
                {
                    "name" : "details",
                    "type" : "activityView",
                    "activityView" : "OP-Deck-Incident"
                }
            ],
            "lifecycle" : {
                "stageMap" : {
                    "Review" : {"showInList": true},
                    "Escalation Review": {"showInList": true}
                }
            }
        }
    ],
    "dueDateGroup" : {
        "group" : [{"number": 5, "unit": "day"},{"number": 30, "unit": "day"}]
    },
    "maxTodoObjects" : 25
}
```

Approval app certification questions

Approval app certification questions provide an opportunity to prompt a user taking a lifecycle action to respond to questions that certify the details of what they are agreeing to. Certification questions can also remind them of the requirements of the certification or attestation they are performing.

The following table shows the supported field data types:

Field data type	Supported	Details	Valid `deck_config.json` displayType value
Currency	X		
Enumerated String	X	Single-select only	Radio Button/Checkbox
Simple String	X		Text and Text Area
Long String	X	Medium String Size only	Text and Text Area

Attention:

- Certification questions display the field guidance as the Question in the approval app—not as the field label, as the field guidance does in OpenPages.
- For the approval app, if a field-level security (FLS) rule is applied on a question, the question is still displayed on the card page for the lifecycle stage that is configured in the `deck_config.json` file, even if the user does not meet the FLS rule to view the question. When the user submits the question, the user sees the following message: `You do not have permission to write on the field <field name>`.

The following list shows some example certification questions.

Certification Language without values
Use a single-select Enumerated String field. This causes the question to appear without any values to select.

Single select checkbox
Use a single-select Enumerated String field with a single value. This causes the question to appear with a single check box.

Make a follow up question required
Use Requiredness field dependencies in OpenPages.

Note: The approval app does not support both Requiredness and Visibility dependencies at the same time.

Hide a follow up question unless a specific Enum value is selected
Use Visibility field dependencies in OpenPages.

Note: The approval app does not support both Requiredness and Visibility dependencies at the same time.

For a transition, make the lifecycle comment or other Simple/Long string required

```
"<SOME_STAGE>" : {
 "transitionMap" : {
  "<SOME_TRANSITION>" : {
   "requiresValidation" : true
  }
 },
 "questionFieldLists" : [
  {
   "rule" : "default",
   "fields" : [{
     "systemName":"<COMMENT/OTHER FIELD NAME>",
     "displayType":"Text Area",
     "requiredValue" : "NON_EMPTY"
   }]
  }
 ]
}
```

Make a Simple/Long string field appear in a single-line text box

```
"<SOME_STAGE>" : {
 "questionFieldLists" : [
  {
   "rule" : "default",
```

```
   "fields" : [{
     "systemName":"<FIELD NAME>",
     "displayType":"Text"
   }]
  }
 ]
}
```

Make a Simple/Long string field appear in a multi-line text area

```
"<SOME_STAGE>" : {
 "questionFieldLists" : [
  {
   "rule" : "default",
   "fields" : [{
     "systemName":"<FIELD NAME>",
     "displayType":"Text Area"
   }]
  }
```

Customizing the JSON file for the approval app

The `deck_config.json` file is ready to use, but you can customize it.

About this task

The `deck_config.json` is preconfigured to be ready for use. If you want, there are changes that you can make. For example, the `parentViews` property is optional: its default value is 0, in which case no parent objects are shown even though the `parentViews` property supports multiple parent views.

This configuration example shows how to define what appears in the Related Content section for the Controller object.

```
"parentViews" : [
{
"type" : "SOXBusEntity",
"activityView" : "OP-Deck-Control-BE"
},
{
"type" : "SOXRisk",
"activityView" : "OP-Deck-Control-Risk"
}
]
```

The following examples show various cases of properties that are supported but might not be enabled by default.

Example: Grouping a To Do list for 5 and 30 days

```
"dueDateGroup" : {
  "group" : [{"number": 5, "unit": "day"},{"number": 30, "unit": "day"}]
 }
```

Example: Making the comment field a required field for specified transitions

The comments field is not required in the standard configuration, and users can transition in a detail page without adding a comment.

You might submit an action in the approval app and see a message similar to the following: `Success! Your <action> and comments have been submitted to <recipient>`, even though there are no comments.

You can configure the comment field to be a required field for specified transitions in the `deck_config.json` file. In the following case, the comment field is required for the Review De-escalate transition of the Escalation Review lifecycle stage.

```
                    "Escalation Review" : {
"transitionMap" : {
"Review De-escalate" : {
"requiresValidation" : true
}
```

```
},
"questionFieldLists" : [
{
"rule" : "default",
"fields" : [{
"systemName":"OPLC-Std:LCComment",
"displayType":"Text Area",
"requiredValue" : "NON_EMPTY"
}]
},
{
"rule" : "default",
"fields" : [{
"systemName":"DECK-Questions:EnumQuestion",
"displayType":"Radio Button/Checkbox"
}]
}
]
}
```

Example: Approval app stage with certification questions

```
"stageMap" : {
     "Attestation" : {
      "showInList": true,
      "questionFieldLists" : [
       {
        "rule" : "default",
        "fields" : [{
          "systemName":"OPSS-Ctl-Cert:DesEff",
          "displayType":"Radio Button/Checkbox"
         },
         {
          "systemName":"OPSS-Ctl-Cert:DesEffExplain",
          "displayType":"Text Area"
         }]
       }
      ]
     }
    }
```

Chapter 29. Configuring OpenPages Loss Event Entry

IBM OpenPages Loss Event Entry is an optional, chargeable component that users across an organization can access to create loss events. You can customize the component by configuring how it works for your organization, and the way users view and interact with it. OpenPages Loss Event Entry can be used to create only loss events together with loss impacts, loss recoveries, and files. You cannot use it to create other object types.

You use the Loss Event Entry Configuration tool to configure the OpenPages Loss Event Entry component. For more information about this tool, see "Using the Loss Event Entry Configuration tool" on page 716. Review that topic and access and open the tool as you learn about how to configure OpenPages Loss Event Entry.

Read "Planning the configuration " on page 709 to learn about whether you can use the out-of-the-box configuration that is included in OpenPages Loss Event Entry. If you choose to modify the out-of-the-box configuration, the following topics explain aspects of the system you need to understand before you begin:

- "How users are handled" on page 711
- "Where loss events get created" on page 711
- "Who loss events get assigned to " on page 711
- "How dates are validated" on page 712
- "How to launch OpenPages Loss Event Entry " on page 712
- "How confirmation emails are configured" on page 715

For more information about OpenPages Loss Event Entry, see the topic *OpenPages Loss Event Entry* in the *IBM OpenPages GRC New Features Guide*.

Planning the configuration

You can use OpenPages Loss Event Entry either as it is out-of-the-box with a minimal amount of configuration or you can make modifications for your organization.

To use OpenPages Loss Event Entry as it is out-of-the-box, you need to complete the following configuration tasks:

1. In the Loss Event Entry Configuration tool, change the passwords of the ten dedicated users that are included in OpenPages Loss Event Entry. For information, see "Using the Loss Event Entry Configuration tool" on page 716.
2. Review the creation views for loss events and decide whether you want to display or hide the **Loss Impacts** and **Loss Recoveries** tabs. If displayed, you can also decide whether to make them mandatory. Creation views are described later in this topic. How you can make the tabs mandatory is described in "Using the Loss Event Entry Configuration tool" on page 716.
3. Change the role template assignment for the `Loss Event Entry` role template so that it grants the lowest level of access needed.
4. In the Loss Event Entry Configuration tool, define **Default Parent Path** and **Default Triage Team**. For information, see "Using the Loss Event Entry Configuration tool" on page 716.
5. Place a URL on your organization's intranet. For information, see "How to launch OpenPages Loss Event Entry " on page 712.

You can, alternatively, modify many aspects of OpenPages Loss Event Entry. To do this, review what is included in the system and modify any of the following items to meet your requirements:

- Decide what locales you need. It is a best practice to disable locales that you do not use and disable or do not load the dedicated users for them.

- Review the user group, `Loss Event Entry`, and make changes if needed. It contains ten dedicated users, one for each locale: `LEE_EN_US`, `LEE_EN_GB`, `LEE_IT_IT`, `LEE_PT_BR`, `LEE_FR_FR`, `LEE_ES_ES`, `LEE_DE_DE`, `LEE_ZH_TW`, `LEE_ZH_CN`, and `LEE_JA_JP`. For more information, see "How users are handled" on page 711.
- Review the role template, `Loss Event Entry`, and make changes if needed. The ten dedicated users are assigned to this role template at the root business entity. It is a best practice to change the role template assignment for the `Loss Event Entry` role template so that it grants the lowest level of access needed.
- Review the profile, `Loss Event Entry`, and make changes if needed. The ten dedicated users are assigned to this profile.
- Design the content of the loss event form. Review the creation views, `LE Entry - LE`, `LE Entry - LI`, and `LE Entry - LR`, and make changes if needed. They are assigned to the `Loss Event Entry` profile. The system uses the views to determine what tabs and fields are displayed in OpenPages Loss Event Entry. Decide whether you want to display or hide the **Loss Impacts** and **Loss Recoveries** tabs. Both tabs are set to display in the creation views included with the system. To hide them, remove them as child views on `LE Entry - LE`. If you want to display these tabs in creation views you create, they must be defined as child views on the loss event creation view. If you want to make it mandatory that a user enter a loss impact or loss recovery, you can configure that in the Loss Event Entry Configuration tool.
- Review the field groups, `OPSS-LE-BE` and `OPSS-LE-Contact`. `OPSS-LE-BE` contains Business Entity Selector fields that are used to identify the involvement of business entities in loss events. `OPSS-LE-Contact` contains fields that contain user information such as name, email, and phone number.
- Review the date validation rules that are included in the system and make changes if needed. You configure date validation rules in the Loss Event Entry Configuration tool. For information, see "How dates are validated" on page 712.
- Determine how you want to set the parent business entity and the triage team. For information, see "Where loss events get created" on page 711 and "Who loss events get assigned to " on page 711. Fields that contain parent business entities must be of the display type, Business Entity Selector. For information about this display type, see "Configuring the Business Entity Selector display type for simple string fields" on page 263.
- Enable auto-naming for the Loss Event, Loss Impact, and Loss Recovery objects. Although not required, it prevents failures due to duplicate names and inconsistencies in user-given names. Users who create loss events do not know the naming rules in OpenPages.
- Customize the informational text displayed in OpenPages Loss Event Entry.
  - To change the text that displays when users click the  icon for the Information box in the header, change the text associated with the Application Text key, `loss.event.entry.overall.help`, in the Application Messages folder.
  - To change the information that is displayed at the top of the tab for each object type, change the text for the keys, `loss.event.entry.file.intro`, `loss.event.entry.loss.event.intro`, `loss.event.entry.loss.impact.intro`, and `loss.event.entry.loss.recovery.intro` in the Application Messages folder.
  - Customize the logo on the loss event form to be your company logo. File specifications are as follows:
    - Size: 1130 pixels wide by 36 pixels high
    - Name: `Logo.png`
    - Folder location: `../sosa.war/image/lossevent/`

      Changes to the logo file can be overwritten in subsequent upgrades.
- Design and configure the email confirmation that is sent to users when a loss event is created. For information, see "How confirmation emails are configured" on page 715.

How users are handled

Users can create loss events in OpenPages Loss Event Entry without a user account for OpenPages. A dedicated user group that includes ten dedicated users, one for each supported locale, is included in OpenPages Loss Event Entry. When users access OpenPages Loss Event Entry, they do not have to enter a user ID and password. The system automatically logs them in to OpenPages Loss Event Entry with the dedicated user associated with the locale.

Users with access to OpenPages can create loss events as they always have or choose to use OpenPages Loss Event Entry. However, OpenPages users cannot log in to both at the same time in the same browser. Instruct your OpenPages users that they must log out of OpenPages when they want to use OpenPages Loss Event Entry. If you want to force OpenPages users to use IBM OpenPages Loss Event Entry, you can add Loss Event to the list of objects that are disabled for Add New. For more information, see "Controlling the availability of object types in the Add New wizard" on page 204. Additionally, the profile and role template assignments for OpenPages users is disregarded when they use OpenPages Loss Event Entry.

Where loss events get created

Loss events must be assigned to a parent business entity within the organization. You determine how this assignment is made when you define Default Parent Path and Parent Field Name in the Loss Event Entry Configuration tool.

For information about the Loss Event Entry Configuration tool, see "Using the Loss Event Entry Configuration tool" on page 716.

You can choose one of the following methods:

- Static: your organization assigns all loss events to one default business entity. The triage team then reassigns them to the correct business entities. To use this method, you enter the default business entity in **Default Parent Path** and leave **Parent Field Name** blank.
- User-selected: your organization assigns loss events to a business entity that the user selects, for example, the Primary Caused Entity or the Primary Impacted Entity. To use this method, you enter the field name that contains the business entity in **Parent Field Name**. The field must be in the creation view.
- Pre-filled in a URL: your organization assigns loss events to a business entity that you pass in the URL. To use this method, you enter the field name that contains the business entity in **Parent Field Name**. Pass the value that you want in the URL.
- Custom: your organization sets the business entity based on information in the loss event or elsewhere in the system. For example, the system can automatically assign a loss event to Business Entity A if the loss amount is less than $1,000,000 and to Business Entity B if it is over that amount. This method can be implemented with triggers. To use this method, you can leave **Parent Field Name** blank because it is set by the triggers.

The **Default Parent Path** is mandatory for all methods. The system defaults to it if the value in **Parent Field Name** is not given, is invalid, or there is an error. Ensure that the dedicated users have access rights to create loss events under the business entity in **Default Parent Path**.

Who loss events get assigned to

Loss events are typically assigned to a triage team that is responsible for reviewing the initial information and taking next steps. You determine how this assignment is made when you define **Default Triage Team** and **Triage Team Field Name** in the Loss Event Entry Configuration tool.

For information about the Loss Event Entry Configuration tool, see "Using the Loss Event Entry Configuration tool" on page 716.

You can choose one of the following methods:

- Static: your organization assigns all loss events to a list of users and user groups. To use this method, you enter the list of users and user groups in **Default Triage Team** and leave **Triage Team Field Name** blank.
- User-selected: your organization assigns loss events to users or user groups that the user selects. To use this method, you put the field name that contains the actor field in **Triage Team Field Name**. The field must be in the creation view.
- Pre-filled in a URL: your organization assigns loss events to users or user groups that you pass in the URL. To use this method, you put the field name that contains the actor field in **Triage Team Field Name**.
- Custom: your organization assigns loss events to user or user groups based on information in the loss event or elsewhere in the system. For example, a trigger can take the value of a loss event's Primary Impacted Entity field and go to that entity's Preference record to get the name of the triage team. It can then put that triage team name into the triage team field on the loss event. To use this method, you can leave **Triage Team Field Name** blank because it is set by the triggers.

The **Default Triage Team** is mandatory for all methods. The system defaults to it if the value in **Triage Team Field Name** is not given, is invalid, or there is an error. Ensure that the field given in **Triage Team Field Name** is one of the seven actor display types. If you pre-fill it in a URL, ensure that the values passed in the URL are consistent with the actor display types you chose in the **Triage Team Field Name**.

A third field, **Populate Triage Team Field Name**, is typically used as the assignee in the first stage in configurable life cycles for loss events. It is a mandatory field. When a loss event is created, the users and user groups in **Triage Team Field Name** are copied to the field given in **Populate Triage Team Field Name**. If **Triage Team Field Name** is not given, the users and user groups in **Default Triage Team** are copied to the field given in **Populate Triage Team Field Name**. All three field types must be compatible. The display type of the field that is given in **Populate Triage Team Field Name** must be able to accept any value that comes from **Default Triage Team** or **Triage Team Field Name**. For example, if **Triage Team Field Name** is a multiple user/group field, **Populate Triage Team Field Name** must also be a multiple user/group field.

How dates are validated

You define how dates are validated in rules in the **Date Validation** field in the Loss Event Entry Configuration tool. For example, you might want to ensure that a loss event's discovery date occurs before today's date or that its discovery date falls after its occurrence date.

The following date validation rules would test for these situations:

```
LossEvent:OPSS-LossEV:Discovery Date >= LossEvent:OPSS.LossEV:Occurrence Date
```

```
LossEvent:OPSS-LossEV:Discovery Date <= TODAY
```

OpenPages Loss Event Entry displays a red X and an explanation next to dates that fail the validation rules. Users must resolve errors before they can submit a loss event.

OpenPages Loss Event Entry includes date validation rules that you can keep or modify. The date validation rules are effective only in OpenPages Loss Event Entry and not in OpenPages. If you want the same rules to apply in OpenPages, they can be implemented with triggers.

How to launch OpenPages Loss Event Entry

Users typically access IBM OpenPages Loss Event Entry from one or more links on your organization's intranet.

There are many ways that you can configure the URLs in these links:

- You do not pass parameters in the URL. Use this approach if you want users to provide information for loss events and you do not want to pre-fill information for them.
- You can set what locales users access. If all users access one locale, you can add the locale to the URL in the link on your organization's intranet. If users can access multiple locales, you can either place multiple links on your organizations intranet, for example, a link for users in North America and a link for users in France, or you can have one link and pre-fill the locale in the URL.
- You can pre-fill user information on the loss event form by passing fields and values in the URL. You can include user data from the network login and determine programmatically how to put it in the URL. When a user creates a loss event, values from the URL can pre-fill fields on the form. For example, the user's name, phone number, and email can be passed in the URL so that the user does not have to enter this information.
- You can pre-fill where in the organizational structure the loss event will be created and who it will be assigned to. Use this approach if your organization is structured in a way that loss events can be created in and assigned to multiple areas of the organization. You can use multiple URLs to pre-fill the primary caused business entity and the triage team. Then, users who create loss events do not have to enter this information, it is pre-filled for them and set to the correct value for where they are in the organization.
- You can pre-fill no information so that users can create loss events anonymously. Create a link where you do not pass user information. You must also ensure that users are not required to provide their name and email on the loss event form.

Follow these guidelines when you construct a URL:

- The fields that you pass must be defined for the top-level Loss Event object type.
- The fields that you pass must exist in the creation view.
- The fields that you pass cannot be read-only.
- The fields that you pass must be defined as simple string fields. Other fields types are not supported.
- The display type of the simple string fields that you pass can be: Text Box, Text Area, URL, Business Entity Selector, User Drop-down, User Selector, Group Selector, User/Group Selector, Multi-Valued User Selector, Multi-Valued Group Selector, and Multi-Valued User/Group Selector. All other display types are not supported.
- The values that you pass must be valid for the display type.
- The URL is limited to 2083 characters for Internet Explorer.

Follow these syntax rules when you construct a URL:

- Start the first parameter with ?.
- Separate multiple parameters with &.
- Provide locales in the format `locale=<locale code>`. Valid locale codes are:
  - `en_US` (US English)
  - `en_GB` (UK English)
  - `it_IT` (Italian)
  - `pt_BR` (Brazilian Portuguese)
  - `fr_FR` (French)
  - `es_ES` (Spanish)
  - `de_DE` (German)
  - `zh_TW` (Chinese Traditional)
  - `zh_CN` (Chinese Simplified)
- Provide fields and values in the format `<field group>:<field name>=<field value>`. Enter the field name not the field label.

- For fields whose display type is Multi-Valued User Selector, Multi-Valued Group Selector, or Multi-Valued User/Group Selector, you can pre-fill the field with one or multiple values. Begin and end values with `$;`, for example:

  ```
  $;user1$;
  ```

  Separate multiple values with `$;`, for example:

  ```
  $;user1$;user2$;user3$;
  ```

- For text fields that pass email addresses, for example, **Submitter Email Field Name**, you can pre-fill the field with only one value.

The following examples illustrate how you can construct URLs.

Example 1: Set the locale.

```
http://<server>:<port>/openpages/app/jspview/appLoader/lossevent?locale=en_GB
```

Example 2: Pre-fill the primary caused entity to /Global Services/North America Banking. The display type of `OPSS-LE-BE:Primary Caused Entity` is business entity selector.

```
http://<server>:<port>/openpages/app/jspview/appLoader/lossevent
?OPSS-LE-BE:Primary Caused Entity=/Global Services/North America Banking
```

Example 3: Pre-fill the triage team to Risk Team New York and two users:

```
http://<server>:<port>/openpages/app/jspview/appLoader/lossevent
?ABC-LE:UsersToNotify=$;Risk Team New York$;user1$;user2$;
```

Example 4: Pre-fill user information from the network sign-on:

```
http://<server>:<port>/openpages/app/jspview/appLoader/lossevent
?OPSS-LE-Contact:Your Name=User One&OPSS-LE-Contact:Your Email=user1@example.com
```

Example 5: Pre-fill user information, primary caused business entity, and locale:

```
http://<server>:<port>/openpages/app/jspview/appLoader/lossevent
?OPSS-LE-Contact:Your Name=User One&OPSS-LE-Contact:Your Email=user1@example.com
&OPSS-LE-Contact:Your Phone=555-111-2222&OPSS-LE-BE:Primary Caused Entity=
/Global Services/North America Banking&locale=en_GB
```

Example 6: Pre-fill information if you have multiple primary caused business entities and multiple triage teams in your organization. Assume that you have two divisions, /Global Services/North America/Division/East and /Global Services/North America/Division/West. You want to prefill the parent business entity with the division's Primary Caused Entity and the triage teams from `ABC-LE:UsersToNotify`.

You create two URLs. This URL is for users in the East division.

```
http://<server>:<port>/openpages/app/jspview/appLoader/lossevent
?OPSS-LE-BE:Primary Caused Entity=/Global Services/North America/Division/East
&ABC-LE:UsersToNotify=DivisionEastTriage
```

This URL is for users in the West division.

```
http://<server>:<port>/openpages/app/jspview/appLoader/lossevent
?OPSS-LE-BE:Primary Caused Entity=/Global Services/North America/Division/West
&ABC-LE:UsersToNotify=DivisionWestTriage
```

Example 7: Pre-fill no information for a URL that you use for loss events that are created anonymously. Do not pass user information. You might want to send the email confirmation to a person designated to handle these situations.

```
http://<server>:<port>/openpages/app/jspview/appLoader/lossevent
```

```
?LE-Submitter:Confirmation Emails=user5@example.com
```

How confirmation emails are configured

You can design and configure the confirmation email that is sent to users when a loss event is created.

The confirmation email has the following parts:

- Submitter email address

  Define **Submitter Email Field Name** in the Loss Event Entry Configuration tool. Email confirmations are sent to this email field. The default is `OPSS-LE-Contact:Your Email`.

- Text and parameters to put in the subject

  To build the email subject, you define fields in **Submitter Email Subject Parameters** in the Loss Event Entry Configuration tool that you want to put in the email subject. Then, write the text and enter parameters for those fields in `lossevent.confirm.subject` Application Text. The order of the fields that are listed in **Submitter Email Subject Parameters** must match the numbering of the parameters in the `lossevent.confirm.subject` Application Text.

- Text and parameters to put in the body text

  To build the email body text, you define fields in **Submitter Email Body Parameters** in the Loss Event Entry Configuration tool that you want to put in the email body text. Then, write the text and enter parameters for those fields in `lossevent.confirm.content` Application Text. The order of the fields that are listed in **Submitter Email Body Parameters** must match the numbering of the parameters in the `lossevent.confirm.content` Application Text.

- Sender email address

  Enter the system email address that sends confirmation emails in `lossevent.confirm.from.address` Application Text. Parameters are not allowed in `lossevent.confirm.from.address`.

Use the following syntax in `lossevent.confirm.subject` Application Text:

- Enter `{0}` for the first parameter, which in the out-of-the box configuration is the name of the loss event. Enter remaining parameters in the syntax `{value}`. The values of fields given in **Submitter Email Subject Parameters** are put in the email subject.

Use the following syntax in `lossevent.confirm.content` Application Text:

- Enter `{1}` for the first parameter, which in the out-of-the box configuration is the name of the submitter. Enter remaining parameters in the syntax `{label}:{value}` or `{value}`. For example, `{2}:{3}` puts the label and value of the second field given in **Submitter Email Body Parameters** in the email body. Then, `{4}:{5}` puts the third field, `{6}:{7}` the fourth field, and so on. For example, `{2}:{3} \n {4}:{5}` puts the second field's label and value, a line break, and the third field's label and value in the body text. Enter `{value}` to omit a field label. For example, `{3} \n {5}` puts the second field's value, a line break, and the third field's value in the body text (without the field labels).
- Use `$children` to include loss event impacts and loss recoveries in the email.
- Use `$title` to include the label of the loss event object type in the email.
- Enter `\n` to force a line break.

For example, if **Submitter Email Body Parameters** is defined as:

```
OPSS-LE-Contact:Your Name,OPSS-LossEv:Owner,System Fields:Name,
System Fields:Description,OPSS-LE-BE:Primary Caused Entity
```

And `lossevent.confirm.content` Application Text is defined as:

```
{1}, \nThe following $title was entered by you. \n{2}: {3} \n{4}: {5} \n{6}: {7}\n \n
```

```
{8}: {9}  \n $children
\n\nIf you are an OpenPages user, you can click $url to view in OpenPages.
\n\nDo not reply. Automated email from OpenPages
```

The confirmation email contains the following body text:

```
User One,
The following Loss Event was entered by you.
Owner: $;user1$;OpenPagesAdministrator$;
Name: Library_LE_0022
Description: This is a description
Primary Caused Entity: /Global Services/North America

Do not reply. Automated email from OpenPages
```

The value for `OPSS-LE-Contact:Your Name` is substituted into parameter `{1}` followed by a line break, text, and another line break.

The label and value for `OPSS-LossEv:Owner` is substituted into parameters `n{2}: {3}` followed by a line break.

The label and value for `System Fields:Name` is substituted into parameters `n{4}: {5}` followed by a line break.

The label and value for `System Fields:Description` is substituted into parameters `n{6}: {7}` followed by a line break.

The label and value `OPSS-LE-BE:Primary Caused Entity` is substituted into parameters `n{8}: {9}` followed by a line break.

The ending text is included.

Using the Loss Event Entry Configuration tool

You use the Loss Event Configuration tool to configure IBM OpenPages Loss Event Entry.

Before you begin

Read Chapter 29, “Configuring OpenPages Loss Event Entry,” on page 709 to learn about OpenPages Loss Event Entry and “Planning the configuration ” on page 709 to learn about decisions to make before you begin.

Procedure

1. Open the Loss Event Entry Configuration tool with the following URL.

   ```
   http://<server>:<port>/openpages/app/jspview/lossevent#/editconfig
   ```

   Log in with your OpenPages user account. You must be a member of the `OPAdministrators` user group to access the tool. You can have it open and simultaneously be logged in to OpenPages to work on other administration tasks. Click **Save** in the tool to refresh it with the most recent changes you make in OpenPages. For example, if you change information text in OpenPages and return to the Loss Event Entry Configuration tool, you do not see the changes until you click **Save**.

   When you provide fields in the format, `<Field Group>:<Field Name>`, ensure that no spaces exist before and after the colon.
2. Complete the fields in the tool. Hover over a field to see a description.
3. Complete the fields in the **Object Types** section.
   a) In **Loss Event View Name**, enter the name of a loss event creation view that is used to determine the information on the **Loss Event** tab. The default is `LE Entry - LE`.

b) In **Loss Impacts View Name**, enter the name of a loss impact creation view that is used to determine the information on the **Loss Impacts** tab. The default is `LE Entry - LI`. Click **Required** to make it mandatory for a user to enter information on the tab.

c) In **Loss Recoveries View Name**, enter the name of a loss recovery creation view that is used to determine the information on the **Loss Recoveries** tab. The default is `LE Entry - LR`. Click **Required** to make it mandatory for a user to enter information on the tab.

d) For **Files**, click **Present** to show the **Files** tab. Users can click the **Files** tab to add attachments to a loss event. Clear **Present** to hide the **Files** tab. Click **Required** to make it mandatory for a user to attach at least one file.

4. Complete the fields in the **Locales** section for each locale.

a) Click **Enabled** to allow users to access that locale.

b) Enter a **Password** for the dedicated, locale user.

You must enter a password and save the configuration for users to be able to access OpenPages Loss Event Entry. The user password is automatically updated in OpenPages. To change the dedicated users' passwords in the future, use the Loss Event Entry Configuration tool rather than OpenPages.

Important: Do not change the dedicated users' passwords by using OpenPages. Always use the Loss Event Entry Configuration tool to change the passwords. If you change the passwords in OpenPages, users will not be able to use Loss Event Entry because the passwords will be out of sync.

You can use the user names included in the out-of-the box system. If you change the user names in the Loss Event Entry Configuration tool, they must match the user names of the dedicated users.

5. Complete the fields in the **Other** section.

a) In **Default Parent Path**, enter a path, for example, `/Global Services/North America Banking`, to the business entity that is the default parent of new loss events if users cannot or do not select a parent. Mandatory.

b) In **Parent Field Name**, enter the name of a Business Entity Selector field that users can use to select a parent business entity for a new loss event. Format is `<Field Group>:<Field Name>`. It must be included in the selected creation view, and it must have a display type of Business Entity Selector. The default is `OPSS-LE-BE:Primary Caused Entity`. If not given or the user does not select a value in this field, the value in **Default Parent Path** is used as the parent for a loss event.

c) In **Submitter Email Field Name**, enter the name of a field that email confirmations are sent to. It must be defined in the creation view and be a Text Box display type. The default is `OPSS-LE-Contact:Your Email`.

d) In **Default Triage Team**, enter the default users and user groups that loss events are assigned to for follow up. Can contain multiple actors separated by commas. Mandatory.

e) In **Triage Team Field Name**, enter the name of an actor field. Format is `<Field Group>:<Field Name>`. It must be defined in the creation view. Optional. If not given or the user does not select a value in this field, the value in **Default Triage Team** is used to assign a triage team to a loss event.

f) In **Populate Triage Team Field Name**, enter the field in which the triage team is stored. Format is `<Field Group>:<Field Name>`. The default is `OPSS-LossEv:Owner`. Mandatory. The selected actor or actors from either **Default Triage Team** or **Triage Team Field Name** are copied to the field given in the **Populate Triage Team Field Name**.

g) Select **Display Resource ID of Created Objects** to show a loss event's internal system-generated identifier to the user on the confirmation window and confirmation email.

h) Review the **Date Validation** rules that are delivered with the system and make changes, if needed.

Follow these guidelines:

- You write the rules in the syntax `<object type name>:<field group name>:<field name>`. In all three portions use the item's name, not its label.
- You can use the Loss Event or any of the other object types used by OpenPages Loss Event Entry. A rule cannot cross object types.
- You can use: <= and >=.

- You can use the word TODAY.
- You can use only date fields, and they must exist in the creation view.

i) Select a **Default Locale**. This is the default locale if one is not specified in the URL. The default locale is listed first in the selection list, then all other locales are listed in alphabetical order in the user's language.

j) In **Submitter Email Subject Parameters**, enter fields that are included in the subject of the confirmation notification email that is sent to the submitter. Default is `System Fields:Name`.

You can choose any of the fields in the Loss Event profile. The Application Text that is located in `lossevent.confirm.subject` references these parameters.

For information, see "How confirmation emails are configured" on page 715.

k) In **Submitter Email Body Parameters**, enter fields that are included in the body of the confirmation email that is sent to the submitter. Default is `OPSS-LE-Contact:Your Name,System Fields:Name,System Fields:Resource ID,System Fields:Description`.

You can choose any of the fields in the Loss Event profile. The Application Text that is located in `lossevent.confirm.content` references these parameters.

For information, see "How confirmation emails are configured" on page 715.

6. Click **Validate** to verify the configuration. You cannot save the configuration if fatal errors exist. Resolve them and validate again. You can save the configuration if non-fatal errors exist.

   If you have numerous errors, the **OK** icon rolls to the bottom of the list and is not visible. In the browser settings, zoom out to make the screen small enough to access the OK icon.
7. Click **Save**. The **Last Saved** time stamp on the page is updated.

Chapter 30. Configuring and maintaining Business Process Manager

You can use IBM OpenPages GRC Platform together with IBM Business Process Manager to develop business processes that are aligned to your specific requirements. IBM Business Process Manager is a leading industry process automation system that is both scalable and highly configurable.

Configuring Business Process Manager

To use IBM OpenPages GRC Platform together with IBM Business Process Manager, you must complete several configuration tasks.

Before you begin

Ensure that IBM Business Process Manager is installed. Verify that the post-installation steps in the *OpenPages for Business Process Manager Installation Guide* are completed.

Procedure

1. Configure the IBM BPM server URL in the **Administration** > **Settings** > **Platform** > **Workflow Implementations** > **IBM BPM** > **Server URL** registry settings. For more information, see "Workflow implementations settings" on page 353.
2. Customize the portal page in **Administration** > **Settings** > **Platform** > **Workflow Implementations** > **IBM BPM** > **Portal Page Path** (optional). The system is delivered with a default portal page but you can choose a different one. For more information, see "Workflow implementations settings" on page 353.
3. Update user and user group definitions for administrators who work with IBM Business Process Manager. They need to have the application permission, IBM BPM. It controls whether the new menu items on the Administration menu are displayed. It is located in **SOX** > **Administration**.
4. Check whether you have an OpenPages administrator with the user name `admin`. If you keep it, it creates conflicts in both the federated repository and the default user registry that is provided by WebSphere. Websphere contains an `admin` user account for the WAS admin console. It also causes an authentication issue with the OpenPages REST API security. You must remove the Websphere `admin` user from the default user registry and create a new administrator with a different name. For information, see http://www.ibm.com/support/knowledgecenter/SS7K4U_8.5.5/com.ibm.websphere.wim.doc/MultipleEntitiesWithSamePrincipalName.html (http://www.ibm.com/support/knowledgecenter/SS7K4U_8.5.5/com.ibm.websphere.wim.doc/MultipleEntitiesWithSamePrincipalName.html).
5. Update profiles for OpenPages users who work with business processes. The profiles need to have **Process Portal** in the **Home Page Tab Configuration** set to *Visible*. The **Process Portal** tab is then displayed on the Home Page. The profile also determines where the tab is displayed relative to other tabs.
6. Determine whether to use auto-login. If it is enabled, OpenPages users can access the IBM BPM menu items in OpenPages without having to log in to IBM BPM. They can move seamlessly between the two systems. When users log in and out of OpenPages, the system also automatically logs them in and out of IBM BPM. When users log in directly to the IBM BPM applications, such as BPM Process Portal or BPM Process Center, without accessing them through OpenPages, the auto-login feature is not used. They must log in with their OpenPages credentials.
   a) Set the **Enable Login SSO** registry setting. For more information, see "Workflow implementations settings" on page 353.
   b) Edit the `/<OP_HOME>/aurora/conf/aurora.properties` file on the application server.

c) Look for a property that is named `logout.url.ibmbpm`. If it does not exist, create it.

d) Set `logout.url.ibmbpm` to the URL of your BPM server hostname/FQDN. Use the same hostname/FDQN that you used for the **Server URL** registry setting.

Use the `https` protocol rather than `http` in the URL.

For example, if you used `https://bpm.server.com:9443/` for the **Server URL**, type:

```
https\://bpm.server.com\:9443/ProcessPortal/logout.jsp
```

e) Restart the OpenPages servers.

7. Configure automatic IBM BPM email notifications (optional). IBM BPM can automatically send email notifications when a task is assigned to users or groups. If you use automatic email notifications:

   - You can also define email notifications in business processes.
   - IBM BPM provides an email template, which you can optionally customize.
   - The email recipient is always the task assignee.
   - Users can choose whether to receive this type of email notification.

   If you do not use this email notification method, all email notifications must be defined in business processes.

   To configure automatic email notifications:

   a) Copy the email configuration from `99Local.xml` to `100Custom.xml` file as described in IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SSV2LR/com.ibm.wbpm.admin.doc/topics/tadm_portal_email.html). There are multiple `100Custom.xml` files under the IBM BPM installation directory. For information about what file to change, see table 3 in IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SSV2LR/com.ibm.wbpm.admin.doc/topics/managing_twks_config_settings.html).

   b) Populate the change to all the clustered servers by restarting the server. Stop all WebSphere processes (server, nodeagent, and deployment manager). Start the deployment manager. Run `syncNode.sh`. Start nodeagent and server.

   c) Users can control whether they receive automatic email notifications with the **Send me an email when I have a new task assignment** setting on their BPM profile. They can edit their profile by logging in to the BPM Process Portal. Users cannot access the BPM profile in the **Process Portal** tab in OpenPages.

8. Set up who can be IBM BPM process authors and administrators. Sign on to the Process Admin Console and click **User Management**. Users from OpenPages exist as BPM users. Use **Group Management** to assign them to the user groups, `tw_admins` or `tw_authors`. Assign the OpenPages Super Administrator user to both groups.
9. Ensure that you set up a backup schedule for the BPM database. The OPBackup utility does not back up BPM.
10. You are ready to begin designing processes and getting started with IBM BPM.

What to do next

After IBM BPM is operational, complete the maintenance tasks that are described in "Maintaining Business Process Manager" on page 720.

Maintaining Business Process Manager

After IBM Business Process Manager is operational, you must complete maintenance tasks on an as-needed basis.

After IBM BPM is operational, complete the following maintenance tasks on an as-needed basis:

- The OpenPages Platform Toolkit, the OpenPages Solutions Toolkit, IBM BPM, and IBM OpenPages GRC Platform need to remain synchronized. Two situations can get them out of sync:
  - You install a new release or fix pack that contains changes to the toolkits
  - You change your data model, object texts, or application texts

  In both situations, you must follow these steps:
  - Regenerate the OpenPages Solutions Toolkit.
  - Update the dependencies between the process applications and the latest snapshots of the toolkits.
  - Take a snapshot of the process applications.
  - Install that snapshot from the Process Center to the Process Servers.
- Users who access OpenPages and IBM BPM remain synchronized because they are defined in a federated repository. However, the email addresses and locales in OpenPages and IBM BPM require an extra step to remain synchronized. You must replicate the email addresses and user locales from OpenPages to IBM BPM on a scheduled basis, for example, daily. For more information, see *Replicating user email addresses and locales* in the *OpenPages for Business Process Manager Installation Guide*.
- If you change the logon user name or password of the Super Administrator account after installation (using the application interface), you must make the corresponding changes in IBM BPM.

  If a mismatch exists between the logon user name or password and the specified user name or password in IBM BPM, the user cannot log on to IBM BPM.

  1. Log on to the BPM server's WebSphere admin console.
  2. Click **Security** > **Global Security** .
  3. Under the **Authentication** section, expand **Java Authentication and Authorization Services** and click **J2C authentication data**.
  4. Click the *OpenPages System Task Authentication Alias*.
  5. Change the **User ID** or leave it as the default, *OpenPagesAdministrator*.
  6. Change the **Password** to the new value.
  7. Click **OK** and then **Save**.
- Set up a schedule to periodically archive process apps and toolkit snapshots in IBM Business Process Manager. If you frequently regenerate the OpenPages Solutions Toolkit, you can encounter memory and performance issues. For more information, see the following topics in IBM Business Process Manager:
  - https://www.ibm.com/developerworks/bpm/bpmjournal/1312_spriet/1312_spriet.html
  - https://developer.ibm.com/answers/questions/198315/bpm-856-standard-snapshot-cleanupdelete-scripting.html

Chapter 31. Configuring cognitive services

You can use an IBM Watson Natural Language Classifier service in IBM Bluemix to interpret and classify text that users enter in IBM OpenPages GRC Platform. It understands the intent behind text and returns suggestions, together with a confidence score.

You can configure a Natural Language Classifier service to suggest either taxonomy classifications or parent and child object associations. You can use it for any objects in OpenPages but it is typically used to classify loss events, waivers, issues, and incidents or to associate them to a risk, policy, or control.

If you configure it to suggest taxonomy classifications, you can use it, for example, to support users when they classify a loss event to the correct Basel II categorization or when they classify waivers as exceptions to regulatory compliance. The text description that a user enters is used as input to a Natural Language Classifier service that has been trained with knowledge from your domain specialists.

If you configure it to suggest object associations, you can use it to support users when they, for example, create an Issue object and need to associate it to a parent Control object. Again, the text description that a user enters is used as input to a Natural Language Classifier service but in this case it returns a suggested parent Control object together with a confidence score. Object association suggestions can be configured to suggest either parent or child associations. They are synchronized with associations that users make on the **Parent** tab or children tabs.

Using a Natural Language Classifier service is best suited to situations where users are generating a high volume of objects, hundreds or even thousands per year. Cognitive computing adds value when it is scaled to a large data set and to a large group of users. The data the classifier is trained on should be relatively small and static. For example, you would want to train a classifier to provide object association suggestions to a small number of Controls in the Controls Library, which is small and relatively static, rather than to all the Controls in your business, which are numerous and dynamic. You would not want to train a classifier to make object associations between objects that change rapidly, for example, Audit Findings and Issues, because Issues are constantly changing and there might be thousands of them.

You can link OpenPages to one or more Natural Language Classifier services in IBM Bluemix, either to support different purposes or multiple languages.

Terms to understand

Natural Language Classifier
A Natural Language Classifier is a Watson service in IBM Bluemix that uses machine learning algorithms to return the top-matching predefined classes for short text inputs. You configure, train, and connect to a Natural Language Classifier service from OpenPages. A Natural Language Classifier service learns from your data and then can return information for texts that it is not trained on.

Classifier Configuration
A classifier configuration in OpenPages defines connection information to an instance of the Natural Language Classifier on IBM Bluemix. For taxonomy classifications, it specifies the classifier target fields for the instance. For object associations, it specifies the object type to associate, whether it is a child or parent relationship, and other attributes. You define a classifier configuration in **Administration** > **Cognitive Services** > **Natural Language Classifiers**.

Classifier Field
A classifier field is a field group in OpenPages that contains the name of a classifier configuration and a classifier input field. The **View Suggestions** button is displayed next to a classifier field.

Classifier Input Field
A classifier input field is a field in OpenPages that contains the short text input that a Natural Language Classifier interprets and classifies. It is typically a **Description** field.

Classifier Target Fields
For taxonomy classifications, classifier target fields are fields in OpenPages that are set when a user chooses suggestions for a classifier field.

This video demonstrate how to use a Natural Language Classifier to make object association suggestions:

https://youtu.be/VFUxni9tsrc

This video demonstrates how to use a Natural Language Classifier to make taxonomy suggestions:

https://youtu.be/ZysbwttRpwA

Configuring cognitive services

To use OpenPages together with a Natural Language Classifier service in IBM Bluemix, you must design how you want the system to work and complete several configuration tasks.

Before you begin

- Decide the purpose of the classifier: taxonomy suggestions or object association suggestions.
- Verify that the application server has outgoing internet access so that it can communicate with a Natural Language Classifier service.
- Verify that the data type for the classifier input field is Simple String.
- If the classifier is for taxonomy suggestions:
  - Decide what area you want to support, for example, helping users select Basel II categorizations.
  - Decide what objects the classifier field is available on, for example, loss events, waivers, issues, and incidents.
  - Verify that the data type for the classifier target fields is Enumerated String. You can have up to three classifier target fields.
  - Decide whether you want to allow users to select one or many suggestions. Set **Multi-valued** to false on at least one of the classifier target fields to allow users to select only one suggestion. Set **Multi-valued** to true on all classifier target fields to allow multiple selections.
- If the classifier is for object association suggestions:
  - Decide what object association you want to support, for example, helping users choose a Control object as a parent.
  - Decide what objects the classifier field is available on, for example, loss events, waivers, issues, and incidents.
  - Verify the path to the object type.
  - Decide what names and descriptions are displayed when a user selects an object.

About this task

The following steps describe how to configure a Natural Language Classifier service.

Procedure

1. Configure and train the Natural Language Classifier service on IBM Bluemix. For information, see “Configuring a Natural Language Classifier in Bluemix” on page 725.
2. Import the Watson certificate into the Websphere trust store. Do this only one time, not for every service you configure. For information, see “Importing a Watson certificate to the local trust store ” on page 727.
3. Define a classifier configuration. For information, see “Defining a Classifier Configuration” on page 728.
4. Define a classifier field. For information, see “Defining a classifier field” on page 729.
5. Add the field group that the classifier field is in to the object type, if it is not already there.
6. Add the classifier field to the profile.
7. Add the classifier field to views where you want it to display. You can add it to Detail, Activity, and Add New views. You can also add it to Loss Event Entry. On these views, ensure that **Read-Only** is cleared

so that the fields are editable. On the Add New view, although you can place the classifier field anywhere, you might want to place it immediately following the description field where users enter the text input. You can also add it to Filtered List Views, Grid, Context, List views, and to home page portlets. On these views classifier fields are read-only.

8. If the classifier is for taxonomy suggestions, add the classifier target fields to views where you want them to display (optional). Ensure that **Read-Only** is cleared so that the fields are editable. On the Detail and Add New views, although you can place the classifier target field anywhere, you might want to place them immediately following the classifier field. You can also choose not to display the classifier target fields on the views.
9. Re-create the reporting framework so you can access usage data in Cognos. Do this only one time, not for every service you configure. For information, see “Generating the reporting framework ” on page 683.
10. Test the configuration and resolve errors.

What to do next

After the service is in use, you can download data and monitor performance. For information, see “Monitoring and downloading classifier data usage ” on page 730.

A Natural Language Classifier service is in one language. IBM supports a fixed set of languages. You can use multiple Natural Language Classifier services simultaneously, either for different purposes or to support multiple languages for the same purpose.

If you use multiple services for taxonomy suggestions, each Natural Language Classifier service requires a unique classifier configuration, classifier field, and classifier output fields. A classifier input field can be used in more than one classifier field. However, ensure that each classifier configuration updates different classifier target fields. Do not define multiple classifier configurations that update the same classifier target fields.

For object associations, you must configure a Natural Language Classifier service for each object type and relationship that you want to support. For example, if you want to provide parent association suggestions to Control objects and child association suggestions to Risk objects, you need two Natural Language Classifier services. You can have multiple services per object type. Each service requires a unique classifier configuration and classifier field. A classifier input field can be used in more than one classifier field.

Configuring a Natural Language Classifier in Bluemix

To use a Natural Language Classifier with OpenPages, you must configure it on IBM Bluemix.

Before you begin

Learn about cognitive technology and IBM Bluemix. IBM provides extensive documentation, tutorials, and videos for the Natural Language Classifier. For information, see the Bluemix Knowledge Center (https://www.ibm.com/watson/developercloud/doc/natural-language-classifier/index.html).

About this task

A Natural Language Classifier service is empty when you begin and must be trained for what you want to classify. If, for example, you want to help users correctly classify loss events to the correct Basel II categorization, you map short texts that they might write to the correct Basel II categories. The challenge when you create training data is to write short text inputs that reflect how users describe various loss events. The Natural Language Classifier does not simply search through the texts, but instead interprets their meaning. When the meaning of a text is matched to a classification, it has a higher confidence score.

Procedure

1. Create a IBM Bluemix account.

2. Log in, create the service, and get your service credentials (a user name and password). You need the service credentials later when you define a classifier configuration in OpenPages.

   After you create an instance of the Natural Language Classifier service, you can view the username and password by selecting **Service Credentials** from the left pane of the service dashboard. Service credentials are different from your Bluemix account username and password.
3. Build the training data. Define the short text inputs and map them to classifications. The training data must be in a CSV file. The first column in the file is the short text input to classify. The additional columns are classes that apply to that text.

   If the classifier is for taxonomy suggestions, define the short text inputs and map them to classifications. The training data must be in a CSV file. The first column in the file is the text to classify. The additional columns are classes that apply to that text. The number of classes must be equal to the number of classifier target fields that you define in the classifier configuration. If you set up three classifier target fields, as in the following example, you must have three classes.

Table 227: Example training data for taxonomy suggestions

Short text input	**Class 1**	**Class 2**	**Class 3**
Checks were forged	Internal Fraud	Theft and Fraud	Forgery
Check kiting	Internal Fraud	Theft and Fraud	Check kiting
Smuggling	Internal Fraud	Theft and Fraud	Smuggling
External party stole assets	External Fraud	Theft and Fraud	Theft/Robbery
Product defect	Clients, Products and Business Practices	Product Flaws	Product Defects
Model error	Clients, Products and Business Practices	Product Flaws	Model Errors

If the classifier is for object associations, define the short text inputs and map them to object types. The training data must be in a CSV file. The first column in the file is the short text. The second column is the system name of the object that applies to that text.

Table 228: Example training data for object association suggestions

Short text input	**Class**
Key Management	10.1.2 Key management
Cryptographic key management	10.1.2 Key management
Key management system should be storing keys	10.1.2 Key management
Key management system should be backing up or archiving keys	10.1.2 Key management
Key management system should be destroying keys	10.1.2 Key management

Table 228: Example training data for object association suggestions (continued)	
Short text input	**Class**
Key management system should be backing up or archiving keys	10.1.2 Key management
Security perimeters should be defined	11.1.1 Physical security perimeter
Clear desk policy	11.2.9 Clear desk and clear screen policy
Clear screen policy	11.2.9 Clear desk and clear screen policy

4. Load the CSV file into the Natural Language Classifier service you created on IBM Bluemix.
5. Train the classifier. After it is trained, IBM Bluemix assigns it a classifier ID. You need the classifier ID later when you define a classifier configuration in OpenPages. Every time that you train the classifier, you get a new classifier ID.
6. Ensure that the service is running.

What to do next

Complete the remaining tasks that are described in "Configuring cognitive services" on page 724.

Training the classifier is an iterative process. As users work with it, you can improve and expand the short text inputs. You might need to change or expand the categorizations as they change over time. You can also download classifier usage and improve it. For information, see "Monitoring and downloading classifier data usage " on page 730.

Optionally, set up more security, for example, use a firewall to restrict access to Bluemix. For information, see https://console.ng.bluemix.net/docs/security/index.html#security .

Importing a Watson certificate to the local trust store

You must import a Watson certificate to the local trust store. It is needed to build an SSL communication between the OpenPages GRC Platform servers and the Watson server on IBM Bluemix.

Before you begin

- Obtain the host name of the secure target server, in this case the Watson server. Currently, it is `gateway.watsonplatform.net`. You can verify it on Bluemix (https://www.ibm.com/watson/developercloud/natural-language-classifier/api/v1/). The target secure server is the server that OpenPages GRC Platform connects to in order to retrieve the certificates.
- The target secure server application from which you are going to retrieve the certificate must be running and listening on the port.

About this task

Complete this step even if you do not use SSL. You can use the **Retrieve from port** option in the IBM WebSphere administrative console to retrieve the certificate. The root certificate contains the public key and has been verified by the certificate authority (CA).

Procedure

1. Log on to the IBM WebSphere administrative console.
2. Expand **Security** and click **SSL certificate and key management**.
3. Under **Related Items**, click **Key stores and certificates** and click the **CellDefaultTrustStore** keystore.

4. Under **Additional Properties**, click **Signer certificates** and **Retrieve from port**.
5. Enter the host and port information.
   - **Host**: Enter the host name of the secure target server, for example:

     ```
     gateway.watsonplatform.net
     ```

   - **Port**: Enter the port number of the secure target server application, for example, 443.
   - **Alias**: Enter a descriptive name for the certificate, for example, `watson-nls`.
6. Click **Retrieve signer information**.
7. Verify that the certificate information is for a certificate that you trust.
8. Click **Apply** and then click **Save**.
9. Restart the OpenPages GRC Platform services.

What to do next

Complete the remaining tasks that are described in "Configuring cognitive services" on page 724.

Defining a Classifier Configuration

A classifier configuration defines connection information for an instance of the Natural Language Classifier on IBM Bluemix.

Before you begin

Configure the Natural Language Classifier that you want to connect to. For information, see "Configuring a Natural Language Classifier in Bluemix" on page 725.

Procedure

1. Click **Administration** > **Cognitive Services** > **Natural Language Classifiers**
2. Click **New**.
3. Complete the fields in the **Classifier Information** section.
   a) In **Name**, enter a name.
   b) In **Description**, enter descriptive information.
   c) In **Link**, enter a link to the training page in IBM Bluemix where you can add training data. The link is optional and for information purposes only. The default is `http://www.bluemix.net`.
   d) In **Type**, select Enumeration (taxonomy suggestions) or Association (object association suggestions).
4. Complete the fields in the **IBM Watson Natural Language Classifier Service** section.
   a) Retain the default value in **URL for Request**. It is the URL to the Natural Language Classifier on IBM Bluemix:

      ```
      https://gateway.watsonplatform.net/natural-language-classifier/api/v1/classifiers/
      ```

   b) In **User name**, enter the user from the service credentials of the Natural Language Classifier instance you created.
   c) In **Password**, enter the password from the service credentials of the Natural Language Classifier instance you created.
   d) In **ID**, enter the identifier of the Natural Language Classifier instance that you created and trained.
5. In the **Usage Information** section, in **Confidence Threshold** enter the lowest confidence score that a suggestion must meet.

6. If **Type** is set to Enumeration, in the **Field Settings** section you can provide up to three fields in **Classifier Target Field**. Format is `<Field Group>.<Field Name>.` The order of the fields is important. Place the top-level field first, then the second-level field, and so on.
7. If **Type** is set to Association, complete the **Association** section:
   a) In **Object Type**, enter the name of the object type that is associated, for example, SOXControl.
   b) In **Association Type**, select Child or Parent.
   c) In **Object Path**, enter a path to directories to search, for example, `/Library`.
   d) In **Name Field**, specify the field that is displayed as the object's name after a user selects an object to associate, for example, `System Fields.Name`. Format is `<Field Group>.<Field Name>.`
   e) In **Description Field**, specify the field that is displayed as the object's description after a user selects an object to associate, for example, `System Fields.Description`. Format is `<Field Group>.<Field Name>.`

Results
The system saves the classifier configuration as a JSON file. To make changes, use the **Administration** > **Cognitive Services** > **Natural Language Classifiers** task. Do not edit the JSON files directly.

What to do next

Complete the remaining tasks that are described in "Configuring cognitive services" on page 724.

Defining a classifier field

A classifier field contains the name of a classifier configuration and a classifier input field. The **View Suggestions** button is displayed next to a classifier field.

Before you begin

Define a classifier configuration. For information, see "Defining a Classifier Configuration" on page 728.

About this task
A classifier field is a field whose **Data Type** is set to Classifier. Like other fields in OpenPages, you must add them to views and profiles. For more detailed information, see Chapter 9, "Fields and field groups," on page 137.

You can use Fastmap to import and export classifier fields and the values for suggestions in associated classifier target fields. This is typically done during a migration process. Do not change the classifier field or the values for suggestions after you export and before you re-import.

Procedure

1. Click **Administration** > **Field Group** and create a field group or select a field group for the classifier field.
2. Click **Add** to create a new field.
   a) In **Data Type**, select Classifier.
   b) In **Classifier Configuration Name**, enter the name of the classifier configuration that you created in "Defining a Classifier Configuration" on page 728.
   c) In **Classifier Input Field**, enter the field that contains text to be interpreted by a Natural Language Classifier service, for example, `System Fields.Description`. Format is `<Field Group>.<Field Name>.`
3. Save the field.

What to do next

Complete the remaining tasks that are described in “Configuring cognitive services” on page 724.

Monitoring and downloading classifier data usage

After a Natural Language Classifier service has been implemented, you can monitor data usage and make improvements. You can view what users are searching for and what suggestions they select.

Procedure

1. Click **Reporting** > **Team content** > **OPENPAGES_REPORTS_V6** > **General Reporting** > **General Reporting (Relational)** > **Audit Trail** > **Classifier Audit Trail**.
2. Click **Insert**.
   The results show all requests that were sent to a classifier. Analyze the following columns:
   - **Text sent to Classifier** are the descriptions users entered.
   - **Selected Suggestion** are the suggestions that users chose.
   - **Confidence** is the confidence score that the classifier returned for the selected suggestion.
   - **Classifier Results** are the suggestions that the classifier issued for a description.

What to do next

Use the results to improve the classifier. You can download the usage data as a CSV file and use it as a basis for new training data for the Natural Language Classifier service.

Chapter 32. Configuring IBM OpenPages Regulatory Compliance Management

You can configure IBM OpenPages Regulatory Compliance Management (RCM).

For example, you can configure the RCM Theme Deployer.

RCM Theme Deployer

The RCM Theme Deployer is a tool that you can use to automatically create requirements that are ready for assessment. The tool can also automatically create the appropriate associations.

The RCM Theme Deployer helps you to create the theme structure for business entities. Once you select a theme to deploy to the business entities, the structure is created, including the compliance plan, compliance theme, and the relevant requirement evaluation records beneath the theme, linked to the relevant Control objects.

Users can launch the Theme Deployer in two ways: from the Compliance Theme object (pushing a theme out to business entities) or from the Compliance Plan object (pulling themes into a specific business entity).

The Theme Deployer creates the Compliance Theme object and its related child requirements, represented as Requirement Evaluation (ReqEval) objects. The ReqEval objects are used to evaluate the requirements in an assessment. An association is created between the library Requirement object and the ReqEval object.

You can also link the ReqEval and relevant control instances in that area of the business.

You can also copy library instances of the related customer controls that do not already exist in the target business area.

Note: When users run the RCM Theme Deployer, they will be copying and/or linking objects from the configured Library folders to the configured business entity objects. The users must have the following security access:

- Read access to the Library folders they are copying from
- Read, Write, and Associate access to the business entity objects that they are writing to

Process overview for the RCM Theme Deployer

You can set up the IBM OpenPages Regulatory Compliance Management Theme Deployer if you have the 7.3 or later solutions schema.

If you did a fresh installation of 7.4 with solutions, the IBM OpenPages Regulatory Compliance Management Theme Deployer is already installed. Do the following steps to complete the setup:

- “Configuring the RCM profile” on page 733
- “Setting up auto-naming for RCM objects” on page 733
- “Using the RCM configuration tool” on page 734

If you upgraded to 7.4, you might need to do some post-upgrade steps.

- If you used the RCM Theme Deployer in version 7.3.0.1 or later, you do not need to do any additional steps after you upgrade OpenPages.
- If you upgraded from a fresh installation of 7.3.x with solutions and you did not use the RCM Theme Deployer in your earlier version, do the following steps to set up the RCM Theme Deployer.
  - “Installing the RCM Theme Deployer” on page 732
  - “Configuring the RCM profile” on page 733

– “Setting up auto-naming for RCM objects” on page 733
– “Using the RCM configuration tool” on page 734

Installing the RCM Theme Deployer

If you upgraded to IBM OpenPages GRC Platform 7.4 and you want to use the IBM OpenPages Regulatory Compliance Management Theme Deployer, you need to install it.

About this task

Install the IBM OpenPages Regulatory Compliance Management Theme Deployer to make the tool available to your RCM users.

You can install the RCM Theme Deployer if your environment meets the following requirements:

- You upgraded from a fresh installation (not an upgrade) of OpenPages GRC Platform version 7.3.0.0 or later.
- You have the 7.3 or later solutions schema.

Note: If you did a fresh installation of version 7.4 with solutions, you do not need to install the RCM Theme Deployer. Skip this procedure and continue with the setup. See “Process overview for the RCM Theme Deployer” on page 731.

Procedure

1. Log on to the admin application server as a user with administrative privileges.
2. Go to the *<OP_HOME>*`/installer/migration/upgrade/Module/loaderdata/RCM` directory.
3. Edit the `Environment_Variables.bat|.sh` file.

   Set the following parameters for your environment at the beginning of the file. This file is used by all loading scripts.

   ```
   openpages_domain_folder=<OP_HOME>/bin
   login_username=<OP_Admin_Username>
   login_password=<OP_Admin_Password>
   loader_data_folder=<OP_HOME>/installer/migration/upgrade/Module/loaderdata/RCM
   ```
4. Go to the *<OP_HOME>*`/bin/` directory.
5. Edit the `ObjectManager.properties` file and set the following property to `true`.

   ```
   configuration.manager.force.update.application.strings=true
   ```
6. Go to the *<OP_HOME>*`/installer/migration/upgrade/Module/loaderdata/RCM` directory.
7. Run the `Load_RCM_Config.bat|.sh` script.
8. For security purposes, remove the password from the `Environment_Variables.bat|.sh` file.
9. Edit the *<OP_HOME>*`/bin/ObjectManager.properties` file and set the following property to `false`.

   ```
   configuration.manager.force.update.application.strings=false
   ```
10. Restart the OpenPages admin application server.

    For more information, see Chapter 20, “Starting and stopping servers,” on page 549.
11. Configure the IBM OpenPages Regulatory Compliance Management profile.

    See “Configuring the RCM profile” on page 733.
12. Set up auto-naming for the CompliancePlan object.

    See “Setting up auto-naming for RCM objects” on page 733.
13. Configure IBM OpenPages Regulatory Compliance Management.

    See “Using the RCM configuration tool” on page 734.

Configuring the RCM profile

Use this procedure to configure the IBM OpenPages Regulatory Compliance Management profile so that you can use the RCM Theme Deployer.

Before you begin

The RCM Theme Deployer must be installed. For more information, see "Installing the RCM Theme Deployer" on page 732.

Procedure

1. Log in to OpenPages as a user with administrative privileges.
2. Go to **Administration** > **Profiles**.
3. Click **OpenPages RCM 7.3.0 Master**.
4. Update the **CompliancePlan** object.
   a) Click the **CompliancePlan** object type.
   b) Under **Object Fields**, click **Include** and add the field `RCM-ComPlan:Theme Deployer` as **Display Type** `URL`.
   c) Click **Object Views**.
   d) Click **Detail**.
   e) Click **Choose Fields** and add the `RCM-ComPlan:Theme Deployer` field to the Detail view. Set the field to read-only.
5. Update the **ComplianceTheme** object.
   a) Click the **ComplianceTheme** object type.
   b) Click **Include** and add the field `RCM-Theme:Theme Deployer` as **Display Type** `URL`.
   c) Click **Include** and add the field `RCM-Theme:Theme Type` as **Display Type** `List`.
   d) Click **Detail** under **Object Views**.
   e) Click **Choose Fields** and add the `RCM-Theme:Theme Deployer` field to the Detail view. Set the field to read only.
6. Enable the libraries.
   a) Click the **CompliancePlan** object type.
   b) Click **Detail** under **Object Views**.
   c) Clear **Read only** on the **Library ID** field.
   d) Click the **ComplianceTheme** object type.
   e) Click **Detail** under **Object Views**.
   f) Clear **Read only** on the **Library ID** field.
   g) Click the **Requirement** object type.
   h) Click **Detail** under **Object Views**.
   i) Clear **Read only** on the **Library ID** field.
   j) Click the **ReqEval** object type.
   k) Click **Detail** under **Object Views**.
   l) Clear **Read only** on the **Library ID** field.

Setting up auto-naming for RCM objects

You must set up auto-naming for the CompliancePlan object. Optionally, you can also set up auto-naming for the ComplianceTheme and ReqEval objects.

Procedure

1. Log in to OpenPages as a user with administrative privileges.
2. Go to **Administration** > **Settings**.
3. Set up auto-naming for the CompliancePlan object.
   a) Expand the **GRCM** > **Auto Naming** > **CompliancePlan** > **Auto-Named** folder.
   b) Set the value of **Copied Object** to `True`.
   c) Set the value of **New Object** to `True`.
4. Set up auto-naming for the ComplianceTheme object.
   a) Expand the **GRCM** > **Auto Naming** > **ComplianceTheme** > **Auto-Named** folder.
   b) Set the value of **Copied Object** to `True`.
   c) Set the value of **New Object** to `True`.
5. Set up auto-naming for the ReqEval object.
   a) Expand the **GRCM** > **Auto Naming** > **ReqEval** > **Auto-Named** folder.
   b) Set the value of **Copied Object** to `True`.
   c) Set the value of **New Object** to `True`.

Using the RCM configuration tool

You can use the RCM configuration tool to configure IBM OpenPages Regulatory Compliance Management (RCM).

About this task

When you type fields, use the format *<Field Group>*:*<Field Name>*, ensure that no spaces exist before and after the colon. For example, type `RCM-Req:Reqt Owner`. For system fields, you can type just the field name.

To add another field, click the plus sign, and then type the field.

Note: Rich text fields are shown in plain text in the RCM Theme Deployer.

Procedure

1. Log in to OpenPages as an administrator.
2. Open the RCM configuration tool in a new browser tab or window.
   The URL is:
   `http://<hostname>:<port>/openpages/app/solutions/rcm/config/showConfig`
3. Log in with your OpenPages user account. You must be a member of the `OPAdministrators` group to access the tool. You can have the tool open and simultaneously be logged in to OpenPages to work on other administration tasks.
4. Expand the **Common Properties** section.
5. Enter the following information.
   RCM uses these paths to locate the libraries. Use a forward slash (/) as a separator. For example, enter `/Library/Control`.
   a) Enter the path for the **Control Library Folder**.
   b) Enter the path for the **Requirement Library Folder**.
   c) Enter the path for the **Theme Library Folder**.
   d) Enter the path for the **Root Entity Folder**.
   The **Root Entity Folder** is used to locate the business unit hierarchy.
6. Expand the **Theme Deployer Properties** section.

7. Under **Control Deployment Options**, select one or more of **Create & Link**, **Link**, and **None**.

   These options define the deployment of controls during the deployment of themes. The selections that you make are displayed as options to the end user within the **Theme Deployer** helper.

   - Select **Create & Link** to give the end user the option to create controls, if they do not exist, and to associate existing controls to the deployed Requirement Evaluation (ReqEval) objects.
   - Select **Link** to give the end user the option to associate existing controls to the deployed Requirement Evaluation objects. New objects are not created.
   - Select **None** to give the end user the option of not deploying any controls during the theme deployment process.
8. In the section **Theme Fields to be Copied**, specify the fields to be copied from the Theme Library to the deployed Compliance Theme.

   By default, the field to be copied is set to **Name**, unless auto-naming is enabled. For information about auto-naming, see "Setting up auto-naming for RCM objects" on page 733.
9. In the section **Requirement Fields to be Copied**, specify the fields to be copied from the library Requirement object to the Requirement Evaluation object that is created during deployment.

   By default, the field to be copied is set to **Name**, unless auto-naming is enabled.

   During the copy process, a new Requirement Evaluation (ReqEval) object is created. This object might use different field groups and fields than its parent Requirement.

   If the source and target fields are different, type the fields separated by the vertical line character (|). For example, type `RCM-Req:Overall Reqt Score|RCM-Req-Eval:Applied Overall Rating`.
10. If you selected the **Create & Link** option, use the **Control Fields to be Copied** to enter the fields to be copied from the library Control object to the Control object that is created during the deployment process.

    By default, the field to be copied is set to **Name**, unless auto-naming is enabled.

    This field applies only if you selected **Create & Link** as a control option, because this option creates a Control during the deployment process.
11. In the section **Define BE Grid Columns**, enter the Business Entity grid columns to be displayed in the helper when accessed through the Compliance Theme.
12. In the section **Define Theme Grid Columns**, enter the Theme grid columns to be displayed in the helper when accessed through the Compliance Plan.
13. Click **Validate** to validate your entries.

    The folder paths are validated to ensure that they are in the correct format, and that the folders exist.

    The fields are validated to ensure that the fields that you selected in **Define BE Grid Columns** and **Define Theme Grid Columns** exist in the application.
14. Click **Save**.

Chapter 33. Importing IBM Regulatory Compliance Analytics data

You can import data from IBM Regulatory Compliance Analytics, now called IBM Watson Regulatory Compliance, into IBM OpenPages GRC Platform.

IBM Regulatory Compliance Analytics is an integrated governance, risk, and compliance platform that enables companies to manage risk and regulatory challenges across the enterprise. In addition to its cognitive capabilities, IBM Regulatory Compliance Analytics also provides a common platform to house regulatory documents and their associated obligations across multiple jurisdictions, sectors, and regulators.

The following table shows how the object types in the two systems are mapped:

Table 229: RCA to OpenPages object mapping

This RCA object type ...	**Maps to this OpenPages object type...**
Document	Mandate
Obligation	Requirement
Control	SOXControl

For each object type, you map RCA fields to OpenPages fields. When you import RCA data into OpenPages, new OpenPages objects are created and fields are populated with values from RCA.

Associations between RCA objects are also imported into OpenPages. Each system allows the following associations:

- In RCA:
  - An obligation can have a document as a parent object.
  - A control can have an obligation as a parent object.
  - A control can have a document as a parent object.
- In OpenPages:
  - A Requirement can have a Mandate as a parent object.
  - A SOXControl can have a Requirement as a parent object.
  - A SOXControl cannot have a Mandate as a parent object.

The associations in RCA are imported into OpenPages, except for the associations of RCA controls to documents, which are not imported.

You can partner the RCA data with the capability in OpenPages to use an IBM Watson Natural Language Classifier service when you associate parent and child objects. For example, you can import RCA obligations into OpenPages and then use a Natural Language Classifier service to link them to the most appropriate controls in your library. For information, see Chapter 31, “Configuring cognitive services,” on page 723.

Categorizations and tags in RCA are also imported into OpenPages. They provide meaning and context for an obligation. In OpenPages you can use this information as search criteria, to group requirements together, or to organize requirements by themes. This valuable content is available for you to use as you require.

If the RCA data changes after it is imported into OpenPages, you can reimport the data to pick up the changes in OpenPages. If you change object associations or de-associate objects in RCA and reimport the objects into OpenPages, the object association changes are also made to objects in OpenPages.

After the RCA data is in OpenPages, you can use it to assess the impact of new, changed, and deprecated requirements on your GRC policies and procedures, training and awareness, monitoring and testing, and risk assessments.

Completing the prerequisites for importing IBM Regulatory Compliance Analytics data

You must complete several prerequisites before you can import IBM Regulatory Compliance Analytics data into IBM OpenPages GRC Platform.

Procedure

1. Verify that the RCA post-installation steps in the *IBM OpenPages GRC Installation and Deployment Guide* are completed. The steps contain object schema changes to the Mandate, Requirement, and SOXControl objects.
2. Verify that OPSS-Mand:Type has the enumerated string value `Guideline`.
   a) Click **Administration** > **Field Groups**.
   b) Click **OPSS-Mand**, and then click **Type**.
   c) Verify that `Guideline` is in the list. If not, add it.
3. In OpenPages, update user and user group definitions for administrators who work with RCA data. They need to have the RCA Integration application permission. It controls whether the new menu items on the Administration menu are displayed. It is located in **SOX** > **Administration**.

   They need to have the application permission, RCA Integration. It controls whether the new menu items on the Administration menu are displayed. It is located in **SOX** > **Administration**.

   For more information, see “Types of application permissions” on page 32.
4. Update user and user group definitions for administrators who work with RCA data. They must have read/write permissions to edit the RCA import configuration and to import RCA data.
   a) From the menu bar, click **Administration** > **Manage System Files** > **Files**.
   b) Click the **View** drop-down arrow, and select **Folder View** from the list.
   c) Click the `End User Applications Config` folder.
   d) In the **Access Controls** pane, select **Actions** > **Add**.
   e) In the **Select User or Group to add Access Controls** pop-up, select the user or group that you want to grant access. Grant Read and Write permission.
   f) Click **Add**.

What to do next

You are ready to configure the RCA import. For information, see “Configuring the IBM Regulatory Compliance Analytics data import ” on page 738.

Configuring the IBM Regulatory Compliance Analytics data import

You use the **Administration** > **RCA Integration** > **Configure Import from RCA** task to configure how data from IBM Regulatory Compliance Analytics is mapped to data in IBM OpenPages GRC Platform.

Before you begin

Ensure that the prerequisites are met. For information, see “Completing the prerequisites for importing IBM Regulatory Compliance Analytics data ” on page 738.

About this task

Follow these guidelines when you define the RCA import configuration:

- The **ID** field is mandatory and must be a string data type. It is used to match objects in the two systems.
- The data types of mapped fields must be the same, for example, a date field in RCA must be mapped to a date field in OpenPages.
- The format for the **Categorizations** fields is `<Categorization>=<Field Group>.<Field Name>`, where `<Categorization>` is an RCA categorization and `<Field Group>.<Field Name>` is the OpenPages field that it is mapped to. You can map multiple categorization fields.
- The format for the **Fragments** field is `<Fragment>=<Field Group>.<Field Name>`, where `<Fragment>` is an RCA fragment and `<Field Group>.<Field Name>` is the OpenPages field that it is mapped to. You can map multiple fragment fields.
- For all other fields, the format is `<Field Group>.<Field Name>`.
- Field mapping values are case sensitive.
- If you leave a field mapping blank, the field is not imported into OpenPages.
- The object types in OpenPages (Mandate, Requirement, and SOXControl) are fixed and you must use all three. You cannot, for example, import Mandates and Requirements and not SOXControls.
- The RCA fields in the configuration are fixed. You cannot add more fields.

Procedure

1. Click **Administration** > **RCA Integration** > **Configure Import from RCA**.
2. Complete the fields in the **Regulatory Compliance Analytics Information** section. You can get this information from RCA.
   a) In **URL**, enter the URL for RCA, for example `https://rca.ibmcloud.com`.
   b) In **API Key**, enter the API key for RCA.

      For information about generating API keys in RCA, see the RCA Knowledge Center (https://www.ibm.com/support/knowledgecenter/SS9KS2/using_rca/t_api_key.html).
   c) In **Organization ID**, enter the organization ID for RCA.

      For information about organization IDs in RCA, see the RCA Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS9KS2/using_rca/t_export_to_op.html).
3. Complete the fields in the **OpenPages Information** section.
   a) In **Parent Business Entity Path**, enter the path where the parent business entity is located. Use a forward slash (/) as a separator, for example, `/Library/RCA`.
4. Retain the default values for the Mandate object fields in the **RCA Document field mapping to OpenPages Mandate object fields** section or change them to meet your requirements.

Table 230: RCA Document field mapping to OpenPages Mandate object fields section

RCA Document field	OpenPages Mandate field (default values)
Name	`OPSS-RCA-Base.RCA Name`
Description	`System Fields.Description`
ID	`OPSS-RCA-Base.RCA Id`
Identifier	`RCM-Mand.Library Id`
Content source	`OPSS-Mand.Content Source`
Owner	`OPSS-RCA-Base.RCA Owner`
Assignee(s)	`OPSS-RCA-Base.RCA Assignees`

Table 230: RCA Document field mapping to OpenPages Mandate object fields section (continued)	
RCA Document field	**OpenPages Mandate field (default values)**
In force date	RCM-Mand.Mandate In Force Date
Publish date	RCM-Mand.Mandate Proposal Date
Regulator	OPSS-Mand.Issuer
Document type	OPSS-Mand.Type
Categorization	IT Process Model=OPSS-RCA-Base.IT Process Model Line of Business=OPSS-RCA-Base.Line of Business Product=OPSS-RCA-Base.Product

5. Retain the default values for the Requirement object fields in the **RCA Obligation field mapping to OpenPages Requirement object fields** section or change them to meet your requirements.

Table 231: RCA Obligation field mapping to OpenPages Requirement object fields section	
RCA Obligation field	**OpenPages Requirement field (default values)**
Description	System Fields.Description
ID	OPSS-RCA-Base.RCA Id
Content source	OPSS-Req.Content Source
External ID and External System ID	RCM-Req.Library Id
Owner	OPSS-RCA-Base.RCA Owner
Assignee(s)	OPSS-RCA-Base.RCA Assignees
Approval State	OPSS-RCA-Req.Obligation Status
Interpretation	OPSS-RCA-Req.Interpretation
Fragments	Requirement=UCF-Req.Supporting Requirements Guidance=UCF-Req.Guidance

Table 231: RCA Obligation field mapping to OpenPages Requirement object fields section (continued)	
RCA Obligation field	**OpenPages Requirement field (default values)**
Categorization	Compliance Activity=OPSS-RCA-Ext.Compliance Activity Compliance Theme=OPSS-RCA-Ext.Compliance Theme Geography=OPSS-RCA-Ext.Geography IT Process Model=OPSS-RCA-Base.IT Process Model Key Role=OPSS-RCA-Ext.Key Role Line of Business=OPSS-RCA-Req.Materiality Process=OPSS-RCA-Req.Process Product=OPSS-RCA-Base.Product Risk Type=OPSS-RCA-Ext.Risk Type

6. Retain the default values for the SOXControl object fields in the **RCA Control field mapping to OpenPages Control object fields** section or change them to meet your requirements.

Table 232: RCA Control field mapping to OpenPages Control object fields section	
RCA Control field	**OpenPages SOXControl field (default values)**
Name	OPSS-RCA-Base.RCA Name
Description	System Fields.Description
ID	OPSS-RCA-Base.RCA Id
External ID and External System ID	OPSS-Shared-Lib.Library ID
Owner	OPSS-RCA-Base.RCA Owner
Assignee(s)	OPSS-RCA-Base.RCA Assignees
Policy ID	OPSS-RCA-Ctl.Policy ID
Next Review Date	OPSS-RCA-Ctl.Next Review Date
Last Review Date	OPSS-RCA-Ctl.Last Review Date
Last Updated Date	OPSS-RCA-Ctl.Last Updated Date
Status	OPSS-RCA-Ctl.External Status
Comments	OPSS-Ctl.Additional Description

Table 232: RCA Control field mapping to OpenPages Control object fields section (continued)	
RCA Control field	**OpenPages SOXControl field (default values)**

Categorization	`Compliance Activity=OPSS-RCA-Ext.Compliance Activity`
	`Compliance Theme=OPSS-RCA-Ext.Compliance Theme`
	`Control Type=OPSS-Control.Level 1 Category`
	`Geography=OPSS-RCA-Ext.Geography`
	`IT Process Model=OPSS-RCA-Base.IT Process Model`
	`Key Role=OPSS-RCA-Ext.Key Role`
	`Line of Business=OPSS-RCA-Base.Line of Business`
	`Product=OPSS-RCA-Base.Product`
	`Risk Type=OPSS-RCA-Ext.Risk Type`

7. Click **Validate**. Resolve any errors.

What to do next

You can begin importing RCA data into OpenPages. For information, see "Reimporting IBM Regulatory Compliance Analytics data " on page 743.

Importing IBM Regulatory Compliance Analytics data

You use the **Administration** > **RCA Integration** > **Import from RCA** task to import data from IBM Regulatory Compliance Analytics into IBM OpenPages GRC Platform.

Before you begin

Ensure that the following prerequisites are met:

- Define how the data is mapped between the two systems. For information, see "Configuring the IBM Regulatory Compliance Analytics data import " on page 738.
- Verify that you can log in to IBM Regulatory Compliance Analytics.

Procedure

1. Click **Administration** > **RCA Integration** > **Import from RCA**.
2. Click **Import Data**.
   The system starts a long running process that calls the RCA APIs and loads the objects.
3. When the process finishes, click **View Log** or go to **My OpenPages** > **Background Processes** > **My Background Processes** to see the results.
4. Verify that the data loaded correctly in the library that is specified in the import configuration:
   - Verify that new RCA objects were added as new objects in OpenPages.
   - Check that the fields were mapped correctly and that OpenPages fields are now populated with the RCA data.
   - Verify that parent and child associations were correctly imported.

What to do next

The import is finished and you can begin using the information in OpenPages. For information about reimporting data, see “Reimporting IBM Regulatory Compliance Analytics data ” on page 743.

Reimporting IBM Regulatory Compliance Analytics data

You can also use the **Administration** > **RCA Integration** > **Import from RCA** task to reimport data from IBM Regulatory Compliance Analytics into IBM OpenPages GRC Platform.

About this task

If you rerun the import, changes to objects in RCA are replicated to objects in OpenPages. For example, if you add a document or change an obligation description in RCA, the changes are replicated to the objects in OpenPages when you reimport the RCA data. As long as you do not change the parent business entity path, the system finds previously imported objects and does not create duplicate objects.

If you change the object associations in RCA and reimport the changes into OpenPages, the system follows these rules:

- If you remove an association between an obligation and a control in RCA, the matching Requirement and SOXControl in OpenPages are disassociated. The SOXControl might be orphaned.
- If you remove an association between a document and an obligation in RCA, the matching Mandate and Requirement in OpenPages are disassociated. The Requirement might be orphaned.
- If you remove an association between a document and a control in RCA, no action is taken because no matching Mandate and SOXControl association exists in OpenPages. The Mandate remains unchanged in OpenPages.

If you change the objects in OpenPages, those changes can be overwritten if you reimport the matching objects from RCA.

Procedure

1. Follow the steps that are described in “Importing IBM Regulatory Compliance Analytics data ” on page 742. The import process loads both new and changed data.
2. Verify that the data loaded correctly in the library that is specified in the import configuration:
   - Verify that changes to existing OpenPages objects were made.
   - Verify that parent and child associations were updated.
   - Verify that new data was imported.

Appendix A. 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 emails 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 email to a user. The user responsible for the item will receive the email 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 email 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.

The notification reports

If the legacy sample notification reports were installed, a folder on the IBM OpenPages GRC Platform 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 747 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 GRC Platform Notifications Template.

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.

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. For more information, see “Types of application permissions” on page 32)
- Administrator access to the IBM OpenPages GRC Platform server machine (for scheduling reports to run automatically)
- Your notification mail server configured. For more information, see “Set the mail server address” on page 322.

Setting up a notification

Three procedures are required to set up and execute a notification.

- “Task 1: Preparing your data” on page 746
- “Task 2: Creating the notification” on page 747
- “Task 3: Triggering the notification” on page 756

After each task is completed, you can run the notification manually or schedule it to run automatically.

Task 1: Preparing your data

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** icon. 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: Creating the notification

The second task in setting up a notification is to create the notification. IBM OpenPages GRC Platform comes with templates for creating notification reports: **Test Notification**, 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 steps in the following procedure apply to creating either a **Test Notification** or a **General IBM OpenPages FCM Notifications** report.

Procedure

1. Log on to the OpenPages GRC Platform 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. From the folder list, click the **Add Page** icon. 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 "The Test Notification fields" on page 747
      - For **General IBM OpenPages FCM Notifications**, see "The general IBM OpenPages GRC Platform FCM notifications fields" on page 751
   e) Click **Apply** to save your changes.
7. Click **Finish** to save the new report.

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 233: 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 GRC Platform application. This is required if you wish the notification e-mails to be sent in each recipient's selected locale.
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 OpenPages GRC Platform 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.

Table 233: Test Notification template fields (continued)

Parameter	Description
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 OpenPages GRC Platform 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.
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 OpenPages GRC Platform 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.

Table 233: Test Notification template fields (continued)

Parameter	Description
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 OpenPages GRC Platform 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.
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 OpenPages GRC Platform 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.*

Table 233: Test Notification template fields (continued)	
Parameter	**Description**
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 "Set the mail server address" on page 322.
SOX Server	The full URL of the OpenPages GRC Platform 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** icon 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.*

The general IBM OpenPages GRC Platform FCM notifications fields
This topic contains an explanation of the various fields available to reports based on the **General IBM OpenPages FCM Notifications** template.

Table 234: The general 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.
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 OpenPages GRC Platform 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 OpenPages GRC Platform 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.

Table 234: The general template fields (continued)

Parameter	Description
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 OpenPages GRC Platform 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.
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 OpenPages GRC Platform 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 234: The general 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 234: The general 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 "Set the mail server address" on page 322.
SOX Server	The full URL of the OpenPages GRC Platform 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". 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". 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** icon 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 234: The general template fields (continued)	
Parameter	**Description**
Project	Internal parameter. *Do not modify.*
Reporting Period	Internal parameter. *Do not modify.*

Task 3: Triggering 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 **Common** > **Custom ACL Object Types** setting). For instructions on setting up access for these objects, see "Creating an Access Control List" on page 79.

Using the application user interface

Running a notification report from the IBM OpenPages GRC Platform user interface works the same as running any other report through the user interface.

Note: You cannot use the Preview function in the OpenPages GRC Platform user interface with Notification reports.

Procedure

1. Log on to the OpenPages GRC Platform application and click the **Reporting** menu on the menu bar.
2. Click the **Notifications** sub-menu 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 Notification Manager command line interface

You can manually run the Notification Manager from a command or shell window, or you can use standard operating system scheduler functions to automatically run the Notification Manager command file at a specified time.

For example, in Windows, you could use the built-in Windows scheduler, in AIX and Linux, 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 Notification Manager command file is named as follows:

Windows

`NotificationManager.cmd`

AIX and Linux

`NotificationManager.sh`

The file is located in the *<OP_Home>*|`bin` directory of your IBM OpenPages GRC Platform installation.

The Notification Manager command line interface syntax

This topic contains the Notification Manager command line interface syntax and parameters.

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 235: Notification Manager parameters

Parameter	Description
-Username	The name of a valid IBM OpenPages GRC Platform 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 235: 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 OpenPages GRC Platform 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. Properties and parameters

IBM OpenPages GRC Platform includes different properties files. Depending on the configuration task that you perform, you edit one or more of the properties files.

Aurora properties and parameters

Depending on the configuration task that you perform in IBM OpenPages GRC Platform, you might need to edit the parameters in the Aurora properties file.

The Aurora properties file parameters are described in the following list.

Application server properties

aurora.appserver
The type of Java Platform Enterprise Edition (J2EE) application that is used.

Possible value: websphere.

aurora.initialcontext.factory
Java Naming and Directory Interface (JNDI) initial context factory.

Database properties

database.type
Type of database (Oracle or DB2).

database.URL
Java Database Connectivity (JDBC) URL.

database.DRIVER
Java Database Connectivity (JDBC) driver.

database.USERID
Database user name.

database.PASSWORD
Database password (encrypted).

DB2 database properties

database.NAME
Database name.

database.HOSTNAME
Database host name.

database.PORT
Database port.

database.CATALOG_NAME
Database catalog name.

Database pool properties

database.pool.minsize
Minimum number of connections.

database.pool.maxsize
Maximum number of connections.

database.pool.refresh.interval
Database pool refresh interval.

database.pool.testonreserve
Flag to test a connection before returning it from the pool.

Possible values: true or false.

Database connection test property

database.test.connection.sql
Specify a Microsoft SQL database with which to test the connection.

The default value is: *select sysdate from dual*.

Service locations properties

url.service.protocol
RMI (Remote Method Invocation) protocol.

url.service.host
RMI (Remote Method Invocation) host.

url.service.port
RMI (Remote Method Invocation) port.

Java Transaction API (JTA) properties

jta.initialcontext.factory
Java Naming and Directory Interface (JNDI) Initial Context Factory.

jta.jndi.transaction
Java Naming and Directory Interface (JNDI) name for User Transactions.

Full text search properties

fulltext.index.directory
Full text index folder.

fulltext.index.exclude
File extensions to be excluded.

The default values are: `xra xrl pagespec pagetemplate xrt cha xsd`.

Java Message Service (JMS) properties

jms.initialcontext.factory
Java Naming and Directory Interface (JNDI) Initial Context Factory.

jms.nontx.connection.factory
Java Message Service (JMS) connection factory name (non-transactional).

jms.connection.factory
Java Message Service (JMS) connection factory name (transactional).

jms.topic.RepositoryTopic
Java Message Service (JMS) topic name.

jms.topic.ResourceCacheTopic
Java Message Service (JMS) topic name.

Security service properties

security.accesstoken.timeout
Session token timeout, in minutes.

The default value is 3000000.

security.system.password
Password of the system OPSystem user.

WebDAV properties

base64.encoder.classname
Deprecated.

webdav.console.message.prefix
Deprecated.

webdav.version.default.multiversioned
Deprecated.

AppServer specific properties

appserver.weblogic.install.directory
The installation folder of the Application Server.

appserver.install.directory
The installation folder of OpenPages application.

XML forms property

xmlforms.webapp.directory
Folder where custom forms are dropped.

Cache refresh intervals properties

cache.refresh.interval.namespace
Refresh interval for global cache.

Deprecated.

cache.refresh.interval.usergroup
Refresh interval for global cache.

Deprecated.

cache.refresh.interval.assettype
Refresh interval for global cache.

Deprecated.

cache.refresh.interval.contenttype
Refresh interval for global cache.

Deprecated.

cache.refresh.interval.bundledef
Refresh interval for global cache.

Deprecated.

cache.refresh.interval.apppermission
Refresh interval for global cache.

Deprecated.

Resource cache properties

cache.resource.jms.enabled
Deprecated.

cache.resource.debug.on
Deprecated.

cache.resource.capacity
Deprecated.

Third-party reporting-specific properties

cognos.server
Server URL of Cognos.

cognos.framework.refresh.servlet
Framework refresh URL.

cognos.report.output.dir
Temporary folder for reports.

cognos.computation.server
Cognos computation server URL.

Enable read-access locking property

allow.locking.read.access
Deprecated.

Thread dump interval property

periodic.thread.dump.enabled
Periodically enables a thread dump to the local file system (only used in debugging mode).

Possible values: true or false.

Logout URL property

Add new URLs with the name `logout.url.`*`name`*. The name can be anything.

logout.url.cognos
Cognos logout URL.

Publishweb folder property

publish.web.folder
Location of reporting Java Server Page (JSP) files.

Application URL property

application.url.path
Base URL of the application.

Application server WorkManager properties

workmanager.jndi.name
Java Naming and Directory Interface (JNDI) name of the application server work manager.

workmanager.impl.classname
Work manager implementation class.

Enterprise JavaBeans (EJB) properties

server.use.local.ejb
Use the local interfaces for Enterprise JavaBeans (EJB) instead of remote.

OpenPages Cloud environment properties

cognos.internal.server
The Cognos URL with the Cognos private IP address that is used for internal communication from OpenPages to Cognos.

Value: `http\://<cognos_private_ip>/ibmcognos/cgi-bin/cognos.cgi`

db.storage.temp.dir
On cloud versions of the application, the path on the application server where the OpenPages application creates a temporary file, and then streams the file content to database storage. This property does not exist in on-premise versions of the application.

Value: `/opt/OP/OpenPages/profiles/<hostname>-OPNode1/storage`

product.type
The cloud switch that is used to determine whether the product is on Cloud or on-premise. If the value is not Cloud, or is not specified, then the product is deemed on-premise. This property does not exist in on-premise versions of the product.

Value: Cloud

OpenPages server properties and parameters

Depending on the configuration task that you perform in IBM OpenPages GRC Platform, you might need to edit the parameters in the `<servername>-OPNode<#>Server<#>-server.properties` file.

The OpenPages server properties are described in the following list:

Domain property

appserver.weblogic.domain
Non-configurable system parameter.

Cache properties

cache.synchronizer.classname
Non-configurable system parameter.

cache.listener.enabled
Non-configurable system parameter.

cache.notifier.enabled
Non-configurable system parameter.

jms.providerurl
If you change the OpenPages bootstrap port number (default: 10101), update the bootstrap port value in this parameter.

jms.topic.CacheTopic
Non-configurable system parameter.

Administration server properties

dmgr.hostname
Non-configurable system parameter.

dmgr.iiop.port
Non-configurable system parameter.

Transaction properties

jta.providerurl
If you change the OpenPages bootstrap port number (default: 10101), update the bootstrap port value in this parameter.

periodic.thread.dump.enabled
Possible values: true or false.

URL properties

url.service.port
If you change the OpenPages bootstrap port number (default: 10101), update the bootstrap port value in this parameter.

url.path.openpages
Configurable application URL.

Value: http\://*<hostname>*\:10108/openpages, where *hostname* is fully qualified, and includes the local host and the parent domain name.

If you change the OpenPages application port number (default: 10108), update the application port value in this parameter. For more information, see "Updating port values in IBM OpenPages property files" on page 474.

url.service.rule
If you change the OpenPages bootstrap port number (default: 10101), update the bootstrap port value in this parameter.

url.service.security
If you change the OpenPages bootstrap port number (default: 10101), update the bootstrap port value in this parameter.

url.service.repository
If you change the OpenPages bootstrap port number (default: 10101), update the bootstrap port value in this parameter.

url.service.transformation
If you change the OpenPages bootstrap port number (default: 10101), update the bootstrap port value in this parameter.

url.service.sitegenerator
If you change the OpenPages bootstrap port number (default: 10101), update the bootstrap port value in this parameter.

url.repositoryService
If you change the OpenPages bootstrap port number (default: 10101), update the bootstrap port value in this parameter.

url.service.clientapi
If you change the OpenPages bootstrap port number (default: 10101), update the bootstrap port value in this parameter.

security.providerurl
If you change the OpenPages bootstrap port number (default: 10101), update the bootstrap port value in this parameter.

service.client.providerurl
If you change the OpenPages bootstrap port number (default: 10101), update the bootstrap port value in this parameter.

Web client properties

webclient.http.server.protocol
Enter the value `http` or `https`, based on your configuration. The default value is `http`.

webclient.http.server.name
Non-configurable system parameter.

webclient.http.server.port
If you change the OpenPages application port number (default: 10108), update the application port value in this parameter.

Sosa properties and parameters

Depending on the configuration task that you perform in IBM OpenPages GRC Platform, you might need to edit the parameters in the `<servername>-OpenPagesServer<#>-sosa.properties` file.

The `<servername>-OpenPagesServer<#>-sosa.properties` file parameters are described in the following list.

Application URL properties

application.url.path
Configurable application URL.

http\://*<hostname>*\:10108/openpages, where *hostname* is fully qualified, and includes the local host and the parent domain name.

If you change the OpenPages application port number (default: 10108), update the application port value in this parameter.

application.context
Configurable application context.

/openpages

Service URL properties

openpages.service.protocol
Non-configurable system parameter.

openpages.service.host
Non-configurable system parameter.

openpages.service.port
If you change the OpenPages bootstrap port number (default: 10101), update the bootstrap port value in this parameter.

openpages.service.initial.ctx.factory
Non-configurable system parameter.

Appendix C. Installing and configuring HTTP compression

Installing and configuring HTTP compression applies to Microsoft Windows IIS 7 only and is a one-time setup for HTTP compression on the Cognos server.

For details, see the following topics:

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 or install static or dynamic compression, use the following steps.

Procedure

1. On the Cognos 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" on page 767. 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, follow this procedure.

Procedure

1. On the Cognos 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.
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 D. Legacy Reporting Framework Generation settings

Legacy Reporting Framework Generation settings applies only to systems that have been upgraded from versions of OpenPages 5.x or earlier and are using the Legacy Reporting Framework.

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
```

Table 236: Non-default legacy framework namespace required entries

Entry	Description
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.
BY_RELATIONSHIPS	This entry is only used for non-default namespaces. If no "BY" relationships are required, you can leave this entry blank.
Is Default	In the supplied framework model, the value of the DEFAULT namespace is set to `true` and should not be changed. All other IBM OpenPages GRC Platform 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.
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.
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.
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.

The framework generator uses the definition of a namespace (from **ObjectModel 1** and **ObjectModel 2**) to create corresponding namespaces in the framework model. The following table lists the relationship between objects when a namespace is generated.

Table 237: 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.

For more information about namespaces and the framework model, see the OpenPages GRC Platform documentation located on your installation kit.

Defining a 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.

Legacy Reporting Framework custom namespace names

There are several 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 GRC Platform default namespace name.

Adding a non-default namespace to the Legacy Reporting Framework

You can add a non-default namespace to the Legacy Reporting Framework.

Procedure

1. Access the **Settings** page (see Chapter 15, “Viewing the Configuration and Settings page,” on page 307).
2. Set the value in the **Show Hidden Settings** setting to `true`. For details, see “Show hidden settings” on page 311).
3. Expand the **OpenPages | Platform | Reporting | Framework | Generation | Namespaces** folder hierarchy.
4. Select the **Namespaces** folder, and then click **Add Folder**.

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 **Copy To**.

   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 more information, see “Updating the reporting framework” on page 686.

    After the framework generation is complete, the new namespace is available in Cognos to report authors.

Editing an existing Legacy Reporting Framework namespace

You can modify the values contained in an existing namespace to satisfy your reporting requirements. Do not change the relationships of any IBM OpenPages GRC Platform supplied namespaces.

Procedure

1. Access the **Settings** page (see Chapter 15, “Viewing the Configuration and Settings page,” on page 307).
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 686.

Results

After the framework generation is complete, the modified namespace is available in Cognos to report authors.

Appendix E. Non-role based access control

You can use non-role based access control for backward compatibility with IBM OpenPages Governance Platform 5.1x (and earlier).

For flexible role-based security administration, it is best to migrate your access control data to the role-based security model. For details, see “Role-based security model” on page 43). 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.

You can set 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 GRC Platform 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 GRC Platform 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*).

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 higher-level 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. By default, all users can edit any object in the entire project.

This setup is useful for smaller projects, where there is a single or very few teams working on the same business entity structure. In the case where you have specific users who are denied viewing or editing permissions, you can easily deny them access to a 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 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 GRC Platform 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 previous example, 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.

Procedure

1. Log on to the OpenPages GRC Platform application as a Super Administrator user with the **Access Control Lists** application permission set.
2. Click **Administration** > **Custom Security**.
3. Navigate to the business entity folder where you want to break inheritance (under the *Default* directory).
4. When you have found the desired folder, click the name of the folder to display the detail page.

5. Click **Add** and choose the desired group or user from the list.
6. Choose the desired permissions for the group or user by highlighting the appropriate entries and click the **OK** icon to add the new ACL to the folder.
7. Now that a valid ACL exists for the folder, click the **Disable Inheritance** icon under the Folder heading. The value of the "Inherit ACL" field is changed to "false" and the **Disable Inheritance** icon changes to **Enable Inheritance**.
8. Click **Access Controls** in the breadcrumb trail to return to the Access Controls folder list.

Results

After you break the inheritance on a folder, the new permissions (or lack thereof) go into effect immediately. Only members of the OpenPagesAdministrators and OPAdministrators groups will be able to access the object, unless a specific ACL for a user or group is created.

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 an ACL on a folder

You must have the Access Control Lists application permission to view or edit ACL settings.

Procedure

1. Log on to the IBM OpenPages GRC Platform application as a Super Administrator user with the **Access Control Lists** application permission set.
2. Click **Administration** > **Custom Security**.
3. 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.
4. Click **Add** to add a new access control to the list.
5. In the Create an Access Control Setting page, choose the desired group or user from the drop-down list.
6. 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.
7. 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. Log on to the IBM OpenPages GRC Platform application as a Super Administrator user with the **Access Control Lists** application permission set.
2. Click **Administration** > **Custom Security**.
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 modify and click the **Edit** icon to display the Edit an Access Control Setting page.
5. 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. Log on to the IBM OpenPages GRC Platform application as a Super Administrator user with the **Access Control Lists** application permission set.
2. Click **Administration** > **Custom Security**.
3. Navigate the folder tree to display the folder containing the ACL you want to delete.
4. Click the folder name to display the detail page with the list of existing ACLs.
5. Click the check box next to the existing ACL you wish to remove and click the **Delete** icon 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.

Understand how groups are 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.

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.

After you create 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.). After you create 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

Three procedures are required to configure nested groups and limit user scope. Tasks are : break the inheritance of business entities to restrict the scope of users and groups, nest groups inside one another, and add ACLs to regions and sites.

- "Limiting user access by breaking folder inheritance" on page 781
- "Limiting user access by nesting user groups" on page 781
- "Limiting user access by setting folder Access Control Lists" on page 783

Limiting user access by 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.

Read permission is the most important. Read allows you to see folders underneath the business entity and navigate down to them. However, with many Regions and Sites to set up, we don't want to have to keep Denying access to all sorts of groups.

Procedure

1. Log on to IBM OpenPages GRC Platform as a Super Administrator user with the **Access Control Lists** application permission set.
2. Click **Administration** > **Custom Security**.
3. Navigate to the business entity folder where you wish to break inheritance (under the *Default* directory).
4. When you have found the folder, click the name of the folder to display the detail page.
5. Click **Add** in the Access Controls table and choose the desired group or user.
6. Highlight the desired permissions for the group or user and click **OK** to add the ACL to the folder.
7. Now that a valid ACL exists for the folder, click the **Disable Inheritance** icon under the Folder heading. The value of the "Inherit ACL" field is changed to "false" and the **Disable Inheritance** icon changes to **Enable Inheritance**.
8. Click **Access Controls** in the breadcrumb trail to return to the Access Controls folder list.
9. 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.

Limiting user access by nesting user groups

Now you have a lot of groups with users assigned to them according to their role.

Now, 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:

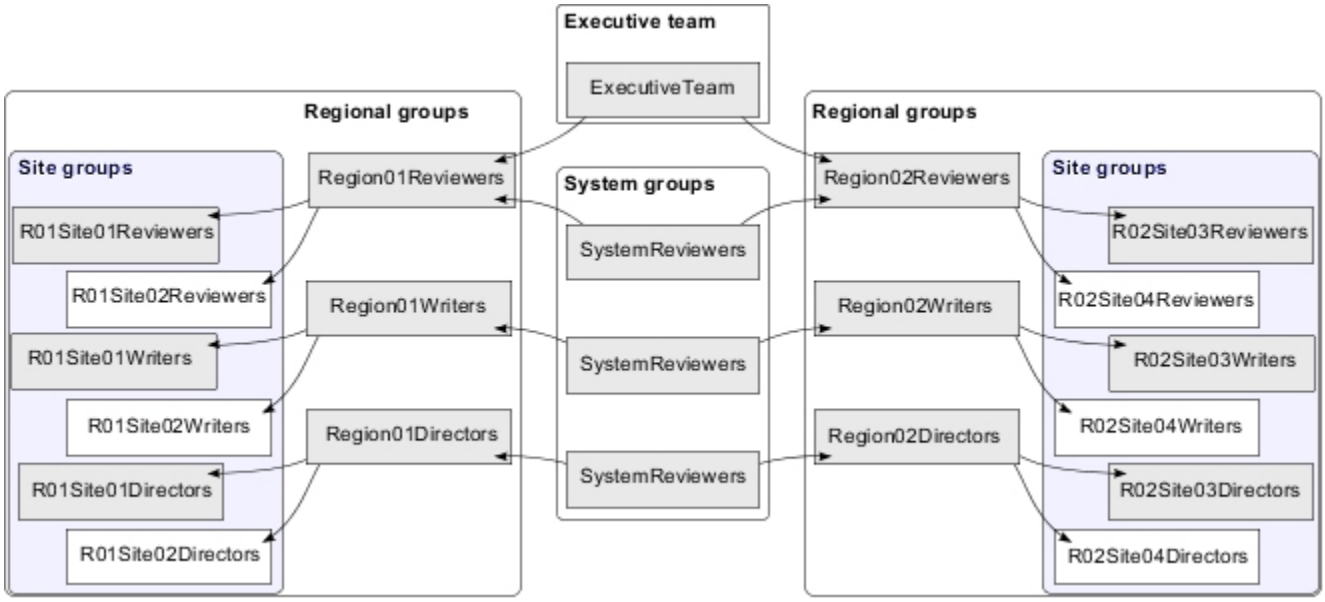


Figure 39: Nesting user groups

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 previous 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 identify how to use the nested groups to set ACLs.

Limiting user access by setting folder Access Control Lists

User groups with different permission needs are defined for each site. The next task is to create ACLs.

For each site, 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:

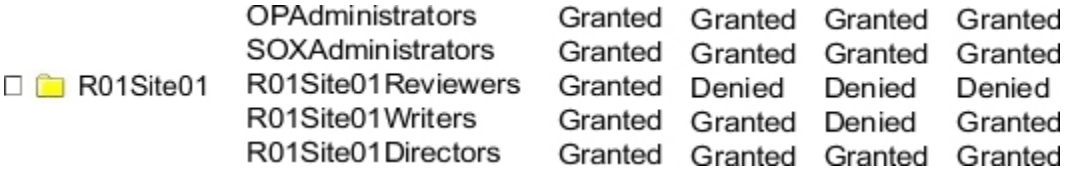


Figure 40: ACLs for the Business Entity folder

It is not necessary to specify the Region01Reviewers, Writers, or Directors. They are included as members of the R01Site01 groups!

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:

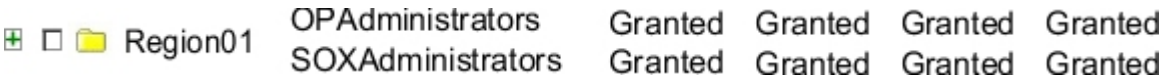


Figure 41: ACLs for the Region01

The following guidelines identify whether to create an ACL for a user group on a business entity:

- If the business entity has accounts or processes associated with it, create an ACL for each entity-specific group (such as R01Site01Writers, etc.) with the correct permissions.
- When you create ACLs for a business entity, 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 no object of that type currently exists in the business entity hierarchy, or parent folder 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 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, complete the following steps:

Procedure

1. Access the Users, Groups and Domains page (see Chapter 3, “Users, groups, and domains,” on page 19).
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 its member groups to browse to their site.
3. Create a similar group for each business entity above the lowest level (Site, in our example).
4. Log on to IBM OpenPages GRC Platform as a Super Administrator user with the **Access Control Lists** application permission set.
5. Click **Administration** > **Custom Security**.
6. Navigate to your business entity folder structure (under *\Default\BusinessEntities*).
7. 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.

   To make the Browsers groups easy to use, roll-up each site users into a single group that can be added to the Region01Browsers group.
8. Add the R01Site01Directors and R01Site01Writers group to the R01Site01Reviewers group.
9. 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.
10. Repeat the process for the rest of the business entities.
11. 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 "Location01," etc., we would create a group called Location01Browsers, and add the Region01Browsers group to it. However, if Region02 was not a child of Location01, you would not add Region02Browsers to the Location01Browsers group.
12. After the groups are added, log out and log back in with a Site level user. Test that the ACLs are working.

Appendix F. Troubleshooting and support for IBM OpenPages GRC Platform

To isolate and resolve problems with IBM products, use the troubleshooting and support information. This information contains instructions for using the problem-determination resources that are provided with IBM products, including OpenPages GRC Platform.

Techniques for troubleshooting problems

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem. Certain common techniques can help with the task of troubleshooting.

The first step in the troubleshooting process is to describe the problem completely. Problem descriptions help you and the IBM technical-support representative know where to start to find the cause of the problem. This step includes asking yourself basic questions:

- What are the symptoms of the problem?
- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can the problem be reproduced?

The answers to these questions typically lead to a good description of the problem, which can then lead you to a problem resolution. For more information, see “Searching knowledge bases” on page 786.

What are the symptoms of the problem?

When you begin to describe a problem, the most obvious question is "What is the problem?" This question might seem straightforward; however, you can break it down into several more-focused questions that create a more descriptive picture of the problem. These questions can include:

- Who, or what, is reporting the problem?
- What are the error codes and messages?
- How does the system fail? For example, is it a loop, hang, crash, performance degradation, or incorrect result?

Where does the problem occur?

Determining where the problem originates is not always easy, but it is one of the most important steps in resolving a problem. Many layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few of the components to consider when you are investigating problems.

The following questions help you to focus on where the problem occurs to isolate the problem layer:

- Is the problem specific to one platform or operating system, or is it common across multiple platforms or operating systems?
- Is the current environment and configuration supported?
- Do all users have the problem?
- (For multisite installations.) Do all sites have the problem?

If one layer reports the problem, the problem does not necessarily originate in that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some

time to completely describe the problem environment, including the operating system and version, all corresponding software and versions, and hardware information. Confirm that you are running within an environment that is a supported configuration; many problems can be traced back to incompatible levels of software that are not intended to run together or were not fully tested together.

When does the problem occur?

Develop a detailed timeline of events that led up to a failure, especially for those cases that are one-time occurrences. You can most easily develop a timeline by working backward: Start at the time an error was reported (as precisely as possible, even down to the millisecond), and work backward through the available logs and information. Typically, you must look only as far as the first suspicious event that you find in a diagnostic log.

To develop a detailed timeline of events, answer these questions:

- Does the problem happen only at a certain time of day or night?
- How often does the problem happen?
- What sequence of events leads up to the time that the problem is reported?
- Does the problem happen after an environment change, such as upgrading or installing software or hardware?

Responding to these types of questions can give you a frame of reference in which to investigate the problem.

Under which conditions does the problem occur?

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These questions about your environment can help you to identify the root cause of the problem:

- Does the problem always occur when the same task is being performed?
- Does a certain sequence of events must happen for the problem to occur?
- Do any other applications fail at the same time?

Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Because multiple problems might have occurred around the same time does not mean that the problems are related.

Can the problem be reproduced?

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem can be reproduced you have a larger set of tools or procedures at your disposal to help you investigate. Problems that you can reproduce are often easier to debug and solve.

However, problems that you can reproduce can have a disadvantage: If the problem is of significant business impact, you do not want it to recur. If possible, re-create the problem in a test or development environment, which typically offers you more flexibility and control during your investigation.

- Can the problem be re-created on a test system?
- Are multiple users or applications encountering the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

Searching knowledge bases

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods.

About this task

You can find useful information by searching the IBM Knowledge Center. However, sometimes you must look beyond the knowledge center to answer your questions or resolve problems.

Procedure

To search knowledge bases for information that you need, use one or more of the following approaches:

- Find the content that you need by using the IBM Support Community.

  The IBM Support Community is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services. Use the IBM Support Community to access the IBM electronic support portfolio from one place. You can tailor the pages to focus on the information and resources that you need for problem prevention and faster problem resolution.
- Search for content by using the IBM masthead search.

  You can use the IBM masthead search by typing your search string into the **Search** field at the beginning of any ibm.com® page.
- Search for content by using any external search engine, such as Google, Yahoo, or Bing.

  If you use an external search engine, your results are more likely to include information that is outside the ibm.com domain. However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on ibm.com.

  Tip: Include "IBM" and the name of the product in your search if you are looking for information about an IBM product.

Getting fixes

A product fix might be available to resolve your problem.

Procedure

To find and install fixes:

1. Determine which fix you need. Go to http://www-933.ibm.com/support/fixcentral/
2. Download the fix. Open the download document and follow the link in Download the package.
3. Apply the fix. Follow the instructions in Installation Instructions of the download document.
4. Subscribe to receive weekly email notifications about fixes and other IBM Support information.

Contacting IBM Support

IBM Support assists with product defects, answers FAQs, and helps users resolve problems with the product.

Before you begin

After you tried to find your answer or solution by using other self-help options such as Technotes, you can contact IBM Support. Before you contact IBM Support, your company or organization must have an active IBM maintenance contract, and you must be authorized to submit problems to IBM. For information about the types of available support, see the Support portfolio topic in the "*Software Support Handbook*".

Procedure

To contact IBM Support about a problem:

1. Define the problem, gather background information, and determine the severity of the problem.

   For more information, see the Getting IBM support topic in the *Software Support Handbook*.
2. Gather the following diagnostic information:

- Environment type (such as production or development).
- Release and patch level (such as IBM OpenPages GRC Platform 7.4.0.0 or 7.4.0.1).
- Application server type (IBM WebSphere).
- Description of the issue.
- Detailed steps to reproduce the issue.
- Screen captures of the issue.
- Expected and actual results.
- OpenPages GRC Platform log files (for more information, see "Using log files" on page 537).
- Any workarounds that you have implemented.
- The date and time that the issue was encountered.
- Database type (such as Oracle 12.1.0.2.0 or DB2 11.1).

3. Submit the problem to IBM Support in one of the following ways:
   - Using IBM Support Assistant (ISA): Use this feature to open, update, and view an Electronic Service Request with IBM. Any data that was collected can be attached to the service request. This feature expedites the analysis and reduces the time to resolution.
   - Online through the IBM Support Community: You can open, update, and view all of your service requests from the Service Request portlet on the **Service Request** page.
   - By phone: For the phone number to call in your region, see the Directory of worldwide contacts web page.

Results

If the problem that you submit is for a software defect or for missing or inaccurate documentation, IBM Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM Support website daily, so that other users who experience the same problem can benefit from the same resolution.

"Contacting IBM Support" on page 787
"Exchanging information with IBM" on page 788

Exchanging information with IBM

To diagnose or identify a problem, you might be necessary to provide IBM Support with data and information from your system. In other cases, IBM Support might provide you with tools or utilities to use for problem determination.

Sending information to IBM Support

To reduce the time that is required to resolve your problem, you can send trace and diagnostic information to IBM Support.

Procedure

To submit diagnostic information to IBM Support:

1. Open a problem management record (PMR). You can use the IBM Support Assistant or The Service Request tool.
2. Collect the diagnostic data that you need. Diagnostic data helps reduce the time that it takes to resolve your PMR. You can collect the diagnostic data manually or automatically.
3. Compress the files by using the `.zip` or `.tar` file format.
4. Transfer the files to IBM.

   You can use one of the following methods to transfer the files to IBM:

- IBM Support Assistant
- The Service Request tool
- Standard data upload methods: FTP, HTTP
- Secure data upload methods: FTPS, SFTP, HTTPS
- Email

All of these data exchange methods are explained on the IBM Support website.

Receiving information from IBM Support

Occasionally an IBM technical-support representative might ask you to download diagnostic tools or other files. You can use FTP to download these files.

Before you begin

Ensure that your IBM technical-support representative provided you with the preferred server to use for downloading the files and the exact directory and file names to access.

Procedure

To download files from IBM Support:

1. Use FTP to connect to the site that your IBM technical-support representative provided and log in as `anonymous`. Use your email address as the password.
2. Change to the appropriate directory:
   a) Change to the `/fromibm` directory.

   ```
   cd fromibm
   ```

   b) Change to the directory that your IBM technical-support representative provided.

   ```
   cd nameofdirectory
   ```

3. Enable binary mode for your session.

   ```
   binary
   ```

4. Use the `get` command to download the file that your IBM technical-support representative specified.

   ```
   get filename.extension
   ```

5. End your FTP session.

   ```
   quit
   ```

Subscribing to Support notifications

To stay informed of important information about the IBM products that you use, you can subscribe to notifications.

About this task

By subscribing to receive notifications about IBM OpenPages GRC Platform, you can receive important technical information and updates for specific IBM Support tools and resources. You can subscribe to notifications by using the following approach:

My Notifications

With My Notifications, you can subscribe to Support notifications for any IBM product. (My Notifications replaces My Support, which is a similar tool that you might have used in the past). With My Notifications, you can specify that you want to receive daily or weekly email announcements. You

can specify what type of information you want to receive (such as publications, hints and tips, product flashes (also known as alerts), downloads, and drivers). With My Notifications you can customize and categorize the products about which you want to be informed and the delivery methods that best suit your needs.

Procedure

1. Go to the IBM Support Portal and click **Other** > **My Notifications**.
2. Sign in using your IBM ID and password, and click **Submit**.
3. Select the updates that you want to receive..
   a) Type OpenPages in the **Product lookup** box.
   b) Click **Subscribe**.
   c) Select the types of notifications that you want to receive; for example, new information about product downloads and discussion group comments.
   d) Click **Submit**.
4. Click **Delivery options**. Choose how you want to receive notifications, and then click **Submit**.

Results
Until you modify My Notifications preferences, you receive notifications of updates that you requested. You can modify your preferences when needed (for example, if you stop using one product and begin using another product).

Known problems and solutions for visualizations

Some common problems with visualizations are documented, along with their solutions or workarounds. If you have a problem with visualizations, review the problem-solution topics to determine whether a solution is available to the problem that you are experiencing.

Cannot read labels on a Business Entity diagram

The Business Entity visualization that you want to view contains many hierarchical levels. When the diagram was scaled to fit the browser window, the labels on the diagram are not readable.

To make the labels readable, try one of the following solutions:

- In the Business Entity diagram, select a different node with child elements, and set it as the root of the organizational chart. By setting a new root, you are narrowing the focus of your visualization to a specific segment of the hierarchy.

  Tip: In the diagram, go to the node that you want to be the root of the hierarchy, right-click the node, and select **Make Root**.
- For a more granular view, choose a different level in the organizational hierarchy.

  Tip: From the **Levels** box, select a different level such as Level 1, Level 2, or Level 3.

Diagrams cannot be rendered during Active Reporting Periods

When you click the diagram link to open a visualization, an error message states that the IBM OpenPages GRC Platform system is unable to render the visualization under the Active Reporting Period.

The following error message is displayed when you tried to open a visualization:

```
Unable to render the visualization.
Diagrams cannot be rendered during Active Reporting Periods.
Please change the reporting period or contact your system administrator.
```

Visualizations require the reporting schema from which to derive their data and to load properly. Because Active Reporting Periods are being closed or finalized, the reporting schema is populated only with the data from the current reporting period. Therefore, when the active reporting period is selected, the

reporting schema has no data and the process diagram or Business Entity organizational chart is not rendered.

To solve this problem, you must switch to the current reporting period. On the **Process Detail** page or the **Business Entity Detail** page, from the **Reporting Period**, select **Current**.

You can also finalize or delete the Active Reporting Period. To complete any Reporting Period operation, the OpenPages GRC Platform system must be in System Administration Mode.

Known problems and solutions for global search

Issues that are related to the IBM OpenPages GRC Platform global search component are most commonly encountered when you are setting it up or when it is updated to synchronize the search index for changes that are made to the OpenPages GRC Platform schema (such as adding or removing object types or fields).

When an administrative operation fails, you can normally resolve these issues by clicking **View Log** to see the log message for the failed global search operation.

The most common failure is that the search service is not started, for which you see this error:

"Could not establish connection to the search engine. Please contact your system administrator."

Ensure that the search service is started or restart to try to resolve the issue.

Global search start fails

If you configured the global search services to start and stop by using a script and you forgot to stop global search before rebooting the system, when you attempt to start the global search services, the services will fail to start. To fix this issue complete the following steps.

Procedure

1. Log on to the search server as a user with administrative privileges.
2. Open a command line on the search server.
3. Go to the *<SEARCH_HOME>*/opsearchtools/ directory and run the following commands.

   On Microsoft Windows operating systems, run:

   ```
   opsearchtool.cmd clearState -indexname openpages
   opsearchtool.cmd clearState -indexname folderacl
   ```

   On UNIX operating systems, run:

   ```
   ./opsearchtool.sh clearState -indexname openpages
   ./opsearchtool.sh clearState -indexname folderacl
   ```

Global search setup fails

In some rare cases, the global search component might encounter a failure during the creation of the search index, before the operation completes. The failure might be caused by hardware issues, database issues, or a power outage, for example. When this happens, the state of the global search setup is in an undefined state and the **Enable** button might become available, giving the misleading impression that global search was set up successfully. To recover from this state, investigate the root cause, resolve it, and then set up global search again.

Procedure

1. Investigate and resolve the root cause of the failure.
2. Log on to OpenPages as a user with administrative privileges.
3. Click **Administration** > **Global Search**.

4. Click **Drop** to drop the search index.
5. Wait for the drop process to complete.

   If the **Drop** button is not available or if the drop process fails, see “ Forcing a reset of global search” on page 792.
6. Click **Create** to re-create the search index.

Forcing a reset of global search

In some rare cases, it might be necessary to reset the IBM OpenPages GRC Platform global search component if you cannot restore it from the global search administration page. These issues might prevent you from successfully completing tasks in the global search administration page. To resolve these issues, complete the following steps.

Procedure

1. Log on to the search server as a user with administrative privileges.
2. Open a command line on the search server.
3. Go to the *<SEARCH_HOME>*`/opsearchtools/` directory to run the commands in the following steps.

   Attention: At the successful completion of each command, the statement "Normal completion of command" should appear. If it does not, contact Customer Support to diagnose the issue.
4. Ensure that Solr is running and is reachable on port 8983. If Solr is not running, then run the following command to start it.

   Microsoft Windows:

   ```
   opsearchtool.cmd startSolr
   ```

   UNIX:

   ```
   ./opsearchtool.sh startSolr
   ```
5. Run the following commands to stop indexing.

   Microsoft Windows:

   ```
   opsearchtool.cmd stopIndexing -indexname openpages
   opsearchtool.cmd stopIndexing -indexname folderacl
   ```

   UNIX:

   ```
   ./opsearchtool.sh stopIndexing -indexname openpages
   ./opsearchtool.sh stopIndexing -indexname folderacl
   ```
6. Verify that no `opsearchtool.jar` processes are running.

   On Microsoft Windows operating systems, use the task manager to see whether any `opsearchtool.jar` processes are running. If there are, terminate them.

   On UNIX operating systems, use the `ps` command to see whether any `opsearchtool.jar` processes are running. If there are, terminate them.
7. Run the following commands to clear any PID states that might still be set if the `opsearchtool.jar` processes did not end successfully.

   Microsoft Windows:

   ```
   opsearchtool.cmd clearState -indexname openpages
   opsearchtool.cmd clearState -indexname folderacl
   ```

UNIX:

```
./opsearchtool.sh clearState -indexname openpages
./opsearchtool.sh clearState -indexname folderacl
```

8. Run the following commands to reset global search.

   Microsoft Windows:

   ```
   opsearchtool.cmd resetSolr -indexname openpages
   opsearchtool.cmd resetSolr -indexname folderacl
   opsearchtool.cmd resetDb
   opsearchtool.cmd stopSolr
   opsearchtool.cmd startSolr
   ```

   UNIX:

   ```
   ./opsearchtool.sh resetSolr -indexname openpages
   ./opsearchtool.sh resetSolr -indexname folderacl
   ./opsearchtool.sh resetDb
   ./opsearchtool.sh stopSolr
   ./opsearchtool.sh startSolr
   ```

9. Log on to OpenPages as a user with administrative privileges.
10. Click **Administration** > **Global Search**.
11. Click **Create** to re-create the search index.

What to do next

Resetting the global search component does not change your global search settings, such as object types, fields that are enabled for search, registry settings, or property settings. The reset disables the global search component. You must enable it again to make it available to users.

Checking for global search setup issues and periodic monitoring

When the incremental indexer is running during global search setup or after setup, some records might not get indexed due to issues with the record, other system errors, or application errors.

About this task

If the issues are not unrecoverable, they do not impede the setup process or the incremental indexer. However, the records that do not get indexed are logged in an error-log file, with an error message that explains the issue so you can take appropriate action. The error-log files are never rotated. Periodically examine this directory for new error files.

Procedure

1. Log on to OpenPages as a user with administrative privileges.
2. Go to the directory *<SEARCH_HOME>*`/opsearchtools/logs_error/ .`
3. Examine this directory for new error files.

Before you contact IBM OpenPages Support

When you contact IBM OpenPages Support, you need to collect diagnostic data and provide a detailed use case of the issue.

About this task

Before you contact IBM OpenPages Support to help with resolving global search issues, follow these steps to collect diagnostic data.

Note: You do not need to stop global search, the OpenPages application server, the database server, or any other application when you run the `collectDiagData` command.

Procedure

1. Log in to the OpenPages global search server as a user with administrative privileges.
2. Start a command prompt.
3. Go to the *<SEARCH_HOME>*/opsearchtools/ folder and run the following commands:
   - Microsoft Windows:

     ```
     mkdir diag
     opsearchtool.cmd collectDiagData -diagpath diag
     ```

   - UNIX:

     ```
     mkdir diag
     ./opsearchtool.sh collectDiagData -diagpath diag
     ```

   Attention: The collectDiagData command might report warning messages that look as if the command failed. This warning can happen due to a number of reasons, such as the data that is being collected cannot be accessed or is not yet available. If you see any such warnings, capture them and include them as part of the diagnostic data to IBM OpenPages Support.
4. Add the contents of the new folder that is created under the diag folder to a compressed file.
5. Send the compressed file and complete details about your issue to IBM OpenPages Support.

Known problems and solutions for the QRadar integration package

Some common problems with QRadar integration package are documented, along with their solutions or workarounds. If you have a problem with QRadar integration package, review the problem-solution topics to determine whether a solution is available to the problem that you are experiencing.

TDI properties file error message

When you run the assembly line in the qradar_integration project, you might see one or more warning messages with the error code CTGDIR103W in the Tivoli Directory Integrator (TDI) console.

This message indicates that the enclosing project is missing a properties file, and that the file will be created if anything is written to it.

The following text is an example of a warning that might appear when you run any of the assembly lines that are contained in the qradar_integration project that is included in the IBM OpenPages GRC Platform 7.2 product release:

```
Wed Aug 19 11:13:35 EDT 2015 [qradar_integration] WARN  - CTGDIR103W
The properties file 'C:/TDI-Solutions/workspace/qradar_integration
/Runtime-qradar_integration/qradar_integration.properties'
for Properties.qradar_integration was not found, and will be
created if anything is written to it.
```

These warnings can be safely ignored. In general, a Tivoli Directory Integrator project typically has an associated properties file named after the enclosing project to hold any project-specific properties, but this file is not strictly required.

Do not include security domain groups when creating object filters or security rule formulas

When creating filters for object types using the **Administration** > **Object Types** pages or security rule formulas that involve fields permitting user group selection, it is possible to select a security domain group because these groups are included in the selection list. The selection will not be flagged as an error. However, if you include a security domain group in the object filter criteria or in the security rule, you might encounter application errors later.

To avoid potential errors, ensure that you select a valid user group, and not a security domain group. In the product user interface, security domain groups are represented by this icon  , and user groups are represented by this icon  .

Objects can be saved with an empty required field

If an object contains a redacted field that is also a required field, a user can successfully save the object even when the redacted field value is empty in the OpenPages repository.

JSON file might not display multibyte characters correctly in Wordpad

When you export a JSON file for a Dashboard tab configuration and open it in Microsoft Wordpad, multibyte characters might be corrupted.

This issue might occur if you go to **Administration** > **Profiles**, select a Dashboard tab that uses multibyte characters, click **Edit** and then click **Export JSON**. If you select Wordpad as the application to open the file, the multibyte characters might not display correctly.

The solution is to open JSON files in a text editor that supports UTF-8. The JSON file will display correctly in Notepad or Microsoft Word.

Remediating after an Enumerated String field is changed to a multi-select field (DB2)

If you are using IBM DB2, a subsequent maintenance task is required whenever you convert an enumerated string from single to multi-select. You do not need to do this task immediately. Do this task during your next available maintenance window.

About this task

After an enumerated string field is changed to multi-select, the associated reporting schema tables in the OpenPages database will contain obsolete columns. The application handles the presence of these columns, but a subsequent cleanup should be scheduled in the next available maintenance window. If left unmanaged, these obsolete columns might eventually cause errors in OpenPages.

You can resolve the issue by running a utility against the DB2 database. Alternatively, you can drop and re-create the reporting schema to resolve the issue.

Procedure

1. Log on to the OpenPages admin application server as a user with administrative privileges.
2. Stop all OpenPages services.
3. If you are using Microsoft Windows, start the DB2 command line processor by typing `db2cmd`.
4. Log in to CLPPLUS as the OpenPages database user, for example `openpages`.
5. Run the following command:

   ```
   call OP_RPS_MGR.DROP_AND_REORG_OBSOLETE_RT_COLS;
   ```

   The length of time that it takes for the command to run varies depending on the number of tables with obsolete columns that need to be dropped and the size of those tables.

   When the command completes, the following message is displayed:

   ```
   DB250000I: The command completed successfully.
   ```

System delay when modifying object types and fields (DB2)

If you are using IBM DB2 and the reporting schema is enabled, you can encounter a significant system delay in OpenPages if you make object model modifications. The delay is due to locking conflicts on the IBM DB2 platform.

The following object model modifications can cause a system delay:

- Associating a field group to an object type
- Adding a new field to a field group that is already associated to an object type
- Converting a single valued enumerated field to a multi-valued enumerated field
- Adding new object type associations

To reduce a system delay, follow this process:

1. Choose a time when there is limited or no activity on the system.
2. Enable System Administration Mode.
3. Shut down Cognos Analytics.
4. Disable global search.
5. Complete the object model modifications.
6. Start Cognos Analytics.
7. Enable global search.

Object model modifications cause implicit DDL operations to be performed against the reporting schema. On the IBM DB2 platform share locks are automatically acquired when a read operation is performed. A read operation can block the object model modification. If the read operation is long running, for example, a long running Cognos report, the object model modification can appear to hang. In reality, the object model modification is not hanging but blocked on the session that is performing the read operation. After the read operation completes, the session that is attempting the object modification can proceed. The read operation needs to complete and clear its locks before the implicit DDL operation can acquire the locks that it needs to implement the object model change. If you kill the object model modification operation, the system can be left in an inconsistent state. If this happens, you must recreate the reporting schema.

The following actions do not cause this issue:

- Creating a new object type
- Creating a new field group
- Adding fields to a field group that is not yet associated to an object type
- Changing object text values
- Switching a field from not required to required or vice versa
- Changing the order of enumerated strings in an enumerated field
- Hiding an enumerated field value
- Adding new values to an existing enumerated field
- Modifying profile definitions
- Creating new reporting periods
- Enabling or disabling existing object type associations
- Enabling or disabling of security rules
- Enabling or disabling field level encryption

Appendix G. Best practices for configuring the IBM OpenPages GRC Platform

To improve the performance of IBM OpenPages GRC Platform, administrators can design, configure, and implement OpenPages GRC Platform applications using best practices. These suggested guidelines are provided to help you maximize, streamline, and get the most out of the product environment.

Use short field names and field group names

When creating field groups and field names, use short field group names and short field names.

The length of field group names and field names have the following impacts:

- Long names restrict the number of fields that you can have on an object type.
- Long names increase the length of object type user defined attributes (UDAs), which have a 64 character maximum.

After creating the short field group names and short field names, an administrator can relabel and localize the field names to add meaning. For example, an administrator might create a field called `AudDesEff`, which can be difficult for a user to interpret. In the **Object Text** area of the application, the administrator can update the locale and change the label to a more meaningful name, such as `Audit Design Effectiveness`. By doing this, the administrator minimizes the length of the name but also retains a positive user experience.

Be aware that Java applets are not supported by the Chrome browser

Some functionality that depends on Java applets, such as the File Upload and OPX, may not work as expected when you use the Chrome browser.

Because the Chrome browser does not support Java applets, the Optimized File Upload button on the detail page does not show on browsers that don't support it. For more information, see “Optimize file uploads” on page 323.

For OPX, publishing and reporting functionality such as Assign Files, Assign Folder, Add Page, and so on, do not work with the Chrome browser. You must use Microsoft Internet Explorer in OPX to use the applets that control these features.

Limit the number of objects in views

The IBM OpenPages GRC Platform application allows end users to access data in various views (such as the Overview, Folder Views, Filtered List View, Detail View, Activity Views, and so on). Limiting the number of objects that are displayed in a view improves performance.

About this task

Limit the number of objects in a particular folder location to no more than 150 or 200 objects. If a folder location has more than 200 objects, end users may see performance issues when expanding the folder location, depending on how fast the server is and how fast the browser is.

Limit the number of associations in the Overview

Limit the number of child associations for objects in the **Overview** screen to improve load time for this view.

About this task

Unlike the other views, the **Overview** screen shows objects by associations. If an object has numerous child associations, the page will take longer to display all the content. Administrators can limit the type of child associations displayed by editing the profile and removing various object types.

Procedure

1. Open a supported browser.
2. Go to the IBM OpenPages GRC Platform URL.
3. Log in with an administrator ID.
4. On the navigation menu bar, click **Administration** > **Profiles**.
5. Click a profile.
6. In the **Object Types** section, click the object type.
7. Scroll to the **Navigational Views** section.
8. Click on the **Overview** link.
9. In the **Included Object Types** section, modify the list accordingly.

Limit the number of portlets on the home page

In IBM OpenPages GRC Platform, you can configure portlets on the home page that contain predefined tables or embedded reports. Each portlet that you add to a tab on the home page increases the work that is required to display that tab. A large number of portlets per tab can negatively impact performance. Therefore, you should limit the number of portlets on the home page.

About this task

The exact cost to fetch and display the data for each portlet depends on a number of factors, for example, the data size, filter criteria, security rules, browser, and available system resources.

Limit activity views with field dependencies and dependent picklists

In dependent picklists, the more fields in the picklist, the more JavaScript is required to display the object to users.

In IBM OpenPages GRC Platform, administrators can create user views within a profile. Administrators can also create dynamic field dependencies and dynamic dependent picklists. Depending on how the business object model was designed, a picklist could have several dozen fields as selectable items. Javascript is used to control this behavior when an end user renders the field. The more field dependencies and dependent picklists that are created for an object type, the more javascript is required for an end user to view the object. Depending on what browser is utilized, this can cause performance issues in rendering the page.

When combined with an activity view, an end user can list multiple objects at once. When multiple objects are displayed (such as a 3-level activity view), it will increase the amount of javascript that is loaded on the page.

Limit the number of security rules and complexity of security rules

As an OpenPages administrator, you can use Field Level Security (FLS) and Record Level Security (RLS) in the IBM OpenPages GRC Platform application to create another level of robustness for implementing security.

You can use the rule engine to implement a variety of business security options. With this flexibility, remember that the more complex the rule, the more time it will take to evaluate the rule. The same is also true for the number of rules that are being implemented.

In other words, security rules and evaluating security rules adds a level of overhead to end user operations. End user operations include but are not limited to tasks such as updating an object, using the bulk update in a grid view, and filtering through data.

Limit the number of SOXBusEntity objects in the system

The SOXBusEntity object type is a special object type. When an OpenPages power user or OpenPages administrator creates a SOXBusEntity object type in the IBM OpenPages GRC Platform application, an additional overhead is associated with it.

For example, it might create an additional security context point for OpenPages administrators. This creates additional administrative overhead for administrators. Additionally, adding additional SOXBusEntity object types also adds additional load to the security cache engine.

Be aware of shared field groups

When using a field group that is shared amongst other object types, the administrator should be aware that a small change in that field group will have an effect on all the object types using it.

The IBM OpenPages GRC Platform application allows an object type to use multiple field groups. These field groups can also be used by other object types.

If an administrator adds one or two fields to the shared field group, those one or two fields will now also be associated with the object types that are using it. If one of the other object types is near the dynamic reporting schema SQL limitation of 32,000, it may cause problems regenerating the reporting schema.

Eliminating unused object type relationships

If the business only requires a subset of the available enabled relationships, those unneeded relationships should be disabled.

About this task

When you install the IBM OpenPages GRC Platform solutions, it loads dozens of object types and hundreds of parent-child relationships. Depending on your business needs, your business object model may only use a small subset of the object types and a subset of the parent-child relationships.

Disabling unused object types will prevent any accidental creations of those relationships.

With Oracle databases, one method of analyzing if there are any unused and enabled relationships is to run an SQL script. From the installation media, there are folders that contain SQL scripts. One of the SQL scripts within the folder is: `Analyze-Object-Type-Relations.sql`.

For DB2-specific information, IBM DB2 Knowledge Center (http://www.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.kc.doc/welcome.html).

Procedure

1. Log on to SQL*Plus as the OPENPAGES oracle id.
2. Type the following command to allow the output to occur: `SET SERVEROUTPUT ON;`.
3. Type the following to spool the contents to a log: `SPOOL AnalyzeRelationships.txt;`.
4. Run the script by typing `@Analyze-Object-Type-Relations.sql`.
5. Run the following to stop the spooling of the log: `SPOOL OFF;` .
   The log file will identify any relationships that are enabled in the system but there are no instances of data utilizing those relationships.

Displaying reporting fragments only on demand

These reporting fragments can be displayed automatically when an end user views the page or on-demand when a user explicitly would like to see the reporting fragment. Set reporting fragments to display only on demand to improve performance of the Cognos server and database instance.

About this task

A reporting fragment is a metadata type that is configured with the administrative screens. It allows an administrator to display Cognos objects within the context of an IBM OpenPages GRC Platform object. Cognos objects can be anything from a simple list to a graph object. Where fragments are unlikely to be necessary, set reporting fragments to display On Demand.

By setting reporting fragments to display on-demand, it reduces excessive calls to the Cognos reporting server. Depending on how complex the design of the reporting fragment is, this can greatly reduce overhead to the Cognos server and to the database instance.

Procedure

1. Open a supported browser.
2. Go to the OpenPages GRC Platform URL.
3. Log in with an administrator ID.
4. On the navigation menu bar, click **Administration** > **Profiles**.
5. Click a profile.
6. In the **Object Types** section, click the name of the object type using the display.
7. In the **Object Fields** table for the selected object type, click the name of the reporting fragment to open its details page.
8. In the **Object Field Information** section, click **Edit**.
9. Update the **Display Type** dropdown.

Displaying Cognos reports on home page tabs

IBM OpenPages GRC Platform administrators can configure Cognos reports to display on the home page tabs instead of on the My Work home page.

About this task

OpenPages GRC Platform administrators can configure the My Work home page to display reports on-demand, configure the My Work home page to display a list of reports, and have users click on tabs to run reports on request.

When the administrator configures the home page to display reports on the tabbed home page, the reports run only when the user specifically wants to view the report. This configuration reduces excessive load and traffic to the IBM Cognos reporting server. When reports are configured to run on demand on the My Work home page, OpenPages GRC Platform users might not even use the data returned from the

report. At times, if the My Work home page is configured to display multiple Cognos reports on demand, the portlets might not display properly, forcing users to refresh the home page.

Procedure

1. Open a supported browser.
2. Go to the OpenPages GRC Platform URL.
3. Log in with an administrator ID.
4. On the navigation menu bar, click **Administration** > **Profiles**.
5. Click a profile.
6. Use the **Home Page Tab Configuration** section to display reports on various tabs or the **My Work Tab Configuration** area to display reports on the My Work home page.

Setting a minimal starting group for display types

IBM OpenPages GRC Platform administrators can change the starting groups for display types to minimize the number of users that are initially displayed.

About this task

OpenPages GRC Platform profiles have various configurable display types. Display types, including user selector, multiple user selector, user dropdown, user/group selector, multiple user/group selector, group selector, and multiple group selector can be minimized. Select a starting group that minimizes the amount of users and/or groups returned by the display type but still has the appropriate business value. By minimizing the starting group, you reduce the number of users that the end user has to search through.

Procedure

1. Open a supported browser.
2. Go to the OpenPages GRC Platform URL.
3. Log in with an administrator ID.
4. On the navigation menu bar, click **Administration** > **Profiles**.
5. Click a profile.
6. In the **Object Types** section, click the name of the object type using the display.
7. In the **Object Fields** table for the selected object type, click the name of the field using one of the display types to open its details page.
8. In the **Display Type Information** section, click **Edit**.
9. Update the **Starting Group** value.

Task-oriented hyperlinking

You can add hyperlinks that are directly oriented to user tasks, from internal or external locations to IBM OpenPages GRC Platform views. These hyperlinks can also include filters.

For example, in a notification email to a risk owner, you can include a hyperlink to the Filtered List View for Risks with the **Risks Awaiting Assessment** filter added to the link.

You can create hyperlinks that include the following target views:

- The Detail View for a specific object instance, in read-only mode.
- A specific activity view for an object instance.
- The Filtered List View for a specific object type with a public filter applied.
- A specific grid view for an object type with a public filter applied.

- Add New wizard within the OpenPages application. The wizard opens in its own browser tab instead of a pop-up, even if the user was logged in to OpenPages when they clicked the link.

You can add hyperlinks to the following locations:

- OpenPages Reports.
- Notification emails.
- OpenPages Java Server Page (.jsp) file type helper applications.
- Within the OpenPages application, using computed fields or URL link fields.

The following sample URLs can help you create task-oriented hyperlinks:

- In the samples the URLs are created by using either the name value, or the resource ID value for views, objects, and filters.
- If you use a name for a value, replace any spaces in the name with the characters %20. URLs cannot contain spaces.
- If you use a fileId, viewId, or filterId to create a URL, the values for the Ids are the resource IDs of specific object instances, views, or filters.
- There is one Filtered List View, but many possible Grid Views. There is one Detail View, but many possible Activity Views.
- For the Add New wizard hyperlinks you can combine the parameters in more ways than are described in the samples. For example, you can specify a parent without specifying a view.

To Filtered List View with the object type, grid view, and filter specified

Syntax:

/openpages/app/jspview/flv?prmt=*<name of the object type>*&view=*<name of the grid view>*&filter=*<name of the public filter>*

Example:

/openpages/app/jspview/flv?prmt=SOXProcess&view=PRSA%20Update&filter=My%20Processes

To Filtered List View with the object type, Filtered List View, and filter specified

Syntax:

/openpages/app/jspview/flv?prmt=*<name of the object type>*&view=Filtered%20List&filter=*<name of the public filter>*

Example:

/openpages/app/jspview/flv?prmt=SOXProcess &view=Filtered%20List&filter=My%20Processes

To Filtered List View or Grid View with the object type, view, and filter specified

Syntax:

In this example, the values are resource IDs instead of names.

Example:

/openpages/app/jspview/flv?prmtId=97&viewId=205&filterId=101

To Filtered List View with the object type and view specified (previous filter is applied)

Syntax:

When a filter is not specified, the most recent, previously used filter is applied. The view, and filter parameters are optional.

Examples:

/openpages/app/jspview/flv?prmt=SOXProcess&view=PRSA%20Update

/openpages/app/jspview/flv?prmtId=97&viewId=205

To Filtered List View or Grid View, object type specified (previous view and filter are applied)

Example:

/openpages/app/jspview/flv?prmt=SOXProcess

To Detail View or Activity View

Syntax:

In the following examples, the fileId value is expressed by using the *<resource ID for the specific object instance>*, while the view value is expressed by using either the view ID, or the *<name of the view>*.

/openpages/view.resource.do?fileId=*<resource ID for the specific object instance>*&view=*<name of the view, which can be Detail, OR the name of one of the specific activity views>*

Examples:

/openpages/view.resource.do?fileId=1903&view=Control%20Assessment

/openpages/view.resource.do?fileId=1903&view=Detail

/openpages/view.resource.do?fileId=1903&viewId=20

To Add New wizard with only the object type specified

Syntax:

/openpages/app/jspview/addNew?objectType=*<name of object type>*

or

/openpages/app/jspview/addNew?objectTypeId=*<id of object type>*

Examples:

/openpages/app/jspview/addNew?objectType=SOXControl

/openpages/app/jspview/addNew?objectTypeId=40

Object type or object type ID is required in a URL that opens the Add New wizard. It is likely that you would use object type ID only if the URL is generated and the object type id is conveniently available.

To Add New wizard with object type and view specified

Syntax:

/openpages/app/jspview/addNew?objectType=*<name of the object type>*&viewName=*<name of the view>*

Example:

/openpages/app/jspview/addNew?objectType=SOXControl&viewName=ShortViewForControl

or

/openpages/app/jspview/addNew?objectType=SOXControl&viewId=3247

View name or ID is optional. If you provide it, it determines the layout of the Add New wizard. You can choose any Creation view or Object View. If you use an Object view with multiple levels of objects, any non-direct children on the second level and all descendants on the third level is ignored. Direct children are used to populate an Associate page in the wizard to enable the associating of children at the same time the object is created.

If no view is specified or the specified view is invalid or disabled, the default Creation view is used. If there is more than one Creation view, the user is prompted to select one.

If there are no Creation views, the Detail view is used.

If the Detail view is disabled or does not exist, the default Object view is used.

For more information about creation views see "Creation views" on page 241.

To Add New wizard with object type, view, and parent object type specified

Syntax:

/openpages/app/jspview/addNew?objectType=*<name of the object type>*&viewName=*<name of the view>*&parentObjType=*<name of the parent object type>*

or

/openpages/app/jspview/addNew?objectType= *<name of the object type>*&viewName=*<name of the view>*&parentObjTypeId=*<id of the parent object type>*

Example:

/openpages/app/jspview/addNew?
objectType=SOXControl&viewName=ShortViewForControl&parentObjTypeId=11

Parent object type or parent object type ID is optional. If multiple object types are suitable as parents for this object type, the default is the one specified in the setting Applications/GRCM/Add New Wizard/Parent Object Type Preferences. If the specified parent object type is invalid, it is ignored.

It is likely that you would use parent type ID only if the URL is generated and the object type id is conveniently available.

To Add New wizard with object type, view, and parent specified

Syntax:

/openpages/app/jspview/addNew?objectType=*<name of the object type>*&viewName=*<name of the view>*&parentObjType=*<name of the parent object type>*&parentObjId=*<id of the parent object >*

Example:

/openpages/app/jspview/addNew?
objectType=SOXControl&viewName=ShortViewForControl&parentObjType=SOXRisk&parentObjId=1234

Parent object ID is optional. Use this parameter to pre-select the parent on the Parents page of the wizard. If specified, the parent object type is required. If you are not creating the URL programmatically, you can find the parentObjId by navigating to the object in the Detail page and using the prmId parameter. If the specified parent object is invalid, it is ignored.

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.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, 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 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.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

Copyright

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 and ibm.com 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 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

In this glossary, you can find terms and definitions for IBM OpenPages GRC Platform

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 beginning 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.

audit universe
The aggregate of all areas within an organization that can be audited.

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. 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

Q

R

S

T

U

V

W

X

Z