HP Release Control

for the Windows® operating systems

Software Version: 4.12

Configuration Guide

Document Release Date: June 2009
Software Release Date: June 2009

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Trademark Notices

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Java™ is a US trademark of Sun Microsystems, Inc.

Adobe® is a trademark of Adobe Systems Incorporated.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign-in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support web site at:

http://www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Table of Contents

Welcome to This Guide

Welcome to the *HP Release Control Configuration Guide*, which explains how to install and configure HP Release Control software. HP Release Control provides a common platform of decision support for Change Advisory Board members and implementation teams during the release life cycle.
HP Release Control analyzes each change request in the system and provides real-time information and alerts during implementation. In addition, HP Release Control enables collaboration, feedback, and review throughout the release life cycle.

This chapter includes:

How This Guide Is Organized

This guide contains the following parts:

Part I Getting Started

Provides an overview of HP Release Control and its configuration.

Part II Setting Up Your Environment

Describes how to set up your environment before starting to configure HP Release Control. It provides detailed instructions on how to configure change request field settings, Universal CMDB-related settings, general server settings, and business CIs.

Part III Configuring Analysis of Change Requests

Describes configuration of processes related to the analysis of converted change requests, including impact analysis, risk analysis, collision calculations, analysis of similar changes. Also describes how to define time periods when changes may and may not be implemented.

Part IV Configuring Collaboration and Review Settings

Describes configuration of collaboration settings, including automatic creation of action items, and latent and detected change settings. It also describes configuration of review and post review settings, including updating the service desk with an approval status and post implementation review data, and sending email notifications.

Part V User Management

Describes configuration of user settings and user authentication.

Part VI System Preferences

Describes configuration of system preferences including email format, log file properties, calendar settings, Dashboard settings, enumeration field display settings, localization settings, and alert settings.

Part VII Special Integration with Other Products

Describes configuration of integration options when HP Release Control is integrated with other products.

Part VIII Appendices

Contains appendices describing password encryption, GMT time zones, preconfigured change request fields, log files, database configuration and maintenance, and HP Release Control utilities.

Who Should Read This Guide

This guide is intended for the HP service engineers who are responsible for configuring HP Release Control. The sections that describe how to configure various elements of the HP Release Control application are written for the application administrator. Regular users of HP Release Control—that is, those involved in the change process, members of the Change Advisory Board (CAB), NOC users, and change implementors—should refer to the *HP Release Control User Guide*.

HP Release Control Documentation

HP Release Control comes with the following documentation:

HP Release Control Deployment Guide explains how to install and deploy HP Release Control. This guide is accessible in the following formats, from the following locations:

- in PDF format on the HP Release Control DVD
- in PDF format by selecting **Help** > **HP Release Control Documentation Library** from the HP Release Control application

HP Release Control Configuration Guide explains how to configure the various parts of the HP Release Control system. This guide is accessible in the following formats, from the following locations:

- in PDF format on the HP Release Control DVD

- in both PDF format and online HTML help format by selecting **Help** > **HP Release Control Documentation Library** from the HP Release Control application
- in HTML help format, from specific HP Release Control application windows, by clicking in the window and pressing F1, or by selecting **Help** from the main menu

HP Release Control User Guide explains how to use the HP Release Control application. This guide is accessible in the following formats, from the following locations:

- in PDF format on the HP Release Control DVD
- in both PDF format and online HTML help format by selecting **Help** > **HP Release Control Documentation Library** from the HP Release Control application
- in HTML help format, from specific HP Release Control application windows, by clicking in the window and pressing F1, or by selecting **Help** from the main menu

HP Release Control API Reference explains how to work with HP Release Control's API. The API Reference is available in CHM format on the HP Release Control DVD, or from the HP Release Control application by selecting **Help** > **HP Release Control Documentation Library**.

HP Release Control Readme provides information on what's new in the current version of the product as well as comprehensive information on known problems and limitations. The Readme is available in HTML format on the HP Release Control DVD, or from the HP Release Control application by selecting **Help** > **HP Release Control Documentation Library**.

Note: Anything published in PDF format can be read and printed using Adobe Reader, which can be downloaded from the Adobe Web site (http://www.adobe.com).

Additional Online Resources

HP Software Support accesses the HP Software Support Web site. This site enables you to browse the Self-solve knowledge base. You can also post to and search user discussion forums, submit support requests, download patches and updated documentation, and more. Choose **Help** > **HP Software Support**. The URL for this Web site is www.hp.com/go/hpsoftwaresupport.

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

To register for an HP Passport user ID, go to:

http://h20229.www2.hp.com/passport-registration.html

HP Software Web site accesses the HP Software Web site. This site provides you with the most up-to-date information on HP Software products. This includes new software releases, seminars and trade shows, customer support, and more. Choose **Help** > **HP Software Web site**. The URL for this Web site is www.hp.com/go/software.

Part I

Getting Started

1

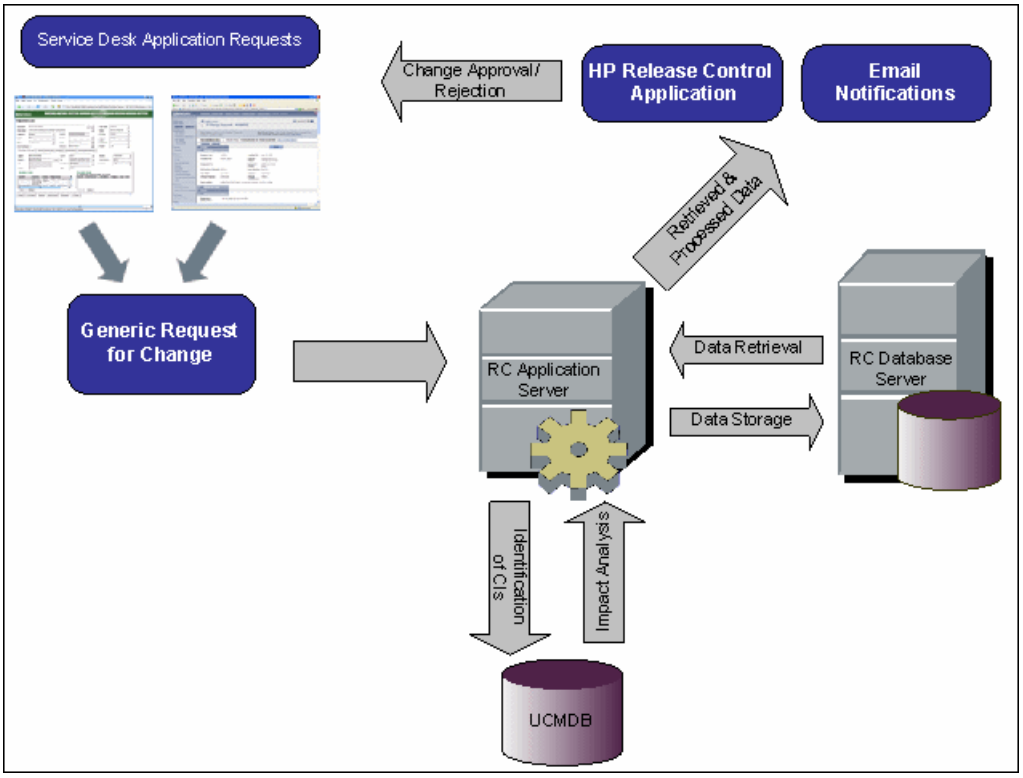
Configuration Overview

This chapter provides an overview of the HP Release Control configuration process.

This chapter includes:

HP Release Control Data Flow

The following diagram illustrates the data flow when running HP Release Control:

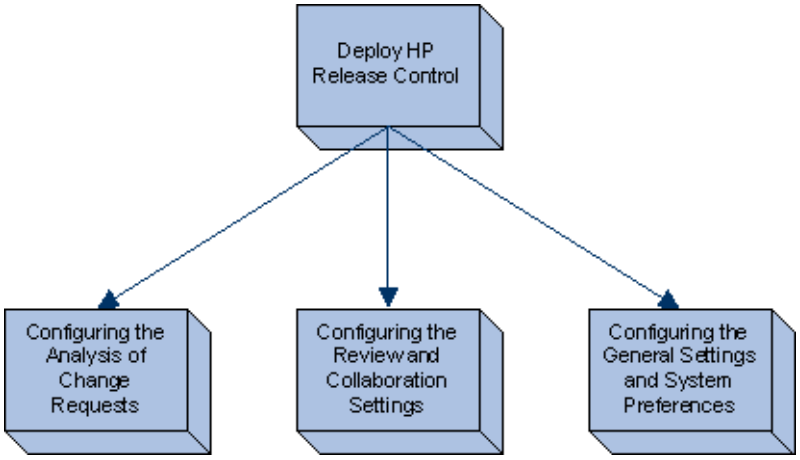


- Change requests originate in the Service Desk Application and are converted into generic requests.
- HP Release Control takes the requests and sends them to HP Universal CMDB to analyze the request and determine the relationships between configuration items (CIs).
- HP Release Control takes the data from HP Universal CMDB and performs impact analysis.
- HP Release Control further analyzes change requests, performing calculations such as risk and collision analysis.

- The information is stored on the RC Database Server.
- Email notifications are sent according to configuration settings to decision makers and changes are approved or rejected.

The Configuration Process: Basic Overview

The following diagram illustrates the major steps involved in the HP Release Control configuration process:



Deploying HP Release Control

For information about installing and deploying HP Release Control, refer to the *HP Release Control Deployment Guide*.

Configuring the Analysis of Change Requests

This section includes the steps to configure the analysis of change requests in HP Release Control.

1 Perform the initial configuration.

The initial configuration consists of configuring the calculation of certain pre- and post-change request processing factors. You can also configure how often change requests will be collected.

For more details, see "Before Configuring Change Request Analysis" on page 105.

2 Analyze the collected requests.

To analyze the collected requests, HP Release Control must identify the location and format of the CIs contained in the requests, using specific analysis rules. For details on configuring the analysis rules you want HP Release Control to use, see "Configuring Analysis Rules" on page 110.

3 Calculate impact analysis for the requests.

HP Release Control calculates the impact of the CIs identified in the collected requests according to a calculation rule that you configure. For details on configuring a calculation rule that determines the point or points at which an impact analysis is performed, see "Determining When to Calculate Impact Analysis" on page 107.

4 Determine the time period categories that your system should include and the rules that should apply to each category.

HP Release Control calculates the compliance of change requests with the rules pertaining to the time period categories in which the requests fit. You must determine the Change Window and Blackout time periods for each category of changes, as well as the criteria by which HP Release Control determines whether a change request is included in a defined time period category. For more details, see "Configuring Time Periods" on page 117.

5 Configure the collision calculation settings.

HP Release Control identifies and calculates collisions between requests according to properties that you define, for the requests that you instruct HP Release Control to include in the collision calculation. For details on configuring HP Release Control's collision calculations, see "Configuring Collision Calculations" on page 127.

6 Calculate risk analysis for the requests.

HP Release Control calculates the risk involved in the implementation of each request based on risk factors that you define and the risk calculation properties that you configure. For details on defining risk factors and configuring risk calculation properties, see "Configuring Risk Analysis" on page 141.

7 Configure similar changes.

HP Release Control automatically identifies and compares elements which are common to all change requests, and generates a list of existing changes which are found to be similar to any proposed change request. By comparing a proposed change against this list of similar changes, you can make use of historical data to gain insight into the nature of the proposed change, and therefore better predict its likely outcome. For more details about configuring similar changes, see "Configuring Similar Changes Analysis" on page 153.

8 Configure KPI Viewing.

If HP Release Control is integrated with HP Business Availability Center 8.x, you can view Key Performance Indicators (KPIs) for the CIs impacted by the selected activity. To enable KPI viewing in HP Release Control, the KPIs need to be configured as federated in HP Business Availability Center. For more details , see "Configuring KPI Viewing" on page 157.

Configuring the Review and Collaboration Settings

This section includes the steps to configure the review and collaboration settings in HP Release Control.

1 **Determine the conditions for which action items should be automatically created.**

By default, HP Release Control automatically creates action items for change requests with a status of **Pending Approval** whose impact severity was equal to or greater than **Low** and whose calculated risk value was greater than **0**. The action items are assigned to the users associated with the business CIs affected by the change requests. For more details, see "Configuring the Automatic Creation of Action Items" on page 161.

2 **Configure the Change Request Approval/Retraction operation.**

HP Release Control contains a feature that allows users to approve and, if necessary, retract the approval of, change requests. For details on configuring this operation, see "Updating Service Desk Data from HP Release Control" on page 163.

3 **Configuring email notifications.**

You can configure HP Release Control to send notifications to users who are associated with certain affected business CIs. For details on formatting the notification content and configuring the circumstances under which HP Release Control sends notifications, see "Configuring Notifications" on page 177.

4 **Configuring the Post Implementation Review (PIR) feature.**

The Post Implementation Review (PIR) feature allows the Change Reviewer to add review notes to any change request with **Evaluation and Closure** status. The review notes present the conclusions regarding the request and provide information about its overall success and satisfaction levels of relevant parties.

Configuring General Settings and System Preferences

This section includes the steps to configure the general settings and system preferences in HP Release Control.

1 Configure the general settings.

Set up the SNMP mail server and the HP Release Control server. For more details, see "Configuring General Settings" on page 79.

2 Configure the business settings.

You can associate users with Business CIs, and configure the business CI details which are displayed in the UI. For details on configuring this operation, see "Configuring Business CI Settings" on page 81.

3 Configure the user settings.

Configure the user settings such as user names, passwords, and user authentication. For more details, see "Configuring User Settings" on page 195 and "User Authentication" on page 203.

4 Configure the system preferences.

Configure the system preferences such as email formats, log file properties, calendar settings, and dashboard settings. For more details see "Configuring System Preferences" on page 219.

Part II

Setting Up Your Environment

2

Configuring Change Request Field Settings

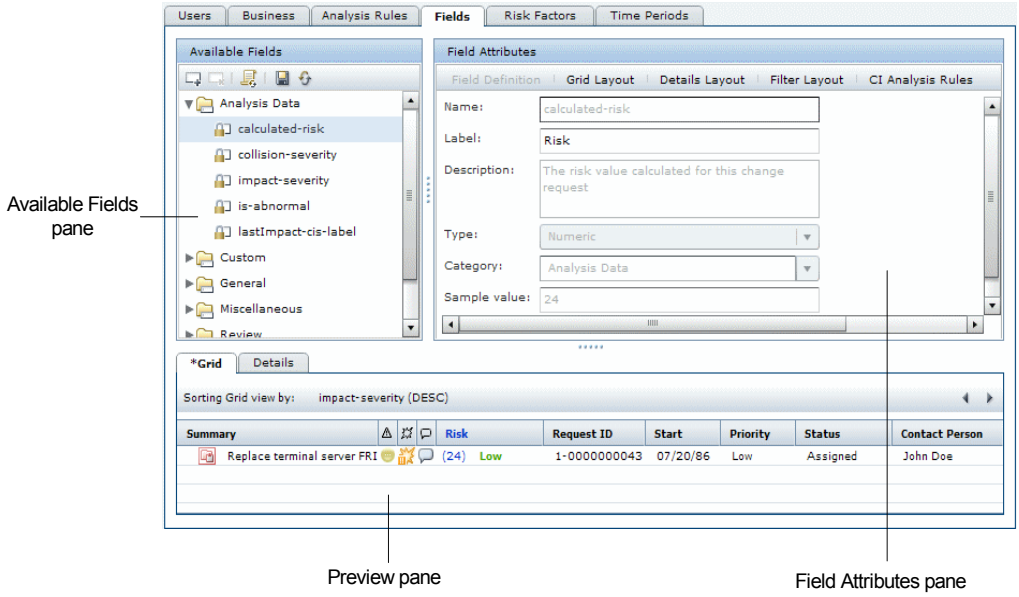
This chapter describes how to configure change request fields for which you want to view data in the HP Release Control application.

Note: For a list of preconfigured change request fields included in HP Release Control, see Appendix C, "Preconfigured Change Request Fields."

This chapter includes:

Understanding the Fields Tab

In the Administration module's Fields tab, you configure change request fields for which you want to view data in the HP Release Control application. You can define the properties of each field and the way in which the field appears in your application.



The Fields tab is divided into the following three sections:

- **Available Fields pane**. Contains a list of all the change request fields. A field selected in the Available Fields pane can be modified in the Field Attributes pane. For filtering purposes, fields are organized into five default categories: **Analysis Data**, **General**, **Miscellaneous**, **Review**, and **Time**. Fields defined as filterable will appear in the Filter Dialog Box, under the category that is defined here in the Available Fields pane. You can create new categories when you create a new field or modify an existing custom field.
- **Field Attributes pane.** You define or modify the properties of the selected change request field in the Field Attributes pane. This pane is divided into the following tabs: **Field Definition**, **List Layout**, **Details Layout**, **Filter Layout**, and **CI Analysis Rules**.

➤ **Preview pane.** In the Preview pane, you can see a preview of the selected field as it will appear in the Analysis module's List view and Preview > Details tab. You can also customize the general layout of the List view and the Preview > Details tab as they appear in the Analysis module.

Creating or Modifying Change Request Fields

You create new change request fields and modify existing ones in the Administration module's Fields tab.

To create or modify change request fields:

1 Click the **Add Field** button to create a new field, or select an existing field that you want to modify.

There are two types of change request fields that appear in the Available Fields pane:

➤ **Predefined fields.** Fields based on ITIL standards, which are common to most service desk applications. Some of these fields are integral to the proper functioning of the HP Release Control application and you therefore cannot remove predefined fields or change their basic properties. The only aspect of these fields that is customizable is the way in which they appear in your application.

➤ **Custom fields**. Fields that are recommended for use in order to optimize HP Release Control analysis features, or any new fields added by users. These fields can be changed or deleted.

Note: The data for these fields can originate from the service desk or from HP Release Control.

---

2 In the **Field Definition** tab, define or modify basic properties of the field.

Note: You cannot change the name or type of an existing field. Instead, you can delete the existing field, save your settings, and then recreate a new field, with a different name, based on the same properties.

You can define the following properties:

Property	Description
Name	The name used to define the field for various configuration purposes. This is not the name that appears in the application. If you are defining a customized field, the name should be unique and in the format **[a-zA-Z][a-zA-Z0-9-]***. The name is not case-sensitive. Once a new field has been saved, its name cannot be modified. Note that when you define a customized field (except for fields of type **Long Text**), a new column is added to the HP Release Control database for this field. Data for **Long Text** fields is stored in a different table.
Label	The text to appear in each location in which the field appears. By default, the value entered here appears in the List Layout tab's **Header** box, in the Details Layout tab's **Label** box, and in the Filter Layout tab's **Label** box. You can modify the value in each of these boxes.
Description	A short description of the field that serves to remind administrators about the usage of the field. The field's description does not appear anywhere in the application.

Property	Description
Type	The field's value type. The following value types are available: ➤ **Short Text.** The request field's value is a simple text string, up to 64 characters. ➤ **Long Text.** The request field's value is a simple text string with an unlimited number of characters. Note that fields of this type cannot be displayed in the List view and you cannot sort or filter according to this field. ➤ **Boolean.** The request field's value is Boolean (true/false; yes/no; 1/0). ➤ **Date.** The request field's value is a date. ➤ **Numeric.** The request field's value is a numeric string.
Category	The filter category in which the customized field is to be included. To create a new category, type a unique category name in the **Category** box. The category name is not case-sensitive. The new category is automatically added in the Available Fields pane. **Note:** You cannot include a customized field in the **Business** or **Union Filters** filter categories.
Sample value	Enables HP Release Control to display a preview of the field, with the sample value, in the Preview pane's **List** tab and/or **Details** tab. Note that you will see a preview only if you configure the field to be displayed in the Analysis module's List view and/or Preview > Details tab (in the List Layout or Details Layout tabs).
Listable (not editable)	Indicates whether the selected field is of a type that can be displayed in the Analysis module's List view. This check box is not editable.
Sortable	Indicates whether HP Release Control can sort according to the selected field. The only fields that can be made sortable are those that can be displayed in the Analysis module's List view. If a field cannot be displayed in the List view, the **Sortable** option is disabled.
Filterable	Indicates whether the field is to be used as one of the filter criteria. In the **Filter Layout** tab, you define the way in which the field should appear in the Filter dialog box.

3 If the **Listable** check box in the Field Definition tab is selected, click the **List Layout** tab to define the way in which the field will appear in the Analysis module's List view. You can define the following properties:

Property	Description
Header	The text to appear in the header of the column in which the change request field value is to be displayed.
Header tooltip	The text of the tooltip that will appear when you hold your cursor on the column header. If this element is left unspecified, the name of the header is displayed as the tooltip.
Value display type	The display type of the value in the list view. The display options that are available depend on the field type you defined in the Field Definition tab. The following display types are available: ➤ **Short Text.** The value is displayed as simple text. ➤ **Boolean.** The value is displayed as a check box (supports true/false, yes/no, and 1/0). ➤ **Date.** The value is displayed as a date. You customize the way the value appears in the **Value display format** box.
Value display format	The format in which the field will appear. For information about valid formats for each value display type, see "Valid Display Formats" on page 40. **Note:** You cannot define a value display format for Boolean value display types.
Tooltip display type	The display type of the tooltip describing the selected field. The display options that are available depend on the field type you defined in the Field Definition tab. The following display types are available: ➤ **Short Text.** The value is displayed as simple text. ➤ **Date.** The value is displayed as a date. You can use the value tooltip to describe the information that appears in the List view in a different way. You use the **Tooltip display format** box, described below, to customize the way in which the tooltip display type appears.

Property	Description
Tooltip display format	The text and format of the tooltip that will appear when you hold your cursor over the field value. For information about valid formats for each value type, see "Valid Display Formats" on page 40.
Resizable	Indicates whether the column width is adjustable. For more information about resizing columns, see "Customizing the List View" on page 42.
Show in List view	Indicates whether the field should be displayed in the Analysis module's List view. **Note:** If you select **Show in List view**, the Preview pane displays a preview of the way in which the field will appear in List view. To see how a sample value is displayed, type a sample value in the Field Definition tab's **Sample value** box.

4 Click the **Details Layout** tab to define the way in which the field will appear in the Analysis module's Preview > Details tab. You can define the following properties:

Property	Description
Label	The text to appear as the label preceding the displayed field value in the Preview > Details tab.

Property	Description
Value display type	The display type of the field value in the Preview > Details tab. The display options that are available depend on the field type you defined in the Field Definition tab. The following display types are available: ➤ **Short Text.** The value is displayed as simple text, adjacent to the label. ➤ **Long Text.** The value is displayed as simple text, underneath the label. Where necessary, the text will wrap. ➤ **Boolean.** The value is displayed as a check box (supports true/false, yes/no, and 1/0). ➤ **Date.** The value is displayed as a date. ➤ **Link.** The value of the current field is displayed as a link. The link leads to a different field, which contains a URL. You customize the way the value appears in the **Value display format** box.
Value display format	The format in which the field will appear. For information about valid formats for each value display type, see "Valid Display Formats" on page 40. **Note:** You cannot define a value display format for Boolean or Long Text value display types.
Tooltip	The text of the tooltip that will appear when you hold your cursor over the label.
Show in Details tab	Indicates whether the field should be displayed in the Analysis module's Preview > Details tab. **Note:** If you select **Show in Details tab**, the Preview pane displays a preview of the way in which the field will appear in the Preview > Details tab. To see how a sample value is displayed, type a sample value in the Field Definition tab's **Sample value** box.

5 If the **Filterable** check box in the Field Definition tab is selected, click the **Filter Layout** tab to define the way in which the field will appear in the Filter dialog Box. You can define the following properties:

Property	Description
Label	The text to appear as the label preceding the displayed field value in the Filter Dialog Box.
Tooltip	The text of the tooltip that will appear when you hold your cursor over the label.
Value display type	Determines the way in which the selected field will operate as a filter. The display options that are available depend on the field type you defined in the Field Definition tab. The following possible options exist: ➤ **Numeric.** Users can filter by specific numbers. ➤ **Numeric Range.** Users can filter by a numeric range. If you select this option, you need to specify the range in the relevant boxes below the **Value display type** list. ➤ **Date.** Users can filter by date. The option to filter fields of type **date** is only available in the Analysis module. ➤ **Boolean.** Users can filter by boolean value. You assign a label to each boolean value in the '**True**' **Label** and '**False**' **Label** boxes below the **Value display type** list. These are the labels that will appear in the Filter Dialog Box. ➤ **Short Text.** Users enter a string that matches the filter value. An asterisk (*****) can be used to match a string to several possible values. (For example, if you use the string Da*, both David and Danny will match.) ➤ **Single Selection.** Users can select only one filter value option from a drop-down list box. ➤ **Multi Selection.** Users can select multiple filter value options from a drop-down list box. ➤ **Editable Selection.** Users can either select filter value options from a drop-down list box or enter a string that matches the filter value.

Property	Description
Value display type (cont'd)	If you select **Single Selection**, **Multi Selection**, or **Editable Selection** from the **Value display type** list, choose one of the following two options: ➤ **Define possible values.** Enables you define the values you want the drop-down list box to contain, as well as the way in which you want each value to be displayed. For information on defining values, see the instructions below. ➤ **Get existing values.** Instructs HP Release Control to get the values to be displayed in the drop-down list box directly from the database. If you select **Define possible values**, you must define the filter value options you want the drop-down list box to contain. **To add a filter value option:** **1** Click the **Add Filter Value** button  . **2** In the boxes below the table, enter the value of the option in the **Value** column and the way in which you want the value to be displayed in the **Display** column. **3** To change the order in which the filter values will appear in the drop-down list box, select the relevant filter value and click the **Move Up** or **Move Down** button  . **To delete an option:** ➤ Select the option and click the **Delete Filter Value** button  .
Show in Analysis Filter	Indicates whether the field will appear as one of the filter criteria in the Analysis module.
Show in Director Filter	Indicates whether the field will appear as one of the filter criteria in the Director module.

6 To apply analysis rules to the change request field, click the **CI Analysis Rules** tab. These are the rules according to which you want HP Release Control to identify the location and format of CIs contained in the field's text.

You can apply analysis rules to change request fields of type **Short Text** or **Long Text**. We recommend that you apply analysis rules to change request fields that contain CIs only, without additional text comments.

For information about how to apply analysis rules to the change request fields, see "Applying Analysis Rules to Fields" on page 112.

7 Ensure that you are satisfied with your Fields tab settings. Before you save your settings, you can undo any changes you made by clicking the  **Refresh and Undo Modifications** button in the Available Fields pane. This restores the fields to their most recently saved settings.

To save your changes and commit these changes to the server, click the  **Save Settings for All Fields** button in the Available Fields pane. A message opens asking you to confirm that you want to save these changes. Once you save these changes, they cannot be undone. Click **Yes** to save the changes.

The save process can take a few minutes, during which time users cannot log in to HP Release Control. Once the changes have been saved, users logging in to HP Release Control will view the new changes.

If any field is invalid, you cannot save your changes. When you try save your changes, you receive an error message informing you to fix the  invalid fields. If a field is invalid, an icon is displayed in the Available fields pane next to the invalid field and the relevant category.

Note: After you have updated your adapter conversion scripts with the new fields that you created or modified, you can apply these updates to  your adapter by clicking the **Reload Adapters** button.

Valid Display Formats

In the Fields tab, there are a number of places where you must define the format in which a specific field will appear. For each display type, a different display format applies. The following table describes valid formats for each display type:

Display Type	Display Format
Short Text	If you selected **Short Text** as the display type, you can include parameters that contain the names of defined fields. Each field must contain two percentage signs on either side of it. For example, if you defined your display format as **Please contact %%contact-person%%**, the parameter **%%contact-person%%** would return the name of the contact person for the request (from the **contact-person** field). If you leave the format box empty, the value of the field will be displayed as is.
Date	If you selected **Date** as your display type, you can specify the way in which the date should be displayed by making use of letter patterns containing the following letters: ➤ **Y.** Year ➤ **M.** Month ➤ **D.** Day in the month ➤ **E.** Day of the week ➤ **A.** AM/PM indicator ➤ **J.** Hour of the day (0-23) ➤ **H.** Hour of the day (1-24) ➤ **K.** Hour in the AM/PM (0-11) ➤ **L.** Hour in the AM/PM (1-12) ➤ **N.** Minute in the hour ➤ **S.** Second in the minute For example, to display **Sat 04 Mar 2006 09:43AM**, you would use the following date format: EEE DD MMM YYYY LL:NNA

Display Type	Display Format
Link	If you selected **Link** as your display type, you must specify the name of a field that contains a URL. You enter the field as a parameter that contains the name of the field, surrounded by two percentage signs on each side of the field (**%%field_name%%)**. The value displayed for this format is the value of the current field (not the field that contains the URL) and the tooltip of this value is the URL. Clicking on the field leads you to the URL destination.

Note: You cannot define a display format for **Boolean** or **Long Text** display types.

Deleting a Change Request Field

You can delete Custom fields that are provided by HP Release Control or manually added by the user. However, you cannot delete fields that are being used in risk factor or time period definitions.

Predefined fields, which are integral to the proper functioning of the HP Release Control application, cannot be deleted.

Caution: When you delete a change request field, all data related to the field is removed.

To delete a change request field:

1 In the Administration module's **Fields** tab, select the field that you want to delete.

2 Click the **Delete Field** button in the Available Fields pane. A message opens asking you to confirm that you want to delete this change request field.

3 Click **Yes** to confirm.

Note: The field is only deleted once you save your field setting changes (see step 7 on page 39 for instructions on saving your settings). Before you save your field settings, you can still undo the delete action by clicking the **Refresh and Undo Modifications** button in the Available Fields pane. This restores the fields to their most recently saved settings.

Customizing the List View

In the Administration module's Fields tab, you can customize the layout of the Analysis module's List view.

To customize the List view:

In the Preview pane, select the **List** tab. A preview of the fields for which you selected **Show in List view** (in the List Layout tab) are displayed.

You can customize the following:

- The width of the columns. To adjust the column width, rest the cursor on the column boundary you want to move until it becomes a resize pointer, and then drag the boundary until the column is at the required width. Note that you can adjust the width of the column only if you selected **Resizable** for the selected column in the List Layout tab.
- The order of appearance of the columns. You can move the columns to the left or to the right by selecting the relevant column header and clicking either the **Move Column Right** or **Move Column Left** button.

➤ The column by which the List view should be sorted by default. To sort the List view according to a specific column, click the relevant column heading twice. An arrow is displayed next to the column header to indicate that the List view is sorted by this column. To change the sorting order, click the column heading again. The arrow points in the opposite direction. Note that you can select a column to sort by only if you selected **Sortable** for the column in the List Layout tab.

Customizing the Preview > Details Tab

In the Administration module's Fields tab, you can customize the layout of the Analysis module's Preview > Details tab.

To customize the Preview > Details tab:

In the Preview pane, select the **Details** tab. A preview of the fields for which you selected **Show in Details tab** (in the Details Layout tab) is displayed.

You can perform the following:

➤ **Add or remove columns.**

You can add additional empty columns to be displayed in the Preview > Details tab. To add a new column, click the **Add Column** button. An empty column is added on the right. You can then move different fields to the new column as explained below.

To delete a column, select the relevant column by clicking inside the column—but not on a particular field—until the whole column is highlighted. Click the **Remove Column** button. The fields that were included in this column move over to another column.

➤ **Change the order of appearance of the fields.**

To move the field to a different column, select the relevant field and click the **Move Right** or **Move Left** button.

To move the fields up or down within the columns, select the relevant field and click the **Move Up** or **Move Down** button.

3

Configuring HP Service Manager/Center

This chapter describes advanced configuration options for HP Service Manager/Center.

Caution: For information about configuring HP Service Manager/Center as your service desk, refer to the *HP Release Control Deployment Guide*.

This chapter includes:

Generating Links to HP Service Manager/Center Tickets

From HP Release Control, you can create links to HP Service Manager/Center tickets via the Web tier.

To create links to HP Service Manager/Center tickets from HP Release Control:

1. By default, HP Service Manager/Center server may be configured to require a security hash with Web tier URL queries. In this case, you need to configure your system to allow access to HP Service Manager/Center via URL links.
   - For HP Service Manager, see "Allowing Access to HP Service Manager via URL Links" on page 47.

➤ For HP ServiceCenter, see "Allowing Access to HP ServiceCenter via URL Links" on page 50.

Note: You can also disable this secure query requirement in the Web.xml file (**querySecurity** in HP Service Manager and **sc.querysecurity** in HP ServiceCenter).

---

2 In the HP Release Control Administrator module, click the **Fields** tab.

3 In the **Available Fields** pane, select **Miscellaneous** > **request-id**

4 In the **Field Attributes** pane, in the **Details Layout** tab enter the URL in the **Value display format** field:

➤ If you are using Lightweight Single Sign-On (LW-SSO), for secure or non-secure queries, enter the following URL:

```
http:// <Host:Port>/SymphonyAdapter/
ui?IsmOperation=edit&IsmFromSystem=ReleaseControl&IsmSubject=125&IsmEnti
tyType=Change&IsmToSystem=ChangeManager&IsmProtocolVersion=1.0&IsmEnti
tyID=%%request-id%%
```

➤ For non-secure queries, without using LW-SSO, enter the following URL:

```
<HP Service Manager/Center Web tier address>/index.do?ctx=docEngine
&file=cm3r&query=number="%%request-id%%"
```

For example

```
http://scserver:8080/sc/index.do?ctx=docEngine
&file=cm3r&query=number="%%request-id%%"
```

➤ For secure queries, without using LW-SSO, enter the following URL:

```
%%url%%
```

5 Click **Save**.

Allowing Access to HP Service Manager via URL Links

If a URL security mechanism is in place, the URL query must contain a hash (generated by HP Service Manager) that is dependent on both the HP Service Manager Web server's name and the query. This configuration should be performed by the HP Service Manager administrator.

To generate a secure URL query:

1 In HP Service Manager, add a new change request field named **url**. This field will contain the generated link for the ticket. Set the data type to **character**.

- Add the field to requests using **System Definition** > **Tables** > **cm3r** > **Fields**.
- Add the field to tasks using **System Definition** > **Tables** > **cm3t** > **Fields**.

2 Expose the new fields in the WSDL.

The following procedure should be carried out twice: Once for ChangeRC External Access objects and once for ChangeTaskRC External Access objects.

a Navigate to **WSDL Configuration**.

b In the **Name** box, type the relevant name:

- For **ChangeRC** External Access objects, type cm3r.
- For **ChangeTaskRC** External Access objects, type cm3t.

c Select the External Access object:

- for **ChangeRC** External Access objects, select **ChangeRC**.
- for **ChangeTaskRC** External Access objects, select **ChangeTaskRC**.

d In the **Fields** tab, ensure that the following field with the appropriate properties is included in the list of exposed fields:

Field	Caption	Type
url	Url	

3 Create a **Format Control Calculation** entry that will generate the URL within this field when a change request is created or modified.

The following procedure should be carried out twice: Once for cm3r records and once for cm3t records.

a Select **Tailoring** > **Format Control**.

b In the **Name** box, type the record name:

- for cm3r records, type cm3r.
- for cm3t records, type cm3t.

c Click the **Calculations** button and enter the relevant calculation:

- For cm3r records, enter the following:

add	update	calculation
true	true	$query="number=\""+number in $file+"\"";$title="Change Request Details"; url in $file=jscall("urlCreator.getURLFrom Query", "cm3r", $query, $title)

The values in the **delete**, **display**, and **initial** columns should be empty.

- For cm3t records, enter the following:

add	update	calculation
true	true	$query="number=\""+number in $file+"\"";$title="Task Details"; url in $file=jscall("urlCreator.getURLFrom Query", "cm3t", $query, $title)

The values in the **delete**, **display**, and **initial** columns should be empty.

d Save your modifications to the Format Control table.

4 Check that the exact machine name (**My Computer** > **Properties** > **Computer Name**) is properly defined (case sensitive) in the following places:

- On the HP Service Manager client, select **System Administration** > **Base System Configuration** > **Miscellaneous** > **System Information Record** and click the **Active Integrations** tab. Ensure that the Web server URL is properly defined. (for example, http://smserver:8080/sm/index.do)
- In the Web server's **web.xml** file, ensure that the Web server URL is properly defined under the **serverHost** property. (for example, http://smserver:8080/sm/index.do)

5 Restart the HP Service Manager server.

6 Regenerate the Web Services stub file (**.jar**):

a Run the **ServiceManagerWsdlGen.bat** utility in the <**HP Release Control Installation directory**>**bin** directory.

b From the <**HP Release Control installation directory**>**bin****result** directory, copy the **tomcat** folder and overwrite the existing **tomcat** folder in the HP Release Control installation root directory. When asked whether you want to overwrite certain files, click **Yes to all**.

7 Map the **url** field that you created in HP Service Manager to the **origin-url** field in HP Release Control by editing the conversion scripts for changes and tasks.

For example, in the **servicemanager-ws-adapter.ext/convertChange.js** file and the **servicemanager-ws-adapter.ext/convertTask.js**, depending on your configuration, you could add the following to the convert function:

```
function convert(sm_rfc, generic_rfc) {
        …..
        generic_rfc.setField("origin-url", sm_rfc.get("url"));
         ….
}
```

8 Continue with step 2 on page 46.

Allowing Access to HP ServiceCenter via URL Links

If a URL security mechanism is in place, the URL query must contain a hash (generated by HP ServiceCenter) that is dependent on both the HP ServiceCenter Web server's name and the query. This configuration should be performed by the HP ServiceCenter administrator.

To generate a secure URL query:

1 In HP ServiceCenter, add a new change request field named **url,** linking to the change request itself. Set the data type to **text**.

a Add the field to requests using **System Definition** > **Tables** > **cm3r** > **Fields**.

b Add the field to tasks using **System Definition** > **Tables** > **cm3t** > **Fields**.

2 Expose the new fields in the WSDL.

The following procedure should be carried out twice: Once for ChangeRC External Access objects and once for ChangeTaskRC External Access objects.

a In HP ServiceCenter, select **Menu Navigation** > **Toolkit** > **WSDL Configuration**.

b In the **Name** box, type the relevant name:

- For **ChangeRC** External Access objects, type cm3r.
- For **ChangeTaskRC** External Access objects, type cm3t.

c In the **Data Policy** tab, ensure that the following field with the appropriate properties is included in the list of exposed fields:

Field Name	API Caption	Exclude	API Data Type
url	Url	false	

3 Create a **Format Control Calculation** entry that will generate the URL within this field when a change request is created or modified.

The following procedure should be carried out twice: Once for cm3r records and once for cm3t records.

a Select **Utilities** > **Tools** > **Format Control**.

b In the **Name** box, type the record name:

- for cm3r records, type cm3r.
- for cm3t records, type cm3t.

c Click the **Calculations** button and enter the relevant calculation:

- For cm3r records, enter the following:

add	update	calculation
true	true	$query="number=\""+number in $file+"\"";$title="Change Request Details"; url in $file=jscall("urlCreator.getURLFrom Query", "cm3r", $query, $title)

The values in the **delete**, **display**, and **initial** columns should be empty.

- For cm3t records, enter the following:

add	update	calculation
true	true	$query="number=\""+number in $file+"\"";$title="Task Details"; url in $file=jscall("urlCreator.getURLFrom Query", "cm3t", $query, $title)

The values in the **delete**, **display**, and **initial** columns should be empty.

d Save your modifications to the Format Control table.

4. Check that the exact machine name (**My Computer** > **Properties** > **Computer Name**) is properly defined (case sensitive) in the following places:
   - On the HP ServiceCenter client, select **Utilities** > **Administration** > **Information** > **System Information Record** and click the **Active** tab. Ensure that the Web server URL is properly defined. (for example, http://scserver:8080/sc/index.do)
   - In the Web server's **web.xml** file, ensure that the Web server URL is properly defined under the **sc.host** property. (for example, http://scserver:8080/sc/index.do)
5. Restart the HP ServiceCenter server.
6. Regenerate the Web Services stub file (**.jar**):
   a. Run the **ServiceManagerWsdlGen.bat** utility in the <**HP Release Control Installation directory**>**bin** directory.
   b. From the <**HP Release Control installation directory**>**bin****result** directory, copy the **tomcat** folder and overwrite the existing **tomcat** folder in the HP Release Control installation root directory. When asked whether you want to overwrite certain files, click **Yes to all**.
7. Map the **url** field that you created in HP Service Manager/Center to the **origin-url** field in HP Release Control by editing the conversion scripts for changes and tasks.

   For example, in the **servicecenter-ws-adapter.ext/convertChange.js** file and the **servicecenter-ws-adapter.ext/convertTask.js**, depending on your configuration, you could add the following to the **convert** function:

```
function convert(sc_rfc, generic_rfc) {
        …..
        generic_rfc.setField("origin-url", sc_rfc.get("url"));
         ….
}
```

8. Continue with step 2 on page 46.

Creating External Links to HP Release Control Interfaces

From HP Service Manager/Center, you can create customized links to various user interfaces of HP Release Control, such as the Change Request Calendar. For more information, see "Linking to HP Release Control Interfaces from Other Applications" on page 247.

Troubleshooting HP Service Manager/Center

This section includes information about troubleshooting HP Release Control when working with HP Service Manager/Center.

Problems Saving Post Implementation Review Comments to HP Service Manager

When using HP Service Manager with IIA, the ability to save post implementation review comments from HP Release Control to HP Service Manager may sometimes be disabled. There is no error message or warning informing the user that this feature has been disabled, and from HP Release Control it appears as if the comments are being saved. The only way to detect this is to check HP Service Manager to verify if the comments have been saved. The following procedure is a workaround which will enable you to save the post implementation review comments to HP Service Manager:

1. In the HP Service Manager Client, go to **Menu Navigation** > **Tailoring** > **Database Dictionary.**
2. Type **cm3t** in the **File Name** box and press ENTER.
3. Select the first item in the table at the bottom of the screen and select the **New Field/Key** button.
4. Type **closure.comments** in the **name** box, and type **array** in the **type** box.
5. Press the **Add Field** button.
6. A similar window opens. Enter **character** in the **type** box.
7. Press the **Add Field** button.

4

Configuring HP Universal CMDB-Related Settings

This chapter describes how to configure HP Release Control to work with HP Universal CMDB.

Note: This chapter uses HP Universal CMDB terminology. Objects are referred to as CIs, and CI types as CITs.

This chapter includes:

Overview of Configuring HP Universal CMDB-Related Settings

HP Universal CMDB is a database which contains the CIs, CITs, and their relationships. HP Release Control interacts with HP Universal CMDB in a number of different ways to obtain relevant calculations such as those regarding impact analysis.

- For information about configuration settings that must be configured for HP Universal CMDB to interact with HP Release Control, see the *HP Release Control Deployment Guide*.
- For information about additional recommended settings, see "Recommended Configuration for HP Universal CMDB 7.x" on page 56 or "Recommended Configuration for HP Universal CMDB 8.x" on page 60.
- For information about advanced settings, see "Advanced HP Universal CMDB Configuration" on page 64.

Recommended Configuration for HP Universal CMDB 7.x

This section includes:

Configuring CI Search Directives

When a ticket is received, it is parsed using the analysis rules. These parsed strings are then used to search HP Universal CMDB for valid CIs. As entries are searched in HP Universal CMDB, only specified attributes of each entry are searched. This section configures which attributes are searched for each CIT.

By default, HP Release Control searches for changed CIs that belong to the **host** or **ip** CITs and whose format matches one of the HP Universal CMDB attributes listed in the <**cmdb-lookup-attributes**> section of the **mam-integration.settings** file.

If you want HP Release Control to search for CIs that belong to a different CIT, you must add this CIT and its relevant attributes to the **mam-integration.settings** file. You do this by including an additional <**lookup-directive**> element in the <**cmdb-lookup-attributes**> section of this file, as follows:

```
<lookup-directive>
 <class-type>[class type name]</class-type>
    <attributes>
      <attribute>[attribute name]</attribute>
      <attribute>[attribute name]</attribute>
    </attributes>
</lookup-directive>
```

To specify an additional format by which to locate a CI belonging to a **host** or an **ip** CIT, you must add the relevant attribute to the CIT's <**lookup-directive**>. For example, to locate an **ip** CIT by domain, in addition to locating it by address or DNS name, add <**attribute**>**ip_domain**</**attribute**> to the **ip** CIT <**lookup-directive**>, as follows:

```
<lookup-directive>
 <class-type>ip</class-type>
    <attributes>
      <attribute>ip_address</attribute>
      <attribute>ip_dnsname</attribute>
      <attribute>ip_domain</attribute>
    </attributes>
</lookup-directive>
```

Configuring System-Business CI Relationships

The relationships that exist between CIs are important in calculations such as impact analysis. In order to understand how a change request on one CI will affect other CIs, you must understand which CIs are linked. The links between different system CIs are detected automatically by HP Universal CMDB. However, if there is a relevant connection between a system CI and a business CI, it must be manually defined in HP Universal CMDB. The procedures for defining these relationships differ depending on which version of HP Universal CMDB you are running.

To configure system-business CI relationships in HP Universal CMDB 7.x:

1. Open the HP Universal CMDB View Manager.
2. Within each view definition, locate the nodes (representing hosts or groups of other CIs) that you want to link to a business CI.
3. Right-click each node and select **Add to Applications**.

For more information on linking nodes to business CIs, refer to the HP Universal CMDB documentation.

Converting System CITs to Business CITs

The initial categorization of CITs into business and system CIs is performed by HP Universal CMDB. When importing a CIT from HP Universal CMDB, the category is carried over to HP Release Control. However, you can configure a system CIT in HP Universal CMDB to be imported as a business CIT in HP Release Control.

To import a system CIT as a business CIT:

1. Open HP Universal CMDB.
2. Go to the CIT and add the **ccmBusiness** qualifier.

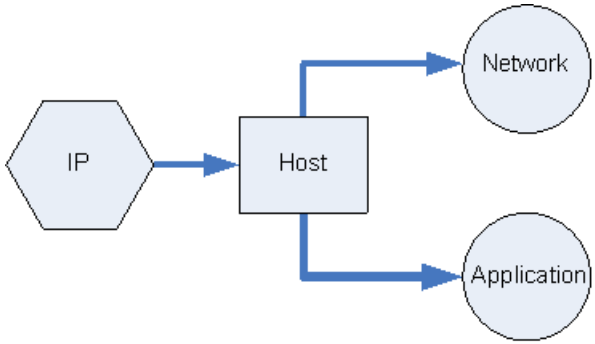
Configuring Correlation Rules

Correlation rules define the relationships between CIs. They are defined in HP Universal CMDB and must be custom-defined to work with HP Release Control. Impact analysis is built on correlation rules.

After correlation rules are defined in HP Universal CMDB, HP Release Control imports selected rules specified by designated prefixes for the purposes of impact analysis.

CIs are related in terms of impact analysis by the direction of impact. This means that with respect to a given CI, other CIs can be labeled as either affected by or affecting that CI. The correlation rules which determine these impact relationships of CIs are defined in the **mam-integration.settings** file's **<impact-correlation-patterns>** section.

By default, only those rules with the prefix **ccm** are imported. This specifies a correlation between CITs of type IP, host, network, and application as follows, where arrows point in the direction of impact:



If you want HP Release Control to use additional or alternative correlation rules, you must define these rules in the <**patterns**> element of the **mam-integration.settings** file's <**impact-correlation-patterns**> section using regular expressions.

For example, if you want to define alternative correlation rules to be used, you can modify the <**patterns**> element using regular expressions as follows:

```
<impact-correlation-patterns>
  <patterns>   operations.*
               database.*
  </patterns>
</impact-correlation-patterns>
```

The above code indicates that any correlation rule found in HP Universal CMDB with the prefix **operations** or **database** will be included in the impact analysis calculations.

Each expression you use should appear on a separate line. For details on working with regular expressions, see http://java.sun.com/j2se/1.4.2/docs/api/java/util/regex/Pattern.html

You can modify the **<patterns>** element without using regular expressions, or using a combination of regular expressions and actual correlation rule names. For example:

```
<patterns>    weblogic
              j2ee
              database.*
</patterns>
```

Triggered CI to Changed CI Correlation Rules

Triggered CIs are those mentioned explicitly on the ticket. Change CIs (CCIs) are CIs which are directly changed as a result of a change request. All Triggered CIs are by definition CCIs. CCIs can be triggered or not triggered. The relationship defining triggered CIs and CCIs is defined by the correlation rules located in the **mam-integration.settings** file's **<directly-affected-correlation-patterns>** section. The **<patterns>** element defines which correlation rules are imported using regular expressions.

Recommended Configuration for HP Universal CMDB 8.x

This section includes:

Configuring CI Search Directives

When a ticket is received, it is parsed using the analysis rules. These parsed strings are then used to search HP Universal CMDB for valid CIs. As entries are searched in HP Universal CMDB, only specified attributes of each entry are searched. This section configures which attributes are searched for each CIT.

By default, HP Release Control searches for changed CIs that belong to the **host** or **ip** CITs and whose format matches one of the HP Universal CMDB attributes listed in the <**cmdb-lookup-attributes**> section of the **mam-integration.settings** file.

If you want HP Release Control to search for CIs that belong to a different CIT, you must add this CIT and its relevant attributes to the **mam-integration.settings** file. You do this by including an additional <**lookup-directive**> element in the <**cmdb-lookup-attributes**> section of this file, as follows:

```
<lookup-directive>
 <class-type>[class type name]</class-type>
    <attributes>
      <attribute>[attribute name]</attribute>
      <attribute>[attribute name]</attribute>
    </attributes>
</lookup-directive>
```

To specify an additional format by which to locate a CI belonging to a **host** or an **ip** CIT, you must add the relevant attribute to the CIT's <**lookup-directive**>. For example, to locate an **ip** CIT by domain, in addition to locating it by address or DNS name, add <**attribute**>**ip_domain**</**attribute**> to the **ip** CIT <**lookup-directive**>, as follows:

```
<lookup-directive>
 <class-type>ip</class-type>
    <attributes>
      <attribute>ip_address</attribute>
      <attribute>ip_dnsname</attribute>
      <attribute>ip_domain</attribute>
    </attributes>
</lookup-directive>
```

Configuring System-Business CI Relationships

The relationships that exist between CIs are important in calculations such as impact analysis. In order to understand how a change request on one CI will affect other CIs, you must understand which CIs are linked. The links between different system CIs are detected automatically by HP Universal CMDB. However, if there is a relevant connection between a system CI and a business CI, it must be manually defined in HP Universal CMDB. The procedures for defining these relationships differ depending on which version of HP Universal CMDB you are running.

To configure system-business CI relationships, model the business CI using the HP Universal CMDB editor. For more information, refer to the HP Universal CMDB documentation.

Converting System CITs to Business CITs

The initial categorization of CITs into business and system CIs is performed by HP Universal CMDB. When importing a CIT from HP Universal CMDB, the category is carried over to HP Release Control. However, you can configure a system CIT in HP Universal CMDB to be imported as a business CIT in HP Release Control.

To import a system CIT as a business CIT:

1. Open HP Universal CMDB.
2. Go to the CIT and select the **MODELING_ENABLED** qualifier.

Configuring Correlation Rules

Correlation rules define the relationships between CIs. They are defined in HP Universal CMDB and can be custom-defined to work with HP Release Control. Impact analysis is built on correlation rules.

CIs are related in terms of impact analysis by the direction of impact. This means that with respect to a given CI, other CIs can be labeled as either affected by or affecting that CI. The correlation rules which determine these impact relationships of CIs are defined in the **mam-integration.settings** file's **<impact-correlation-bundle>** section.

HP Release Control comes with a set of built in correlations. These form a good basis for calculating impact analysis. If you want to increase the accuracy of the impact analysis, you can define more correlation rules.

To define a new correlation rule:

1. In HP Universal CMDB, define a new correlation.
2. Right-click the correlation and select properties.
3. Set the **Correlation Rule Group**s as follows:
   a. **RC_IMPACT.** You must select this option. It indicates that this correlation is relevant to impact in HP Release Control.
   b. **RC_DIRECTLY_AFFECTED.** Select this option only when relevant. It indicates that this correlation defines a direct impact link.

Triggered CI to Changed CI Correlation Rules

Triggered CIs are those mentioned explicitly on the ticket. Change CIs (CCIs) are CIs which are directly changed as a result of a change request. All Triggered CIs are by definition CCIs. CCIs can be triggered or not triggered. The relationship defining triggered CIs and CCIs is defined by the correlation rules located in the **mam-integration.settings** file's **<directly-affected-correlation-bundle>** section. The **<patterns>** element defines which correlation rules are imported using regular expressions.

Advanced HP Universal CMDB Configuration

This section includes:

Configuring CI Attribute Displays

When viewing CI details in HP Release Control, the only attribute that is displayed by default is **name**. To add attributes to this list, they must be added in the **<class-type>** property of each CIT.

You add attributes from the **<HP Release Control installation directory>\conf\mam-integration.settings** file.

To add an attribute, add an **<attributes><attribute-name>[attribute name]</attribute-name></attributes>** property to the **<class-type>** section of the target CIT.

```
<ci-class-attributes>
        <class-type>[name of class type representing the business]</class-type>
        <attributes>
          <attribute-name>[attribute name]</attribute-name>
        </attributes>
</ci-class-attributes>
```

For example:

```
<ci-class-attributes>
        <class-type>host</class-type>
        <attributes>
          <attribute-name>host_hostname</attribute-name>
          <attribute-name>host_dnsname</attribute-name>
          <attribute-name>host_model</attribute-name>
          <attribute-name>host_os</attribute-name>
          <attribute-name>host_snmpsysname</attribute-name>
          <attribute-name>host_vendor</attribute-name>
        </attributes>
</ci-class-attributes>
```

Note: HP Release Control also displays the attributes of the CIT based on the HP Universal CMDB CIT hierarchy. For example, if the displayed CIT is a router, the attributes of the router's host are also displayed.

Configuring Synchronization Frequency

By default, HP Release Control is synchronized with the CMDB database every 7200 seconds—that is, every two hours. To make this synchronization more or less frequent, modify the value in the following line of the **mam-integration.settings** file's <**cmdb-synchronizations**> section:

```
<cmdb-sync-frequency>7200</cmdb-sync-frequency>
```

Advanced Connection Settings

This section describes how to define the type of connection between HP Release Control and HP Universal CMDB.

To set the connection type:

1. Open the <**HP Release Control installation directory**>**conf****mam-integration.settings** file.
2. Locate the **strategy** property in the <**mam-connection**> section:

3 Set the value to **RMI**, **HTTP**, or **HTTPS**. Note that in version 7.0 of HP Universal CMDB, **RMI** is the only valid value and in version 8.0 only **HTTP** and **HTTPS** are valid values.

4 If you specified HTTPS, perform the following steps:

   a Copy the HP Universal CMDB certificate to the **<HP Release Control installation directory>\j2sdk\bin** directory.

   b From the command line, go to the **<HP Release Control installation directory>\j2sdk\bin** directory and run the following command:

   keytool –importcert –alias <uCMDB host name> -file <uDMBD certificate file location> -keypass <uCMDB certificate password> -keystore <RC Installation folder>\j2sdk\lib\security\cacert –storepass changeit

   c When asked if you trust this certificate, type y and press ENTER.

Mapping HP Release Control–HP Universal CMDB Impact Severity Levels

HP Universal CMDB and HP Release Control use different severity level scales. When severity levels are imported from HP Universal CMDB to HP Release Control, there must be a mapping to convert the scales. The following table shows the default mapping scheme.

HP Release Control Impact Severity Level	HP Universal CMDB Severity Levels
Very Low	2 or below
Low	3 - 4
Medium	5 - 6
High	7 - 8
Critical	9

To modify this mapping scheme, change the following lines in the <**enum-mappings**> section of the **mam-integration.settings** file:

```
<entry-name>High</entry-name>
<high-value>8</high-value>
```

The number represents the upper boundary of the given severity level. In the above example, the upper boundary of the **High** severity level is **8**. To modify this, change the number to the required upper boundary.

Upgrading the HP Universal CMDB Version

Perform the steps in this section if you upgrade HP Universal CMDB after installing and configuring it to work with HP Release Control.

1 Back up the mam-integration.settings file.

Create a copy of the mam-integration.settings file located in the <**HP Release Control installation directory**>**conf** directory.

2 Install or upgrade the new version of HP Universal CMDB.

Install or upgrade the new version of HP Universal CMDB on the desired server according to the installation instructions found in the HP Universal CMDB documentation.

3 Run the uCmdbConfigurer utility.

You run the uCmdbConfigurer utility by using the following command:

```
C:\<HP Release Control installation directory>\bin\uCmdbConfigurer.bat <option>
```

Where <option> can be:

Option	Description
usage	Displays a list of valid options, their explanations, and their parameters.

Option	Description
current-version	Displays the version of HP Universal CMDB configured with HP Release Control.
install <version>	Runs the uCmdbConfigurer utility. **version** is the new version of HP Universal CMDB. Valid options are **70**, **751,752**, **80**, and **mock**. If you have installed a patch on one of the above versions and your version number does not match any of the above, see "Manual Configuration for HP Universal CMDB Patches" on page 70.

4 Reconfigure the mam-integration.settings file.

a If you made any modifications to the old **mam-integration.settings** file, copy them over to the new file. Make sure you copy only the sections containing your modifications and do not replace the entire **mam-integration.settings** file.

b In the **mam-integration.settings file**, enter the DNS name of the server on which HP Universal CMDB is installed in the **<mam-server>** property as shown below.

```
<mam-connection version="@onyx.version@">
<mam-version>8.0</mam-version>
<mam-server>ENTER SERVER DNS HERE</mam-server>
<port>8080</port>
<strategy>HTTP</strategy>
</mam-connection>
```

c In the **mam-integration.settings file**, set the **strategy** property as described in "Advanced Connection Settings" on page 65.

d If you are using HP Universal CMDB 7.x with a distributed configuration, set the **locator** property. This property is located next to the **strategy** property (mentioned above). The **locator** property can be defined as either **RMI**, **HTTP**, or **HTTPS**. The default value is **RMI**. We recommend that you set the **locator** property to be the same as the **strategy** property.

5 Redeploy the Release Control package.

Redeploy the **ccm_package.zip** file located in the **<HP Release Control installation directory>\conf\uCmdb-<version>-extensions** where **<version>** is the new version of HP Universal CMDB. Valid options are **70, 751, 752, 80**, and **mock**. For more information about deploying packages, see the HP Universal CMDB documentation.

6 (Optional) Export the application importance property (when upgrading to HP Universal CMDB 8.0).

In earlier versions of HP Release Control, you were able to set the importance property in the Administrator module. In newer versions (8.0 and higher), this property is managed in HP Universal CMDB. You can export the data from this property in HP Release Control to HP Universal CMDB as follows:

a Make sure the HP Universal CMDB and HP Release Control servers are up and running.

b Run the **ApplicationImportanceExporter.bat** file located in the **<HP Release Control installation directory>\bin** directory.

7 Update the synchronization settings.

Note: If you are exporting the application importance property, you must complete the above step before doing this step. Performing these steps out of order can result in loss of data.

In the **<HP Release Control installation directory>\conf\ mam-integration.settings** file locate the **<cmdb-synchronizations>** property. If the **<synchronize-business-cis>** property is present, set the value to **true**.

Manual Configuration for HP Universal CMDB Patches

If you have installed a patch for HP Universal CMDB it may prevent impact analysis from functioning. If HP Release Control has not yet come out with an update to support the patch, you can perform this configuration manually.

To manually configure HP Release Control integration with HP Universal CMDB:

1 Make sure that the files in the appropriate column are located on the HP Universal CMDB server in the **<HP Universal CMDB>\j2f\lib** directory:

➤ **HP Universal CMDB 7.0**

File Names in HP Universal CMDB	File Names in HP Release Control
➤ AllClasses.jar	➤ AllClasses-7.02ga.jar
➤ cmdb_framework.jar	➤ cmdb_framework-7.02ga.jar
➤ cmdb_history_client.jar	➤ cmdb_history_client-7.02ga.jar
➤ cmdb_history_server.jar	➤ cmdb_history_server-7.02ga.jar
➤ cmdb_history_shared.jar	➤ cmdb_history_shared-7.02ga.jar
➤ cmdb_server.jar	➤ cmdb_server-7.02ga.jar
➤ cmdb_shared.jar	➤ cmdb_shared-7.02ga.jar
➤ fnd-adapter.jar	➤ fnd-adapter-7.02ga.jar
➤ hacapi.jar	➤ hacapi-7.02ga.jar
➤ javacore.jar	➤ javacore-7.02ga.jar
➤ jbossall-client.jar	➤ jbossall-client-7.02ga.jar
➤ logging.jar	➤ logging-7.02ga.jar
➤ mam_fw_common.jar	➤ mam_fw_common-7.02ga.jar
➤ mam_fw_server.jar	➤ mam_fw_server-7.02ga.jar
➤ mam-common.jar	➤ mam-common-7.02ga.jar

➤ **HP Universal CMDB 7.5**

File Names in HP Universal CMDB	File Names in HP Release Control
➤ AllClasses.jar ➤ cmdb_framework.jar ➤ cmdb_history_client.jar ➤ cmdb_history_server.jar ➤ cmdb_history_shared.jar ➤ cmdb_server.jar ➤ cmdb_shared.jar ➤ fnd-adapter.jar ➤ hacapi.jar ➤ javacore.jar ➤ jbossall-client.jar ➤ mam-common.jar ➤ setting.jar	➤ AllClasses-7.51ga1866.jar ➤ cmdb_framework-7.51ga1866.jar ➤ cmdb_history_client-7.51ga1866.jar ➤ cmdb_history_server-7.51ga1866.jar ➤ cmdb_history_shared-7.51ga1866.jar ➤ cmdb_server-7.51ga1866.jar ➤ cmdb_shared-7.51ga1866.jar ➤ fnd-adapter-7.51ga1866.jar ➤ hacapi-7.51ga1866.jar ➤ javacore-7.51ga1866.jar ➤ jbossall-client-7.51ga1866.jar ➤ mam-common-7.51ga1866.jar ➤ setting-7.51ga1866.jar

➤ **HP Universal CMDB 8.0**

File Names in HP Universal CMDB	File Names in HP Release Control
ucmdb-api-<version>-impactapi-5.jar	ucmdb-api-8.0-impactapi-5.jar

2 Back up and delete all of the .jar files listed above from the **<HP Release Control installation directory>\tomcat\webapps\ccm\WEB-INF\lib** directory.

3 Take the .jar files from HP Universal CMDB and copy them to the **<HP Release Control installation directory>\tomcat\webapps\ccm\WEB-INF\lib** directory. Rename them to match the HP Release Control file names above.

4 Restart the HP Release Control server.

5

Working in Standalone Mode

This chapter describes how to work with HP Release Control in standalone mode without using HP Universal CMDB.

This chapter includes:

About Working in Standalone Mode

Caution: Working in standalone mode provides limited capabilities and functionality and is intended only as a first step in working with HP Release Control. To take full advantage of the features offered by HP Release Control, you should be working with HP Universal CMDB.

In a regular HP Release Control deployment, when your service desk application is synchronized with the CMDB server, HP Release Control can locate CIs using the CI or change request IDs and perform an impact analysis of the identified CIs.

When you are working in standalone mode, you use the functions within the **<HP Release Control installation directory>\conf\scripts.ext\cmdb-mock.js** script to configure how HP Release Control identifies CIs and how the CIs are used in impact analysis calculations.

To configure HP Release Control to work in standalone mode:

➤ Open the <**HP Release Control installation directory**>**conf****mam-integration.settings** file and enter **Mock** as the value of the <**mam-version**> property.

Configuring the cmdb-mock.js Script

The **cmdb-mock.js** script is divided into the following three sections:

➤ **Analyze CI config**

➤ **Impact config**

➤ **Synchronize Application config**

Analyze CI config

HP Release Control uses analysis rules to locate names of CIs within collected requests. You use the following functions in the **Analyze CI config** section to generate a unique ID for the CI names that were located and to determine how the CIs will appear in the HP Release Control UI:

➤ **getCIType.** This function assigns a type of CI. By default, the CI type is taken from the name of the analysis rule that located the CI.

```
function getCiType(analyserName){
        return analyserName.toLowerCase();
}
```

➤ **getCiID.** By default, this function uses the CI type defined above and the name of the CI itself as it appears in the request, to generate a unique ID for the CI.

```
function getCiID(ciName, ciType){
        return ciName.toLowerCase() + ciType.;
}
```

Caution: The **getCiID** function should always be defined so that the value of ID that is generated is unique in HP Release Control. This ensures that each CI is uniquely analyzed within the system.

➤ **getCiLabel.** This function defines the way the CI will appear in the HP Release Control UI. By default this function returns the name of the CI as it appears in the request.

```
function getCiLabel(ciName, ciType){
        return ciName;
}
```

Impact config

You use the following functions in the **Impact config** section to determine the behavior of CIs during Impact Analysis calculations:

➤ **isSystem.** This function determines whether the CI objects defined above in the **Analyze CI config** section are classified as business or as system CIs (hardware). In the HP Release Control UI, business and system CIs are displayed differently in the impact analysis results.

```
function isSystem(ciName, ciType){

        for(i=0; i< APPLICATION_TYPES.length; i++){
            if(APPLICATION_TYPES[i].toLowerCase() == ciType.toLowerCase()){
                return false;
            }
        }
        return true;
}
```

The above function can either refer to application type variables that you define at the beginning of the **Impact config** section or it can refer to an external javscript file.

➤ **getSeverity.** This function defines the impact severity levels for each CI in impact analysis calculations.

```
function getSeverity(name, type){
        if (type.toLowerCase() == APP_TYPE1.toLowerCase()){
            return SEVERITY_CRITICAL;
        }
        else if(type.toLowerCase() == APP_TYPE2.toLowerCase()){
            return SEVERITY_HIGH;
        }
        else if(name.toLowerCase() == APP_NAME1.toLowerCase()){
            return SEVERITY_MEDIUM;
        }
        return SeverityEnum.getUnknown();
}
```

The return values for this function need to be defined in the **HP Release Control installation directory>\conf\enumerations.settings** file.

Synchronize Application config

In a regular HP Release Control deployment, HP Release Control is synchronized with the CMDB database. When a Business CI no longer appears in the CMDB database, the Business CI is defined as obsolete in the HP Release Control UI.

In standalone mode, you can determine whether you want HP Release Control to differentiate between relevant and obsolete business CIs. If you do want to differentiate, you define a list of relevant business CIs. All business CIs that do not match this list will be defined as obsolete.

You use the following functions in the **Synchronize Application config** section to define this functionality:

➤ **showObsolete.** This function defines whether or not HP Release Control differentiates between relevant and obsolete business CIs.

```
function showObsolete(){
        return false;
}
```

By default, this function is set to **false** and the HP Release Control does not differentiate between relevant and obsolete business CIs. If you set it to **true**, use the **synchronizerApplication** function to define a list of relevant business CIs.

➤ **synchronizerApplication.** This function defines a list of relevant business CIs. All business CIs defined in the above sections that do not match the criteria determined in this function will be defined as obsolete.

```
function synchronizerApplication(applicationsSet){
        // ScriptingApplicationImpl (appName, appType)
        applicationsSet.add(new ScriptingApplicationImpl(APP_NAME1, APP_TYPE1));
        applicationsSet.add(new ScriptingApplicationImpl(APP_NAME2, APP_TYPE2));
        applicationsSet.add(new ScriptingApplicationImpl(APP_NAME3, APP_TYPE3));

        return applicationsSet;
}
```

You can define the criteria for relevant business CIs inside the function as illustrated above or you can refer to an external file or database.

If you define the criteria inside the function and you change the criteria, you need to restart the HP Release Control server for the changes to take effect.

Note: In the HP Release Control UI, you can use the business CIs criteria defined in this function to filter change requests before they come into the system.

6

Configuring General Settings

This chapter describes how to configure the SMTP mail server responsible for sending HP Release Control email notifications and how to reconfigure the HP Release Control application server address.

This chapter includes:

Configuring the SMTP Mail Server

To work with HP Release Control, you must configure connection properties for the SMTP mail server responsible for sending HP Release Control email notifications. The following are the properties you must configure in the **<HP Release Control installation directory>\conf\integrations.settings** file:

- **user name.** Specify the user name required to connect to the SMTP mail server, if one is required.
- **password.** Specify the password required to connect to the SMTP mail server, if one is required. If the password must be encrypted, see Appendix A, "Password Encryption" for details on encrypting passwords.
- **SMTP host.** Specify the host name of the SMTP mail server machine.
- **SMTP port.** Specify the port to be used to connect to the SMTP mail server.

Configuring the HP Release Control Server

The HP Release Control application server name and address are configured automatically during the HP Release Control installation process. HP Release Control uses these settings to create links to requests in the HP Release Control application from email notifications.

If the links from the email notifications to the HP Release Control application are not working properly, this may be a result of DNS resolution problems. To try and resolve this issue for future notifications that are sent, change the server machine name in the following line of the **<HP Release Control installation directory>\conf\server.settings** file to the server IP address.

For example, change:

```
<server-address>http://server1:8080/ccm</server-address>
```

to:

```
<server-address>http://198.10.20.1:8080/ccm</server-address>
```

7

Configuring Business CI Settings

You view details of the Business CIs affected by the change requests that HP Release Control processes, assign importance levels to these business CIs, and associate specific users with them in the Administration module's Business CIs tab.

This chapter includes:

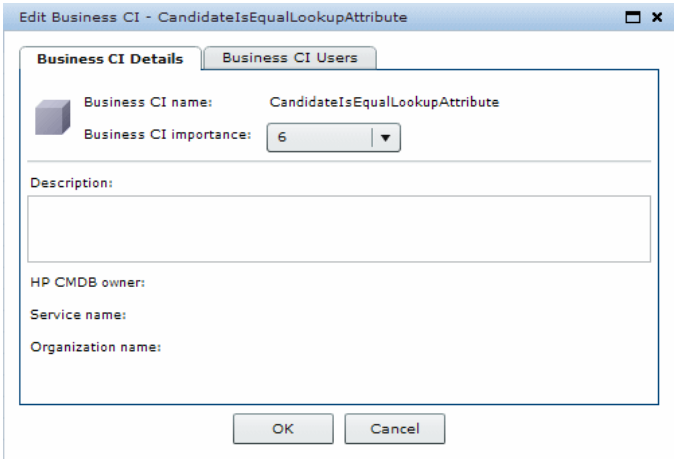
Viewing Business CI Details

You can view details of the Business CIs included in the HP Universal CMDB view that you defined for HP Release Control.

To view business CI details:

1 In the Administration module's **Business CIs** tab, select the business CI whose details you want to view. If the list of business CIs is lengthy, you can use the search box and/or the **First**, **Previous**, **Next**, and **Last** buttons to locate the business CI.

2 Click the **Edit** button in the top left corner. The Edit Business CIs – <Business CI Name> dialog box opens, displaying a description of the business CI as well as other HP Universal CMDB-related details of the business CI.



Assigning Importance Levels to Business CIs

As part of the HP Release Control risk analysis configuration, you assign relative levels of importance to your business CIs. Each business CI can be assigned an importance level between 1 and 10. Change requests that affect business CIs with higher importance levels will be marked by HP Release Control as having a higher risk.

The importance property is configured differently depending on which version of HP Universal CMDB you are using.

Configuring the Importance Property using HP Universal CMDB 8.0

You configure the importance property from within HP Universal CMDB. The property is referred to as **business_criticality_level** in HP Universal CMDB. To export old data from the importance property which was assigned within HP Release Control to HP Universal CMDB, see the section about upgrading the HP Universal CMDB version in the *HP Release Control Deployment Guide*.

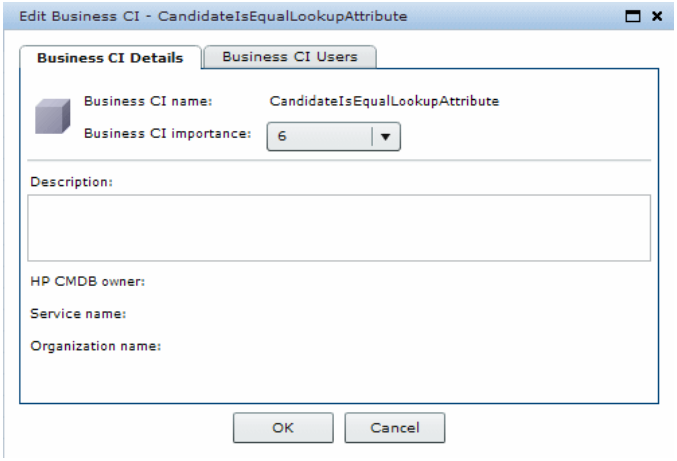
Configuring the Importance Property using HP Universal CMDB 7.x

You configure the importance property from the HP Release Control administration module.

To assign importance levels to business CIs:

1 In the Administration module's **Business CIs** tab, select the business CI for which you want to assign an importance level. If the list of business CIs is lengthy, you can use the search box and/or the **First**, **Previous**, **Next**, and **Last** buttons to locate a business CI.

2 Click the **Edit** button in the top left corner. The Edit Business CIs – <Business CI Name> dialog box opens.



3 From the **Business CI importance** list, select a business CI importance level between 1 and 10.

Note: If you do not assign an importance value to a business CI, the default importance value assigned is zero.

In this case, the default mapping is used for the **business CI importance** risk factor in the risk calculation. For more information about defining risk factors, see "Defining Risk Factors" on page 145.

---

4 Click **OK** to save your settings and close the Edit Business CI – <Business CI Name> dialog box.

Associating Business CIs with Users

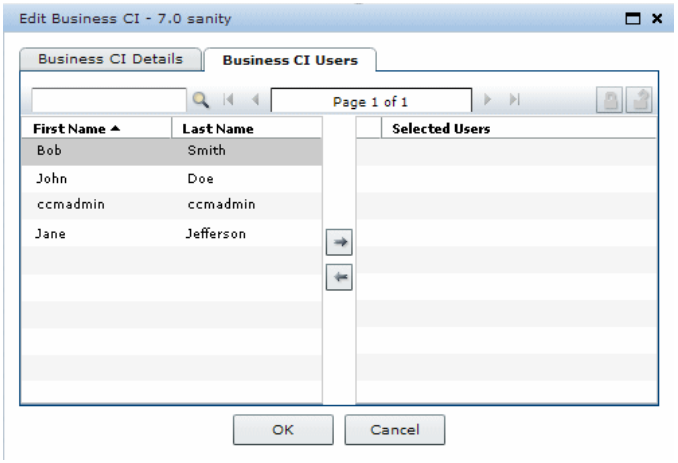
You can associate specific HP Release Control users with each business CI.

To associate HP Release Control users with a business CI:

1 In the Administration module's **Business CIs** tab, select the business CI you want to associate with one or more users. If the list of business CIs is lengthy, you can use the search box and/or the **First**, **Previous**, **Next**, and **Last** buttons to locate the business CI.

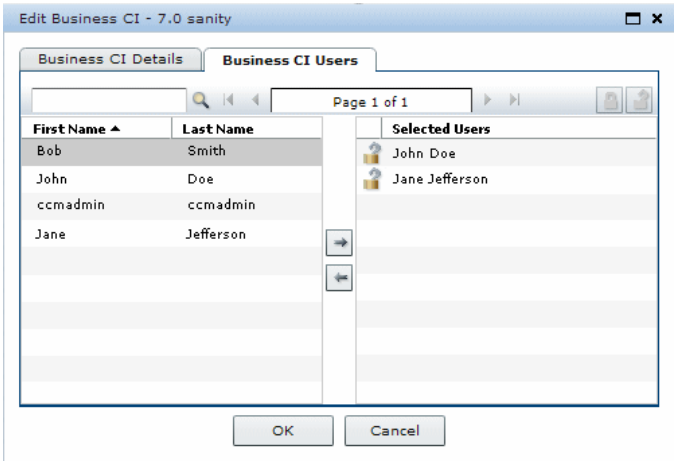
2 Click the **Edit** button in the top left corner. The Edit Business CI – <Business CI Name> dialog box opens.

3 Click the **Business CIs** tab. A list of the HP Release Control users previously defined by the administrator is displayed in the left hand pane.



4 Select the users you want to associate with the business CI from the users list in the left hand pane. If the list of users is lengthy, you can use the search box to display only those users that match the text you enter in the search box. In addition, you can use the **First**, **Previous**, **Next**, and **Last** buttons to locate a user. You can select multiple users using the CTRL key.

5 Click the top arrow. The users appear in the **Selected Users** list.



6 To ensure that a user will not be able to remove the business CI with this business CI, select the user and click the **Enforce Business CI** button.

To restore the user's ability to remove the association with this business CI, select the user and click the **Stop Enforcing Business CI** button.

7 Click **OK** to save your settings and close the Edit Business CI – <Business CI Name> dialog box. Your modifications will take effect when you next log in to HP Release Control.

8

Lightweight Single Sign-On Authentication

This chapter describes how to enable and manage lightweight single sign-on (LW-SSO) capability in HP Release Control.

This chapter includes:

About Lightweight Single Sign-On

Single Sign-On is a method of access control that enables a user to log on once and gain access to the resources of multiple software systems without being prompted to log on again. The applications inside the configured group of software systems trust the authentication, and there is no need for further authentication when moving from one application to another.

The default single sign-on authentication strategy for HP Release Control is Lightweight Single Sign-On (LW-SSO). LW-SSO is embedded in HP Release Control and does not require an external machine for authentication.

LW-SSO System Requirements

The requirements for LW-SSO configuration, per application, are as follows:

Application	Version	Comments
Java	1.5 and later	N/A
HTTP Sevlets API	2.1 and later	N/A
Internet Explorer	6.0 and later	Browser should enable HTTP session cookie and HTTP 302 Redirect functionality
FireFox	2.0 and later	Browser should enable HTTP session cookie and HTTP 302 Redirect functionality
JBoss Authentications	JBoss 4.0.3 JBoss 4.3.0	
Tomcat Authentications	Standalone Tomcat 5.0.28 Standalone Tomcat 5.5.20	N/A

Application	Version	Comments
Acegi Authentications	Acegi 0.9.0 Acegi 1.0.4	N/A
Web Services Engines	Axis 1 - 1.4 Axis 2 - 1.2 JAX-WS-RI 2.1.1	N/A

HP Products Integrated with LW-SSO

The HP products that are currently integrated with the LW-SSO authentication strategy are:

HP Product	Version
Business Availability Center	8.0
Network Node Manager iSPI	8.10
Service Automation Reporter	7.5
SiteScope	10.00
Transaction Vision	7.5
Business Process Insight	7.5
Diagnostics	7.5
Service Manager/Center	6.2

Enabling LW-SSO in HP Release Control

To enable LW-SSO in HP Release Control, in the **HP Release Control installation directory>\conf\security.settings** file, add the following **lw-sso** element under the **authentication-settings** element:

```
<settings>
      <authentication-settings version="...">
            ...
            <lw-sso>
                  <init-string>str</init-string>
                  <domain>d1</domain>
                  <protected-domains>
                        <domain>d1</domain>
                        <domain>d2</domain>
                  </protected-domains>
            </lw-sso>
      </authentication-settings>
</settings>
```

The **lw-sso** elements should then be configured as follows:

- **<init-string>.** This element must contain a shared string that will be used by all trusted applications integrating with LW-SSO.
- **<domain>.** This is an optional element and should contain the HP Release Control server domain. If left undefined, HP Release Control will automatically assign a value to this element.
- **<protected-domains>.** This is an optional element and should contain at least one HP Release Control server domain. In a case where trusted applications are located in other domains, all those domains should be defined in this element.

Web Single Sign-On – Use Cases

This section describes the use cases of LW-SSO via the Web.

This section includes:

- Login Use Case
- Logout Use Case
- Application Checks if Request Is Secured

Login Use Case

The login use case is as follows:

1 The application authenticates the user.

2 The application creates a user context using one of the **SecurityContextFactory** methods:

```
// The application creates user context with SecurityContextFactory.
// Please find below one example. Application can use any API of
SecurityContextFactory
String userName = "Bob";
SecurityContextFactory factory =
SecurityContextFactoryUtils.getSecurityContextFactory();
SecurityContext securityContext = factory.createSecurityContext(userName);
```

3 The application enables Single Sign-On.

```
LWSSOUtils.enableSSO(servletRequest, servletResponse, securityContext);
```

Note: The weakest authentication framework used by the LW-SSO integrated applications determines the level of authentication security for all of the applications. It is recommended that only applications using strong and secure authentication frameworks issue a LW-SSO token.

Logout Use Case

A logout is declarative in LW-SSO. The logout pages are configured in the LW-SSO infrastructure configuration file.

When an application requests a logout URL, LW-SSO cleans the security context.

Application Checks if Request Is Secured

LW-SSO uses the **isRequestSecured** function to verify that the request is secured. This function is used when the **LWSSOUtils.getSecurityContext** returns a value of **null**, and the application wants to determine the following:

- Whether you want to access a protected resource in the application without being authenticated, in which case a login screen is shown.
- Whether you want to access the login page or a resource that is not protected (for example, help documents).

```
boolean isSecured = LWSSOUtils.isRequestSecured(servletRequest);
```

By default, all URLs are secured, but the LW-SSO infrastructure is configured with non-secure URLs.

If a user accesses the non-secure URLs, the function returns a value of **false**.

If a user accesses the secure URLs, the function returns a value of **true**.

Note: The method returns the correct answer only when the LW-SSO Filter is used.

LW-SSO Limitations

This section describes limitations of the LW-SSO configuration:

➤ **Accessing the application:**

- ➤ The client must access the application with the Fully Qualified Domain Name (FQDN) in the login URL, for example: http://flood.mercury.global:8080/WebApp
- ➤ LW-SSO does not support URLs with an IP Address, or URLs without a domain.

➤ **LW-SSO framework integration:**

Applications can leverage and use LW-SSO capabilities only if integrated within the LW-SSO framework in advance.

➤ **JAAS Realm:**

The JAAS Realm in Tomcat is not supported.

➤ **Using spaces in tomcat directories:**

Using spaces in Tomcat directories is not supported.

It is not possible to use LW-SSO when a Tomcat installation path (folders) includes spaces (for example, Program Files) and the LW-SSO configuration file is located in the common\classes Tomcat folder.

➤ **Load balancer configuration:**

A load balancer deployed with LW-SSO must be configured to use sticky sessions.

- **Multi-Domain Support.**
  - Multi-domain functionality is based on the HTTP referrer. Therefore, LW-SSO supports links from one application to another and does not support typing a URL into a browser window, except when both applications are in the same domain.
  - The first cross domain link using **HTTP POST** is not supported.

    Multi domain functionality does not support the first **HTTP POST** request to a second application (only the **HTTP GET** request is supported). For example, if your application has an HTTP link to a second application, an **HTTP GET** request is supported, but an **HTTP FORM** request is not supported. All requests after the first can be either **HTTP POST** or **HTTP GET**.
  - LW-SSO Token size:

    The size of information that LW-SSO can transfer from one application in one domain to another application on another domain is limited to 15 Groups/Roles/Attributes (note that each item may be an average of 15 characters long).
  - Linking from Protected (HTTPS) to Non protected (HTTP) in a Multi domain scenario:

    Multi domain functionality does not work when linking from a protected (HTTPS) to a non protected (HTTP) page. This is a browser limitation where the referring header is not sent when linking from a protected to a non-protected resource. For an example, see: http://support.microsoft.com/support/kb/articles/Q178/0/66.ASP
  - Third-Party cookies behavior in Internet Explorer:

    Microsoft Internet Explorer 6 contains a module that supports the "Platform for Privacy Preferences(P3P) Project", meaning that cookies coming from a Third Party domain are by default blocked in the "Internet" security zone. Session cookies are also considered Third party cookies by IE, and therefore are blocked, causing LW - SSO to stop working. For details, see: http://support.microsoft.com/kb/323752/en-us.

To solve this issue, add the launched application (or a DNS domain subset as ***.mydomian.com**) to the "Intranet"/"Trusted" zone on your computer (on Microsoft Internet Explorer, select **Menu** > **Tools** > **Internet Options** > **Security** > **Local Intranet** > **Sites** > **Advanced**), which causes the cookies to be accepted.

Caution: The LW-SSO session cookie is only one of the cookies used by the Third party application that is blocked.

➤ **SAML2 token:**

➤ When using a Java based application integrated with LW-SSO to access another Java based application also integrated with LW-SSO, do not use the SAML2 token. Using the SAML2 token in this case can lead to unexpected behavior. Use the LW-SSO token instead.

The SAML2 token should only be used when one of the applications is not integrated with LW-SSO.

➤ Logout functionality is not supported when the SAML2 token is used.

Therefore, if the SAML2 token is used to access a second application, then a user who logs out of the first application will not be logged out of the second application.

➤ The SAML2 token's expiration is not reflected in the application's session management.

Therefore, if the SAML2 token is used to access a second application, then each application's session management will be handled independently of each other.

➤ **IdM security and outbound web services.**

Applications that are integrated with LW-SSO, that use IdM security as the security token for outbound web service security, will not be able to create or issue LW-SSO security tokens for UI (either automatically created or otherwise).

In this case, the LW-SSO configuration must include the following values:

- ➤ **enableAutoCreation** = "**false**"
- ➤ **enableCookieCreation** = "**false**"

➤ **Security context:**

The LW-SSO security context supports only one attribute value per attribute name.

Therefore, when the SAML2 token sends more than one value for the same attribute name, only one value is accepted by the LW-SSO framework.

Similarly, if the IdM token is configured to send more than one value for the same attribute name, only one value is accepted by the LW-SSO framework.

➤ **Multi-domain logout functionality when using Internet Explorer 7:**

Multi-domain logout functionality may fail when using Internet Explorer 7 and when the application is invoking more then 3 consecutive HTTP 302 redirect verbs in the logout procedure.

In such a scenario Internet Explorer 7 may mishandle the HTTP 302 redirect response and display an "Internet Explorer cannot display the webpage" error page instead.

As a workaround, we recommend that, if possible, you reduce the number of application redirect commands in the logout sequence.

LW-SSO Security Warnings

This section describes security warnings that are relevant to the LW-SSO configuration:

➤ **Enable LW-SSO only if required:**

LW-SSO should be disabled unless it is specifically required.

➤ **Level of authentication security:**

The application that uses the weakest authentication framework and issues a LW-SSO token that is trusted by other integrated applications determines the level of authentication security for all the applications.

It is recommended that only applications using strong and secure authentication frameworks issue an LW-SSO token.

➤ **Confidential InitString parameter in LW-SSO:**

LW-SSO uses Symmetric Encryption to validate and create a LW-SSO token. The **initString** parameter within the configuration is used for initialization of the secret key. An application creates a token, and each application using the same initString parameter validates the token.

Note:

- ➤ It is not possible to use LW-SSO without setting the initString parameter.
- ➤ The initString parameter is confidential information and should be treated as such in terms of publishing, transporting, and persistency.
- ➤ The initString parameter should be shared only between applications integrating with each other using LW-SSO.
- ➤ The minimum length of the initString parameter is 12 characters.

➤ **Symmetric encryption implications:**

LW-SSO uses symmetric cryptography for issuing and validating LW - SSO tokens. Therefore, any application using LW-SSO can issue a token to be trusted by all other applications sharing the same initString. This potential risk is relevant when an application sharing an initString either resides or is accessible in an untrusted location.

➤ **User mapping (Synchronization):**

The LW-SSO framework does not ensure user mapping between the integrated applications. Therefore, the integrated application must monitor user mapping. We recommend that you share the same user registry (as LDAP/AD) among all integrated applications.

Failure to map users may cause security breaches and negative application behavior, such as the same user name being assigned to different real users in the various applications.

In addition, in cases where a user logs onto an application (AppA) and then accesses a second application (AppB) that uses container or application authentication, the failure to map the user will force the user to manually log onto AppB and enter a user name. If the user enters a different user name than was used to log onto AppA, the following unexpected behavior can arise: If the user subsequently accesses a third application (AppC) from AppA or AppB, then they will access it using the usernames that were used to log onto AppA or AppB respectively.

➤ **Identity Manager:**

Used for authentication purposes, all unprotected resources in the Identity Manager must be configured with the **nonsecureURLs** setting in the LW-SSO configuration.

LW-SSO Important Information

This section contains important information regarding LW-SSO.

➤ **LW-SSO Token expiration.** The LW-SSO Token's expiration value determines the application's session validity. Therefore, its expiration value should be at least the same value as that of the application session’s expiration value.

- **Recommended configuration of the LW-SSO Token expiration.** Each application using LW-SSO should configure token expiration. The recommended value is 60 minutes. For an application that does not require a high level of security, it is possible to configure a value of 300 minutes.

- **GMT time.** All applications participating in an LW - SSO integration must use the same GMT time with a maximum difference of 15 minutes.

- **Multi-domain functionality.** Multi-domain functionality requires that all applications participating in LW-SSO integration configure the **protectedDomains** settings, if they are required to integrate with applications in different DNS domains. In addition, they must also add the correct domain in the **lwsso** element of the configuration.

- **Get SecurityToken for URL functionality.** To receive information sent as a **SecurityToken** for a URL from other applications, the host application should configure the correct domain in the **lwsso** element of the configuration.

- **Login and Logout URLs.** We recommend that you not configure the application's Login and Logout URL's as nonsecureURLs. Configuring them in this way may lead to unexpected behavior.

Troubleshooting LW-SSO

The following tables describe potential problems that can occur with LW-SSO, and possible solutions for these problems.

This section includes:

- LW-SSO Related Use Cases
- SAML2 Related Use Cases

LW-SSO Related Use Cases

Problem	Possible Cause	Possible Solution
LW-SSO cookie is not created after logging in.	A domain is not defined properly in the LW-SSO element of the configuration.	Make sure that the domain defined in the LW-SSO element of the configuration is equal to the application's domain.
	A domain that is passed as a parameter to the enableSSO function is not correct.	Make sure that the domain that is passed as a parameter to the **enableSSO** function is equal to the application's domain.
	You did not access the application with the Fully Qualified Domain Name (FQDN) in the login URL.	Make sure that you access the application with the Fully Qualified Domain Name (FQDN) in the login URL.
LW-SSO fails to create a cookie for AutoCookieCreation functionality.	A domain is not defined properly in the LW-SSO element of the configuration.	Make sure that the domain defined in the LW-SSO element of the configuration is equal to the application's domain.
The LW-SSO token is not validated.	The two applications have different initString parameters in the crypto element of the configuration (or other crypto parameters).	Use the same initString in both applications (in addition to all other crypto parameters in the LW-SSO creation element).
	Some applications have a GMT time difference greater than 15 minutes.	Make sure that all applications participating in a LW - SSO integration are set to the same GMT time, with a maximum difference of 15 minutes.

Problem	Possible Cause	Possible Solution
LW-SSO fails to validate the LW-SSO token in a multi domain environment.	In the configuration of one of the applications, a domain is not defined properly in the LW-SSO element.	The domain defined in the LW-SSO element of the application's configuration must be the same as the application's domain according to real domains in use.
	In the configuration of one of the applications, a domain is not defined correctly in the protectdDomains list.	Make sure that the domains in the protectedDomains list of all of the applications' configurations are defined correctly.
	The LW-SSO session cookie is blocked/denied when using the Internet Explorer 6.0 or 7.0 browsers.	Add all LW-SSO servers to the "Intranet"/"Trusted" zone in the Internet Explorer security zones on your computer (**Tools** > **Internet Options** > **Security** > **Local Intranet** > **Sites** > **Advanced**). This will allow all cookies to be accepted.
	Some applications have different initString parameters in the crypto element of the configuration (or other crypto parameters).	Use the same initString in all applications (in addition to all other crypto parameters in the LW-SSO creation element).
	Some applications have a GMT time difference greater than 15 minutes.	Make sure that all applications participating in a LW - SSO integration are set to the same GMT time with a maximum difference of 15 minutes.
	Multi domain link goes from the protected (HTTPS) to the Non protected (HTTP) resource.	When linking/crossing from one domain to another, make sure that the first link/cross request goes from one protected resource (HTTPS) to another protected resource (HTTPS).

SAML2 Related Use Cases

Problem	Possible Cause	Possible Solution
LW-SSO fails to issue a SAML2 Token.	A keystore configuration for SAML2 creation is not valid and most likely does not point to a valid keystore.	Make sure that the keystore configuration for SAML2 creation is valid and points to a valid keystore.
	A privateKeyAlias or privateKeyPassword configuration for SAML2 creation is not valid. They might not be pointing to a valid private key.	Make sure that the privateKeyAlias or privateKeyPassword configuration for SAML2 creation is valid and point to a valid private key.
LW-SSO fails to validate the SAML2 token.	A keystore configuration for SAML2 validation is not valid. It most likely does not point to a valid keystore.	Make sure that the keystore configuration for SAML2 validation is valid and points to a valid keystore.
	A certificate used for signing is not imported in the configured keystore with a required public key alias. Note that the public key alias may be configured in the SAML2 validation configuration or it can be passed in SAML2 token by the issuer.	Make sure that the certificate used for signing in is imported in the configured keystore with a required public key alias.
LW-SSO fails to receive all roles or groups.	The element's roleAttributeName or groupAttributeName defined in the SAML2 configuration is different then the one configured in the applications' configurations element.	Make sure that the elements roleAttributeName or groupAttributeName is defined equally in all of the applications' configurations as in the SAML2 configuration.

Part III

Configuring Analysis of Change Requests

9

Before Configuring Change Request Analysis

This chapter describes the initial configuration procedures that you need to complete before configuring change request analysis.

This chapter includes:

Configuring the Collection Frequency of Converted Requests

After change requests have been converted from their original service desk application formats to a standard, generic format, they can be processed by HP Release Control. By default, HP Release Control collects the converted requests for processing every 30 seconds. To modify the request collection frequency, you must change the value in the following line of the **<HP Release Control installation directory>\conf\change-flow.settings** file:

```
<change-collection-freq>30</change-collection-freq>
```

Using the Pre- and Post-Change Request Processing Functions

You can use the **preChangeProcess** and **postChangeProcess** functions in the **<HP Release Control installation directory>\conf\scripts.ext\change-flow.js** script to calculate certain pre-change request processing or post-change request processing factors.

For example, if you want to define a risk factor based on the amount of time that a change request is in the HP Release Control system without being processed, you can use the **preChangeProcess** function to calculate the time at which the change request first enters HP Release Control. To do so, you would define a custom field called **first-time** that would be configured to the time at which the change request enters HP Release Control. You would then instruct HP Release Control to calculate the **first-time** value as follows:

```
function preChangeProcess(prevChange, newChange)
{
        If (prevChange == null) {
            var now = java.lang.System.currentTimeMillis();
            newChange.setField("first-time", now);
        }
        else {
            var firstTime = prevChange.getField("first-time");
            newChange.setField("first-time", firstTime);

        }
}
```

You can use the **postChangeProcess** function in a similar manner to calculate factors relating to steps within the request processing itself, such as the calculation of risk or collisions.

For a detailed explanation of the objects that can be included in these functions, refer to the **GenericRFC** class in the **API_Reference.chm** file, located in the **<HP Release Control installation directory>\documentation** folder.

10

Configuring Impact Analysis

This chapter describes how to set up and configure HP Release Control to calculate impact analysis.

This chapter includes:

About Configuring Impact Analysis

Impact analysis calculates the effects of change requests on CIs. Both the CI details, and their relationships are imported from HP Universal CMDB. Therefore, in order for impact analysis to function, you must configure the HP Universal CMDB settings. For more information, see "Overview of Configuring HP Universal CMDB-Related Settings" on page 55.

Determining When to Calculate Impact Analysis

Calculating impact analysis uses a lot of system resources. HP Release Control can be configured to minimize the instances in which impact analysis is performed to save system resources.

Every time a new ticket is created, the impact must be calculated. However, impact is also calculated in some cases in which a change was made to an old ticket/change request. The **shouldCalcImpact** function within the **<installation directory>\conf\scripts.ext\change-flow.js** script contains the protocol which determines when impact must be recalculated. By default, the function appears as follows:

```
function shouldCalcImpact (prevChange, newChange)
{
    if (newChange.isInitialLoadState())
        return true;

    newChangeValidStatus = isStatusValid4Calc(newChange);
    prevChangeValidStatus = isStatusValid4Calc(prevChange);

    if(prevChange == null){
        return true ;
    }

    if ( !prevChangeValidStatus && newChangeValidStatus ){
        return true;
    }

    else if(!newChange.isAnalyzedCisEquals(prevChange)){
        return newChangeValidStatus;
    }

    return newChangeValidStatus;
}
```

The above function works as follows:

- HP Release Control first checks whether there is a pre-existing, valid impact analysis on this change request. If not, it returns true (impact is calculated).
- If the triggered CIs in the original change request are the same after the change to the change request, the impact is not recalculated. If the triggered CIs are different, the impact is recalculated.

For a detailed explanation of the objects that can be included in this function, refer to the **GenericRFC** class in the **API_Reference.chm** file, located in the **docs\pdfs** directory of the HP Release Control CD-ROM.

In the **<impact-calculation>** section of the **change-flow.settings** file, you can specify whether the impact of CIs in tasks (second-level requests) should be calculated separately from the changes to which the tasks belong, or be included in the impact analysis of the tasks' respective changes. By default, an impact analysis of a task will trigger an impact analysis for the change with which it is associated, and the changed CIs of a task are included in the changed CI list of the task's parent change. To modify this, change the value in the following line to **false**:

```
<aggregate-cis>true</aggregate-cis>
```

Adding Operations Before Impact Analysis

Based on your impact analysis calculations, you may want to perform certain operations prior to every impact analysis. For example, you may want to update certain CI data prior to calculating impact if that data will affect the impact analysis.

The **preCalcRisk** function within the **<installation directory>\conf\scripts.ext\change-flow.js** script contains the location in which you can add operations to be performed before each impact analysis. By default, this function is empty, meaning that no operations are automatically performed before each impact analysis. It receives two arguments which are both writable GenericRFC arguments.

For a detailed explanation of the objects that can be included in this function, refer to the **GenericRFC** class in the **API_Reference.chm** file, located in the **docs\pdfs** directory of the HP Release Control.

Configuring Analysis Rules

To analyze the impact of the collected change requests, HP Release Control must first identify the location and format of the CIs contained in the requests. This is done by the analysis rules. You define the analysis rules you want HP Release Control to use in the Administration module's Analysis Rules tab.

This section includes the following topics:

Adding or Editing Analysis Rules

HP Release Control must have a separate analysis rule for each CIT which you want to recognize. Analysis Rules can be added and edited in the Analysis Rules tab.

To add or edit an analysis rule:

1 In the Administration module, click the Analysis Rules tab and select the desired rule you wish to edit.

To add a new rule, click the **Add Rule** button.

2 In the CI Analysis Rule Definition pane, fill in the following fields:

- **Name.** The name of the CIT that you want HP Release Control to locate in the collected requests, as well as the logical name of the analysis rule that can be referenced in the field settings (for more information, see "Configuring Analysis Rules" on page 110).

Notes:

- The name of the CIT must appear as it is defined in the **<HP Release Control installation directory>\conf \mam-integration.settings** file in the <lookup-attributes-directives> tag (if you are working with HP Universal CMDB).
- The **ip-range** analysis rule is an exception to the above specifications, as it corresponds to the **ip** CIT in HP Universal CMDB.

- **Description.** A description of the CIT that you want HP Release Control to locate in the collected requests.
- **Analyzer class.** Select **Use rule name as CI class type** unless your CIT is IP-Range. For IP-Range CITs, select **Use the IP-Range analyzer**.
- **Patterns.** The text from various fields on the collected requests is parsed using regular expressions defined as **patterns**. For details on working with regular expressions, refer to the following URL: http://java.sun.com/j2se/1.4.2/docs/api/java/util/regex/Pattern.html

- To delete a pattern, click the **Remove Pattern** button.

- To add a new pattern, click the **Add Pattern** button.

Patterns are defined by the following two elements:

- **Match Pattern.** A regular expression which defines how to parse the collected requests in the process of identifying CI, using regular expressions.
- **CI Backreference.** Uses regular expressions to specify the exact part of the pattern in which the CI is located. A value of 1 is used to specify the first group in the pattern, a value of 2 is used to specify the second group in the pattern, and so forth. A value of 0 instructs HP Release Control to use the entire pattern in locating the CI.

By default, analysis rules are defined for the **host**, **ip**, and **ip-range** CITs. In addition, there are two predefined, built-in analysis rules that can be used when your service desk application is synchronized with the CMDB server. The **cmdb-object-id** analysis rule locates CIs using the IDs of HP Universal CMDB CIs. The **mam-ticket** analysis rule locates CIs using change request IDs.

You apply analysis rules to change request fields in the Administration module's Fields tab. For more information about applying analysis rules, see "Configuring Analysis Rules" on page 110.

Testing Analysis Rules

Analysis rules can be tested by manually entering a string and running the patterns on it. The results are displayed in the Analyzed CIs pane.

To test an analysis rule:

1. In the Analysis Rules tab, select the rule that you want to test.
2. In the Test Selected Analyzer pane, select **All Patterns** to perform the test using all defined patterns or **Selected Pattern** to perform the test using the selected pattern.
3. When the test is run, the ticket text is broken up into strings. To have HP Release Control check these strings for valid CIs using the uCMDB, select the **Match candidate with CMDB** box.
4. In the **Test Value** pane, enter a string to test the analysis rule.
5.  Click the **Test Analyzer** button to test the analysis rule. The parsed string is displayed in the Analyzed CIs pane.

Applying Analysis Rules to Fields

You apply analysis rules to change request fields in the Administrator module's Fields tab. These are the rules according to which you want HP Release Control to identify the location and format of CIs contained in the field's text.

You can apply analysis rules to change request fields of type **Short Text** or **Long Text**. It is recommended that you apply analysis rules to change request fields that contain CIs only, without additional text comments.

For more information about creating or modifying change request fields, see "Configuring Change Request Field Settings" on page 29.

To apply analysis rules to change request fields:

1 In the Adminstrator module, click the **Fields** tab.

2 In the Field Attributes pane, click the **CI Analysis Rules** tab.

The CI Analysis Rules tab contains all the analysis rules specified in the Analysis Rules tab. When you add a rule to the Analysis Rules tab, it appears as the last rule in the CI Analysis Rules tab.

3 To apply analysis rules to the selected change request field, select the check boxes next to the appropriate analysis rules. By default, the following analysis rules are available:

Rule	Description
cmdb-object-id	A predefined, built-in analysis rule that can only be used when your service desk application is synchronized with the CMDB server. This rule locates CIs using HP Universal CMDB configuration item IDs.
mam-ticket	A predefined, built-in analysis rule that can only be used when your service desk application is synchronized with the CMDB server. This rule locates CIs using change request IDs.
host	Identifies hosts within the selected field.
ip	Identifies IP addresses within the selected field.
ip-range	Identifies IP addresses within the selected field from a range of IP addresses that you define.
business	Identifies Business CIs within the selected field using comma delimiter pattern.

For each analysis rule that you selected, choose the level at which you want to apply the rule:

➤ **Change.** The analysis rule is applied to the field only when the field belongs to a top-level request.

➤ **Task.** The analysis rule is applied to the field only when the field belongs to a second-level request.

You can select both **Change** and **Task** if you want the analysis rule to apply to all requests in which the selected field appears.

Note: The names of the top-level and second-level requests are configurable in the **enumeration-labels.properties file**. For more information see "Configuring Enumeration Field Display Settings" on page 227.

By default, the **host**, **ip**, and **ip-range** analysis rules are applied to the **changed-ci-list** field, at both the **Change** and **Task** levels.

Determining When to Analyze the Tickets

HP Release Control can be configured to minimize the instances in which a ticket analysis is performed to save system resources.

Every time a new ticket is created, the impact must be calculated. However, impact is also calculated in some cases in which a change was made to an old ticket/change request. The **shouldAnalyze** function within the **<installation directory>\conf\scripts.ext\change-flow.js** script contains the protocol which determines when to analyze a ticket. By default, the function appears as follows:

```
function shouldAnalyze(prevChange, newChange){
    if (newChange.isInitialLoadState()){
        return true;
    }

    if(newChange.isTicketAnalyzer()){
        return true;
    }

    return !(newChange.isAnalysisRulesEqual(prevChange));
}
```

The above function works as follows:

- HP Release Control first checks to see if this is the first time this ticket is being loaded. If it is, a ticket analysis is performed.
- If this is not the first time the ticket is being loaded, HP Release Control checks to see if you are using PPM integrated with HP Universal CMDB. If you are, a ticket analysis is performed.
- Next, HP Release Control checks to see if there have been any changes to the ticket. If there have been changes, a ticket analysis is performed. If there have not been changes, no ticket analysis is performed and the function concludes.

For a detailed explanation of the objects that can be included in this function, refer to the **GenericRFC** class in the **API_Reference.chm** file, located in the **docs\pdfs** directory of the HP Release Control CD-ROM.

11

Configuring Time Periods

This chapter describes how to configure time periods in HP Release Control.

This chapter includes:

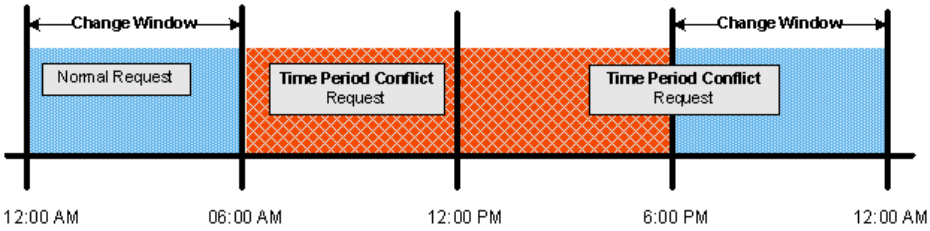
About Configuring Time Periods

You can configure the following types of time periods in HP Release Control:

- **Change Window.** A period of time within which requests must be executed.
- **Blackout.** A period of time within which requests cannot be executed.
- **Neutral to Changes.** A period of time indicating an external event, such as a holiday, which has no direct bearing on request execution.

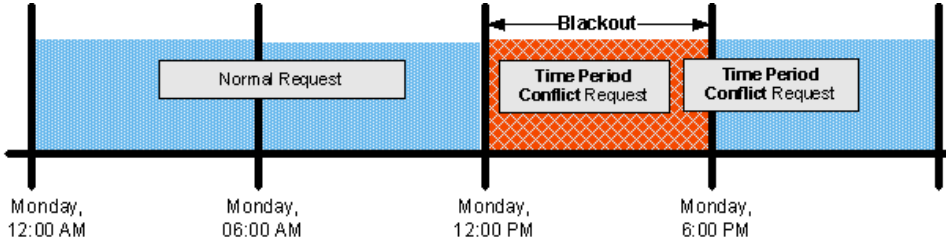
For example, to ensure that your company's service level agreements are upheld, you may define a **Change Window** time period such that changes to your corporate Web site may only take place from 12:00 AM to 6:00 AM or from 6:00 PM to 12:00 AM.

In this case, for a request to be considered **normal**, it must occur completely within a **Change Window** period. If any part of the request occurs outside the **Change Window** period, the entire request is considered to have created a Time Period Conflict.



Likewise, you may define a **Blackout** time period such that changes to the Web site may not take place on Monday mornings from 12:00 PM to 6:00 PM.

In this case, for a request to be considered **normal**, it must occur completely outside a **Blackout** period. If any part of the request occurs inside the **Blackout** period, the entire request is considered to have created a Time Period Conflict.



Configuring Time Period Settings

You configure different types of time periods and group these periods into categories in the Administration module's Time Periods tab. HP Release Control assigns processed change requests to the defined categories based on criteria that you define for each time category, as described below.

To configure time period settings:

1 Configure general time period settings.

In the Time Periods pane, select **General Settings**. Define the following properties in the right pane:

Property	Description
Time period duration	The number of days for which the time period settings should be calculated. The time periods for these days are calculated on a daily basis by HP Release Control so that the duration is always applied from the current date. For example, if you define a time period duration of 200 days, each day you log in to HP Release Control you can view the defined time periods for the following 200 days in the Analysis module's Timeline or Calendar views. Incoming requests are analyzed based on these time periods.

Property	Description
Pattern for 'Change Window' period	The background pattern that HP Release Control's Analysis module should use to display a defined Change Window period in the Timeline and Calendar views. You can select the following background patterns: ➤ **Plain.** The Analysis module displays the **Change Window** period using a solid color background. ➤ **Diagonal Lines.** The Analysis module displays the **Change Window** period using a background of diagonal lines. ➤ **Horizontal Lines.** The Analysis module displays the **Change Window** period using a background of horizontal lines. ➤ **Squares.** The Analysis module displays the **Change Window** period using a background of colored squares.
Pattern for 'Blackout' period	The background pattern that HP Release Control's Analysis module should use to display a defined **Blackout** period in the Timeline and Calendar views. You can select one of the background patterns delineated above.
Pattern for 'Neutral to Changes' period	The background pattern that HP Release Control's Analysis module should use to display a defined Neutral to Changes period in the Timeline and Calendar views. You can select one of the background patterns delineated above.

2 Configure time period categories.

In the Time Periods pane, click the **Add Time Period Category** button. A new time period category appears in the Time Periods pane.

Note: If you created time period categories in earlier versions of HP Release Control, the time period category still remains in the system but you cannot edit any of its properties. It is recommended that you delete these time period categories and create new categories based on the same properties.

Define the following properties of the new category in the right pane:

Property	Description
Name	A descriptive name for the new time period category. For example, if you are defining a category that is to include all change requests involving your corporate Web site, you might enter Corporate Web site as the name of the new time period category. This is the name with which the category will be displayed in the Change Request Filter dialog box and Change Requests pane.
Type	The type of time period —**Change Window**, **Blackout**, or **Neutral to Changes**. All rules in this category will be of this type. For explanations of each of these time period types, see page 117.
Color	The color to be assigned to the new time period category. This is the color that HP Release Control uses to display the category in the Analysis module.

Property	Description
Matching changes	The criteria by which HP Release Control determines whether a change request is included in the newly defined category. You can select one of the following two criteria: ➤ **Field.** Instructs HP Release Control to include a change request in the current category if the value you specify in the **Value** box for the field you select from the **Name** box matches the value of this field in the change request. For example, if you select **contact-person** from the **Name** box and enter Bob in the **Value** box, the change requests whose **contact-person** field contains the value of **Bob** will be included in the newly defined category. ➤ **Filter.** Instructs HP Release Control to include a change request in the current category if the request meets the criteria of the selected filter. To select a filter, click the **Select Filter** button  to the right of the **Filter** box. The Select Filter dialog box opens, enabling you to select a filter that was defined as a time period filter in the Change Request Filter dialog box (meaning the **Time period filter** check box was selected by the administrator who created the filter).

3 Configure time period recurrence rules.

In the Time Periods pane, select the category for which you want to define a recurrence rule and click the **Add Time Period Recurrence Rule** button. A new time period recurrence rule appears in the Time Periods pane. Define the following properties of the new rule in the right pane:

Property	Description
Name	A descriptive name for the new time period recurrence rule. For example, if you are defining a **Change Window** period that comprises specific weekends, you might enter weekends as the name of the new time period rule.
Recurrence pattern	The pattern for the time period's recurrence. You can choose to apply the time period once or on a daily, weekly, monthly, or yearly basis.
Recurs every X days/weeks/ months/years	If you selected a **Daily**, **Weekly**, **Monthly**, or **Yearly** pattern for the time period's recurrence, you can select the frequency with which you want the pattern to recur. For example, if you selected a **Daily** pattern for the time period's recurrence and select **3** from the **Recurs every X days** box, the time period will recur every 3 days.

Property	Description
Start time	The **Start time** options differ depending on the pattern you selected for the time period's recurrence. ➤ If you selected **Once**, enter the date and time for the time period's commencement. ➤ If you selected **Daily**, enter the time at which you want the time period to begin. ➤ If you selected **Weekly**, choose the days of the week and enter a time of day for the time period's commencement. ➤ If you selected **Monthly**, either enter a date and time, or select the week of the month, the day of the week, and the time, for the time period's commencement. ➤ If you selected **Yearly**, either enter a date and time, or select the week of the month, the day of the week, the month of the year, and the time, for the time period's commencement.
End time	The following three **End time** options exist: ➤ A text box in which you enter the date and time for the time period's completion. ➤ **On the same day at X.** You select the time of day at which you want the time period to end. ➤ **After X days at X.** You select the number of days after the start time as well as the time of day for the time period's completion. One or more of the above options may be grayed out, depending on the **Recurrence pattern** and **Start time** you selected.
Effective from	The point in time at which the rule begins to take effect. Enter a date and time of day.
Expires on/Never expires	The point in time at which the rule ceases to be in effect. Enter a date and time of day. Alternatively, you can select the **Never expires** check box if you do not want to fix a time limit for the rule's effect.

Note: You can undo your general setting, category, and rule configurations (before you save these settings) by clicking the **Refresh and Undo Modifications** button. The Time Periods tab is restored to its most recent saved settings.

---

4 Save your configuration settings.

In the Time Periods pane, click the **Save Settings for All Fields** button. A message opens asking you to confirm that you want to save your configuration settings. Bear in mind that once you save these settings, they cannot be undone. Click **Yes** to save the settings.

Note: The save process can take a few minutes. If users log in to HP Release Control during this process, they will need to refresh their Analysis views in order to view the updated time period settings.

HP Release Control calculates the compliance of the change requests that fit the configured categories with the rules pertaining to these categories.

Change requests whose execution is not planned within the configured **Change Window** periods are marked as Time Period Conflict in the Analysis module. Likewise, change requests whose execution is planned within the configured **Blackout** periods are marked as **Time Period Conflicts**. In the Analysis List and Calendar view, these requests' Summary icons are marked with red exclamation points. In the Timeline views, these requests are marked with a black frame.

Change requests whose execution is planned within the configured **Change Window** periods are marked as normal and appear with a white frame in the Timeline views.

Note: If you defined time period-related risk factors and then updated the time period settings, you must click the **Recalculate Risk** button in the Risk Factors tab to calculate risk based on the new time period settings.

12

Configuring Collision Calculations

This chapter describes how to configure the calculation of collisions between requests.

This chapter includes:

About Configuring Collisions

HP Release Control automatically identifies change requests involving common key elements, that are scheduled to take place over the same or adjacent time periods.

Change requests are defined as colliding when:

- a configuration item (CI) or business CI is involved in more than one change over the same period of time or adjacent periods of time
- the same implementor is responsible for implementing more than one change over the same period of time or adjacent periods of time
- a specified field has the same value in more than one change over the same period of time or adjacent periods of time

The severity of a collision is measured in terms of the cause of the collision and the proximity of the change requests to one another.

You can configure how HP Release Control selects which change requests to include in collision calculations, and how it identifies and calculates collisions.

This section includes:

Determining Which Change Requests to Include in Collision Calculations

You can configure HP Release Control to include only specific change requests when calculating collisions, thereby avoiding misleading results and a lot of unnecessary overhead on the system.

You can configure custom filters or predefined filters to define the criteria by which change requests will be included in the collision calculation.

This section includes:

Configuring Custom Filters for Collision Calculations

You can configure two types of global filters to define the criteria by which change requests will be included in the collision calculation:

➤ **field-value-prerequisite**. Include only change requests that have specified values for a specified field. In this case you specify a field name and values for that field. For example, you could use this filter to only include change requests with the **ticket-level** field defined as **2**. In this case, HP Release Control only calculates collisions among second-level (child) requests.

➤ **field-equality-prerequisite**. Include only change requests that have matching values for a specified field. In this case you specify a field name. For example, you could use this filter to only include change requests that have matching values for the **region** field. In this case, HP Release Control only calculates collisions among requests in the same region.

For example, assume that there are two regions, **New York** and **London**. **New York** includes requests **NY1** and **NY2** and **London** includes requests **LON1** and **LON2**. HP Release Control will calculate collisions between **NY1** and **NY2** and between **LON1** and **LON2** but it will not calculate collisions across regions, for example, between **NY1** and **LON1**.

To configure custom filters for collision calculations:

1 Open the **change-flow.settings** file (located in <**HP Release Control installation directory**>**conf**\).

2 In the <**collision-calculation**> section, include the following <**field-prerequisites**> element at the beginning of the section.

```
<field-prerequisites>
        <field-value-prerequisite>
            <field-name>ticket-level</field-name>
            <!-- For fields that define enumeration value use the enumeration name. In
            this example, '2' is the enumeration name. However, if the enumeration
            name was 'Change', you would enter 'Change' instead of '2' -->
            <values>
                <value>2</value>
            </values>
        </field-value-prerequisite>
        <field-equality-prerequisite>
            <field-name>region</field-name>
        </field-equality-prerequisite>
</field-prerequisites>
```

Within this element, you can include the <**field-value-prerequisite**> filter and the <**field-equality-prerequisite**> filter. If you include both filters, HP Release Control applies the criteria of both filters to the change requests.

3 To use the **field-value-prerequisite** filter, define the following sub-elements:

- **<field-name>.** Specify the relevant field name.
- **<values>.** Specify one or more values for the above field name.

4 To use the **field-equality-prerequisite** filter, define the **<field-name>** sub-element by specifying the relevant field name.

Configuring Predefined Filters for Collision Calculations

You can use predefined filters to filter the change requests to be included in the collision calculation based on change request status or duration.

Including Change Requests According to Status

You can determine whether to include a change request in collision calculations based on the change request status.

To select the change request statuses:

1 Open the **change-flow.settings** file (located in <**HP Release Control installation directory**>**\conf**).

2 In the <**collision-calculation**> section, locate the <**statuses**> element.

```
<collision-calculation version="4.0">
    <statuses>
        <status>PRE_APPROVAL</status>
        <status>PENDING_APPROVAL</status>
        <status>APPROVED</status>
        <status>IN_PROGRESS</status>
        <status>CLOSED</status>
    </statuses>
```

By default, change requests of all statuses are included in collision calculations.

3 To exclude change requests statuses, delete the relevant sub-elements.

For example, to exclude closed change requests, remove the sub-element containing the **CLOSED** status:

```
<status>CLOSED</status>
```

4 Save the **change-flow.settings** file.

Including Change Requests According to Duration

|You can determine whether to include a change request in collision calculations based on the change request duration. You specify a maximum acceptable change request duration. If the duration of a particular change request exceeds this value, HP Release Control does not include that change request in collision calculations.

To change the maximum duration value:

1. Open the **change-flow.settings** file (located in <**HP Release Control installation directory**>**conf**\).
2. In the <**collision-calculation**> section, locate the <**max-change-duration**> element:

```
<collision-calculation version="4.0">
.
.
<!--Changes lasting longer than this threshold (hours) will not be analyzed for collisions
    (helps ignoring collisions of long changes, and improves performance)-->
        <max-change-duration>168</max-change-duration>
```

   By default, a change request is included in collision calculations as long as its duration does not exceed 168 hours (seven days).
3. Define a new maximum duration value (in hours). To disregard change request duration, that is, if any duration is acceptable, set this value to **0**.
4. Save the **change-flow.settings** file.

Calculating Change Request Collisions

Change request collisions are calculated based on resource scheduling conflicts. If two or more change requests share a common key element, and their scheduled start and stop times overlap, or are very close to each other, these change requests are known to collide.

You customize the way in which HP Release Control identifies and calculates change request collisions in the <**collision-calculation**> section of the **change-flow.settings** file (<**HP Release Control installation directory**>**conf**\).

This section describes how to configure collision calculation properties.

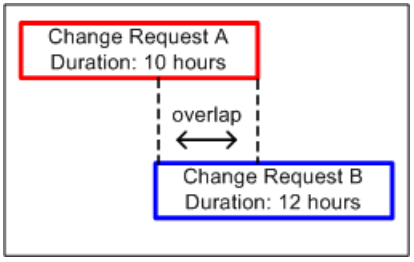
It includes:

- "Configuring Collision Proximity Levels" below
- "Configuring Causes of Collisions" on page 133
- "Configuring Collisions Severity Levels" on page 135

Configuring Collision Proximity Levels

The proximity level of two change requests can be defined as either **Overlap** or **Overlap Warning**:

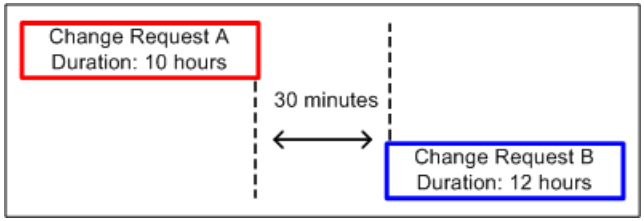
- **Overlap.** The two change requests have overlapping schedules.



- **Overlap Warning.** In reality, planned changes often exceed their original planned duration, which can result in an unforeseen overlap between two change request schedules. When two change requests are scheduled in close proximity to one another, their proximity level is defined as **Overlap Warning**.

By default, change requests are considered to be within close proximity of each other when the time gap between them is shorter than 10% of the duration of the earlier change request.

In the illustration below, the gap between the Change Request A and Change Request B is 30 minutes, which is less than 10% of the duration of Change Request A. The proximity level between the two change requests is defined as **Overlap Warning**.



You configure the definition of an **Overlap Warning** in the **<warning-ratio>** element of the **change-flow.settings** file's **<collision-calculation>** section.

```
<collision-calculation version="4.0">
   ...
    <warning-ratio>1.1</warning-ratio>
```

By setting a value for the **<warning-ratio>** element, you define the time gap according to which HP Release Control determines whether two change requests are in close proximity (proximity level of **Overlap Warning**).

The default warning ratio is **1.1**. This means that the change requests are considered to be within close proximity when the time gap between the first and second change requests is shorter than 10% of the duration of the first change request.

To increase the proximity time gap to 25% of the duration of the first change request, for example, set the warning ratio to **1.25**.

Configuring Causes of Collisions

Two change requests in close proximity to each other are not necessarily considered to collide. They could be taking place at the same time without having any effect on one another. Change requests collide only if they are in close proximity to each other AND share one of the following elements:

- **Configuration Item (CI).** Two change requests involve at least one common CI.

If a CI is changed as a direct result of a change request, it is referred to as a changed CI (CCI). If a CI is not directly involved in the change request, but may be affected as a result, it is referred to as an affected CI (ACI).

For example, if a change request involves increasing the memory on Server A, Server A is referred to as a CCI. If Host Machine B is connected to Server A, but is not directly involved in the change request, it is referred to as an ACI.

Note: If you are working with HP Release Control without HP Universal CMDB, ACIs are not detected.

- **Affected Business CI.** Two change requests affect at least one common business CI.

  If at least one of the CIs associated with a business CI is a CCI, the business CI is referred to as a directly affected business CI (DAB). If all of the CIs associated with an business CI are ACIs, the business CI is referred to as an indirectly affected business CI (IAB).

- **Implementor.** The same implementor is responsible for implementing both change requests.

- **Specified field value.** The value of a predefined or customized field that you specify is identical for both change requests.

Configuring Collisions Severity Levels

HP Release Control determines the severity of a collision based on the elements causing the collision and the proximity between the colliding change requests. By default, collision severity levels are configured as follows:

Elements Causing Collisions	Proximity Level	
	Overlap	**Overlap Warning**
CCI-CCI	Critical	Critical
CCI-ACI	High	High
ACI-ACI	None	None
DAB-DAB	High	High
IAB-DAB	Medium	Medium
IAB-IAB	Low	Low
Implementor	Medium	Very Low
<Customer-Defined> (see note below)	Customer-defined	Customer-defined

For example, if change requests share a common changed CI (**CCI-CCI**) and their proximity level is defined as **Overlap**, the severity of the collision is **Critical**.

Note:

- If there is more than one element causing a collision, the severity is determined by the collision with the highest severity.
- If you define one or more fields as collision causes, for each field you must specify the collision severity level per proximity level. For example, if you add the field **Location** as a collision cause, you must specify the collision severity for both an **Overlap** and an **Overlap Warning** related to the location.

You can change the way in which HP Release Control determines the severity level for any combination of collision cause and proximity level.

To configure collision severity levels:

1. Open the **change-flow.settings** file (located in <**HP Release Control installation directory**>**\conf**).
2. In the <**collision-calculation**> section, locate <**collision-types**>.

```
<collision-calculation version="4.0">
   ...
    <collision-types>
        <collision-type>
            <type-name>CCI_CCI</type-name>
            <proximity-severity-correlations>
                <proximity-severity-correlation>
                    <proximity>OVERLAP</proximity>
                    <severity>CRITICAL</severity>
                </proximity-severity-correlation>
                <proximity-severity-correlation>
                    <proximity>OVERLAP_WARNING</proximity>
                    <severity>CRITICAL</severity>
                </proximity-severity-correlation>
            </proximity-severity-correlations>
        </collision-type>
```

The **<collision-type>** element includes the following sub-elements:

- **<type-name>.** The element causing the collision. The following collision causes are defined by default:

Cause	Description
CCI_CCI	Two change requests involve at least one common changed CI (CCI)
CCI_ACI	The same CI is changed by one change and affected by another
ACI_ACI	Two change requests involve at least one common affected CI (ACI)
IAB_IAB	Two change requests indirectly affect at least one common business CI (IAB)
IAB-DAB	The same business CI is indirectly affected by one change and directly affected by another
DAB-DAB	Two change requests directly affect at least one common business CI (DAB)

Cause	Description
IMPLEMENTOR	The same implementor is responsible for implementing both change requests
FIELD	A specified field has the same value in both change requests. You specify the field you want to define as a collision cause using the <**field-name**> element, which is inserted directly below the <**type-name**> element. For example, to define the **Location** field as a collision cause, you would enter the following: <type-name>FIELD</type-name> <field-name>location</field-name> **Note:** ➤ You must enter the field name as it is defined in the Administration module's Field tab. For details on defining field names, see "Creating or Modifying Change Request Fields" on page 31. ➤ You can specify only those fields whose values are in numeric or short text format. ➤ Collisions are calculated based on the specified field only for new change requests entering the system or for change requests that are updated as a result of an impact analysis following the configuration of this collision cause. Change requests that already exist in the system are not included in collision calculations based on the specified field, and are not updated after configuration of this collision cause.

Caution: You can exclude a particular **type-name** from collision calculations by commenting out the <**collision-type**> element containing that **type-name**. By default, the <**collision-type**> element containing the **ACI_ACI** type-name is commented out. This means that if two change requests involve a common ACI, HP Release Control, by default, does not consider this to be a collision.

When you comment out a <**collision-type**> element, previous collision calculations based on this type are displayed in the Collisions tab, but no new collision calculations are performed based on this type. Similarly, previously defined filters including this collision type do function, but you cannot create new filters based on this collision type.

- **proximity-severity-correlations.** For each collision cause defined in the <**type-name**> element, you specify a proximity level and an associated severity level by defining the following sub-elements:
  - **proximity.** The proximity level of the colliding change requests. This can be defined as either **OVERLAP** or **OVERLAP_WARNING**. For more information about collision proximity levels, see "Configuring Collision Proximity Levels" on page 132.
  - **severity.** The severity level of the collision as outlined in the table above. The severity level can be defined as: **CRITICAL**, **HIGH**, **MEDIUM**, **LOW**, or **VERY_LOW**.

The following definition stipulates that if the cause of the collision was two change requests directly affecting a common business CI (DAB_DAB) and the proximity level of the collision was **Overlap**, then the collision severity level should be defined as **Critical**.

```
<collision-types>
    <collision-type>
        <type-name>DAB_DAB</type-name>
        <proximity-severity-correlations>
            <proximity-severity-correlation>
                <proximity>OVERLAP</proximity>
                <severity>CRITICAL</severity>
            </proximity-severity-correlation>
        </proximity-severity-correlations>
    </collision-type>
```

13

Configuring Risk Analysis

HP Release Control performs risk analysis on each change request, enabling change managers to compare change requests in terms of the risks involved in their implementation.

This chapter includes:

Understanding Risk Analysis

For each change request, HP Release Control calculates a relative risk value using the following formula:

Calculated Risk = **Potential Damage** x **Probability of Failure**

where:

- **Calculated Risk** is a relative value between 0 and 100, with a higher number indicating a higher relative level of risk. The risk value does not reflect an objective, universal risk level. Rather, it indicates the risk level of the selected change request relative to the other change requests.

- **Potential Damage** represents the potential damage that may result from the implementation of the requested change. Potential Damage is calculated as a weighted value between 0 and 10, with a higher number indicating a higher degree of damage.
- **Probability of Failure** represents the probability that the implementation of the change request will fail to some degree and cause possible damage as a result. Probability of Failure is calculated as a weighted value between 0 and 10, with a higher number indicating a higher probability of failure.

Potential Damage and Probability of Failure are calculated based on risk factors that are defined by the HP Release Control administrator during the configuration process.

For example, the administrator could define a Probability of Failure risk factor called **New_technology**, which reflects the amount of time that the technology involved in the change request has been used in the organization.

As part of creating a new risk factor, the administrator defines the source of the data (for example, a field in the integrated service desk application), defines mapping rules that translate the source data into factor values between 0 and 10, and assigns a weight to the factor.

The administrator can also define override rules for the risk calculation. For example, the administrator can determine that if the change request involves a technology that is new to the organization, the risk level is automatically set at 100, regardless of the actual risk calculation.

Example of Risk Analysis Calculation

This section provides a detailed example of the process involved in calculating the risk value for change requests.

During the configuration process, the HP Release Control administrator defines a risk factor called **New_technology**. This will be one of the factors used to measure Probability of Failure for every change request processed by HP Release Control.

The data source for the New_technology risk factor is a required field in the integrated service desk application, which reads as follows: **How long (in months) has the technology involved in this change been used in your organization?** Accepted values are any number between 1 and 36.

The administrator assigns the following mapping rules for the New_technology risk factor that translate the source data into factor values between 0 and 10:

Original Data (Range)	Factor Score
1-12 months	10
12-24 months	5
24-36 months	0

For example, if the technology was introduced 18 months ago, the New_technology risk factor receives a score of 5.

The administrator assigns a weight of 4 to the New_technology risk factor.

The administrator then defines three more risk factors to measure Probability of Failure. The following table summarizes the Probability of Failure risk factors defined by the administrator and their assigned weights:

Factor Name	Weight
New_technology	4
QA_approval	8
Affected_CIs	6
Duration_of_change	2
	Total weight = 20

After defining the risk factors used to measure Probability of Failure for each change request, the administrator performs the same process to define a separate set of risk factors that will be used to measure Potential Damage for each change request.

Now assume that a particular change request involving a fairly new technology is processed by HP Release Control and receives the following Probability of Failure risk factor scores:

Factor Name	Factor Score
New_technology	10
QA_approval	4
Affected_CIs	2
Duration_of_change	0

HP Release Control calculates a weighted value for each factor using the following formula:

```
Weight/Total Weight x Score = Weighted Value
```

where:

- **Weight** is the weight assigned to the risk factor during the HP Release Control configuration process.
- **Total Weight** is the sum of all the weights assigned to the risk factors.
- **Score** is the score of the risk factor as translated from the source data. The mapping used to translate source data into a score is defined during the HP Release Control configuration process.

Substituting the values for the New_technology risk factor (Weight=4, Total Weight=20, Factor Score=10) into this formula, you arrive at a weighted value of 2:

```
4/20 x 10 =2
```

Weighted values are calculated for all the Probability of Failure risk factors as illustrated below:

Factor Name	Factor Score	Weight	Weighted Value
New_technology	10	4	2
QA_approval	4	8	1.6
Affected_CIs	2	6	0.6
Duration of Change	0	2	0
		Total weight=20	**Probability of Failure=4.2**

The Probability of Failure score is the sum of all the weighted values and amounts to 4.2, as illustrated in the above table.

Using the same method (with separately defined risk factors), the Potential Damage score is calculated and amounts to 5.

The final risk score, calculated using the original risk analysis formula, amounts to 21:

```
Probability of Failure (4.2) X Potential Damage (5) = Calculated Risk (21)
```

As illustrated in this example, the final risk score for the change request incorporates all the risk factors which influence both the probability of failure and the potential damage of this change request.

Defining Risk Factors

You use the Administration module's Risk Factors tab to define risk factors to be used in the risk calculation. The Risk Factors tab is divided into the following sections:

- **Factors table.** Contains a list of the available risk factors. When you select a risk factor in the table, the definitions of that risk factor are displayed in the Factor Definition pane. For a risk factor to be included in the risk calculation, the check box next to the risk factor must be selected.

- **Factor weight distribution pie chart.** Displays the weight of each factor in the risk calculation.
- **Factor Definition pane.** You define the properties of each risk factor in this pane.
- **Mapping Definition section.** You define mapping rules for the selected risk factor that translate the source data into factor values between 0 and 10.

To modify or create a risk factor:

1. Above the Factors table, select either the **Damage Factors** or **Failure Probability** tab, depending on the type of risk factor you want to create or modify.
2. Select an existing risk factor from the Factors table, or click the **Add Factor** button to create a new risk factor.

3. Define or modify the following risk factor properties in the Factor Definition pane:
   - **Name.** The name of the risk factor. This is the name displayed in the Analysis module's Risk tab.
   - **Description.** A description of the risk factor to be displayed in the Potential Damage or Probability of Failure section of the Analysis module's Risk tab.
   - **Weight.** The relative weight of the risk factor to be used in the risk calculation.
   - **Source.** You can choose one of the following sources of data:
     - **Field.** A specific change request field whose data originates in the service desk application.

       Select the name of the change request field from the **Field name** list.
     - **Failure Ratio %.** The percentage of similar changes that failed.

       You configure the definition of a failed change in the **Failure outcomes** list. The **Failure outcomes** list contains the possible outcomes that can be attributed to a change. Select the outcomes by which you want to define a similar change as **failed**.

Calculation of the **Failure Ratio %** data source does not include the **Canceled** or **Unknown** statuses. For details, see "Configuring Risk Calculation Properties" on page 150.

- **Implementor Failure Ratio %.** The average failure rate for implementors who were involved with the change request.

  You configure the definition of an implementation failure in the **Failure outcomes** list. The **Failure outcomes** list contains the possible outcomes that can be attributed to a change. Select the outcomes by which you want to define an implementation as **failed**.

  Calculation of the **Implementor Failure Ratio %** data source does not include the **Canceled** or **Unknown** statuses. For details, see "Configuring Risk Calculation Properties" on page 150.

- **Planned Duration (Hours).** The planned duration of the change request (from the planned start to the planned end). This is calculated by HP Release Control.

- **Number of CCIs.** The number of CIs that will be directly affected as a result of the change request. This is calculated by HP Release Control.

- **Importance of directly affected business CIs.** The overall importance of the business CIs that are directly affected by the change. The importance level of CIs is defined in the HP Universal CMDB.

- **Importance of indirectly affected business CIs.** The overall importance of the business CIs that are indirectly affected by the change. The importance level of CIs is defined in the HP Universal CMDB.

- **Time Period Conflict Cause.** Indicates whether the the change request is scheduled to take place outside of a Change Window or inside a Blackout period.

Note: HP Release Control does not support risk factor calculations of time periods that were defined earlier than version 4.10.

- **Map by.** You can either map by range or by value. When you map by value, you map a factor value for each possible source value. When you map by range, you map a factor value for each range of source values.

4 In the **Mapping Definition** section, map the source values or ranges to risk factor values between 1 and 10.

To add a new mapping definition entry, click the **Add Entry** button and define the mapping definitions in the new row that is created in the Mapping Definition section.

5 In the **Default Mapping** list, select a default risk factor value for cases in which the field value is not mapped. To ignore the risk factor in such a case, select **Disregard**.

6 You can run test risk calculations to help you understand the implications of your risk factors before deciding whether or not to save them. For more information, see "Testing Risk Factors" on page 150.

7 Ensure that you are satisfied with all your changes.

- If you are not satisfied with your changes, you can undo any changes you made by clicking the **Refresh and Undo Modifications** button before you save your changes.

Note: When you click the **Refresh and Undo Modifications** button, all the changes you made since the last time you saved your settings are lost.

- If you are satisfied with your changes, you can commit the changes to the server by clicking the **Save Settings** button. A message opens asking you to confirm that you want to save these changes. Bear in mind that once you save these changes, they cannot be undone. Click **Yes** to save the changes.

Note: Saving the changes does not update the risk calculations. In order to update the risk calculations, see below.

You can recalculate the risk for all change requests based on your new settings by clicking the **Recalculate Risk** button. A message opens informing you of the number of change requests for which risk will be recalculated. Confirm that you want to continue recalculating the risk.

Note: If you click the **Recalculate Risk** button during the risk recalculation process, a message opens informing you of the remaining number of change requests for which risk still needs to be recalculated.

When risk factors are calculated, the risk factor's numeric value is tied to a risk level (**low**, **medium**, or **high**). To configure which numeric values correspond to which levels click the arrow on the **Risk Thresholds** button. The **Define Risk Thresholds** dialog box opens.

The green section corresponds to the **low** risk level, the yellow section to **medium**, and the red section to **high**. Drag and drop the arrows to adjust the thresholds for each level.

Testing Risk Factors

You can test risk factors before saving them by importing sample change requests and running the risk calculations on them.

To test risk factors

1 In the Test Risk Factors pane, click the **Add Sample Change Requests**  button. The Add Sample Change Requests dialog box opens.

2 Select sample change requests to test the risk factors by either selecting a filter from the drop-down menu or entering a change request ID. Click **OK** to add the change requests. If change requests are added by using the filtering option, only the first 10 requests will be displayed.

If needed, you can delete change requests from the Test Risk Factors pane  by clicking the **Delete** button.

3 To run the test on the change requests, click the **Simulate Risk Calculation**  button. The risk calculations are updated.

4 Each change request is displayed on its own row with details displayed in columns. Each risk factor, along with its calculated score, is displayed in a separate column on the right.

Configuring Risk Calculation Properties

By default, risk is calculated for change requests that have the default statuses defined in the **HP Release Control installation directory>\conf\enumerations.settings.** You can change the definitions for which risk should be calculated using the **shouldCalcRisk** function in the **HP Release Control installation directory>\conf\scripts.ext\change-flow.js** script.

For example, you can instruct HP Release Control not to calculate risk for change requests that have been approved or closed by not including these statuses in the **shouldCalcRisk** function:

```
function shouldCalcRisk(prevChangeInfo, changeInfo)
{
    status= changeInfo.getField("status");
    shouldCalc= (status==STATUS_ASSIGNED ||
status==STATUS_PENDING_APPROVAL ||status==STATUS_IN_PROGRESS);
    return shouldCalc;
}
```

If required, you can instruct HP Release Control to calculate risk for new change requests that have entered HP Release Control by including the following lines as part of the **shouldCalcRisk** function:

```
if (prevChangeInfo==null)
        shouldCalc= true;
```

You can use the **overrideRisk** function in the **change-flow.js** script to instruct HP Release Control to override the standard risk calculation. For example, you can instruct HP Release Control to assign the maximum risk value to a change request that affects a specific business CI, as the following script illustrates:

```
function overrideRisk(prevChangeInfo, changeInfo, analysis, result)
{
        if (changeInfo.getField("is-sox-app-involved").equalsIgnoreCase("Yes")){
            result.addRule("Sox Application - max risk");
            result.risk= 100;
        }
}
```

For an explanation of the objects that can be included in both the **shouldCalcRisk** and **overrideRisk** functions, refer to the **RiskAnalysis**, **RawRiskFactorCalculationResult**, and **OverrideRulesResult** classes in the **API_Reference.chm** file, located in the <**HP Release Control installation directory**>**documentation** folder.

Adding Operations Before Risk Analysis

Based on your impact analysis calculations, you may want to perform certain operations prior to every risk analysis. For example, you may want to update certain CI data prior to calculating risk if that data will affect the risk analysis.

The **preCalcRisk** function within the **<installation directory>\conf\scripts.ext\change-flow.js** script contains the location in which you can add operations to be performed before each risk analysis. By default, this function is empty, meaning that no operations are automatically performed before each risk analysis. It receives two arguments which are both writable WritableGenericRFCImpl arguments.

```
function preCalcRisk(prevChange, newChange){
}
```

For a detailed explanation of the objects that can be included in this function, refer to the **WritableGenericRFCImpl** class in the **API_Reference.chm** file, located in the **docs\pdfs** directory of the HP Release Control.

14

Configuring Similar Changes Analysis

HP Release Control automatically identifies and compares elements which are common to all change requests, and generates a list of existing changes which are found to be similar to any proposed change request.

By comparing a proposed change against this list of similar changes, you can make use of historical data to gain insight into the nature of the proposed change, and therefore better predict its likely outcome.

This chapter describes how to configure the analysis of similar changes.

This chapter includes:

Understanding How the Similarity Calculation Works

HP Release Control automatically identifies change requests involving common key elements. The definitions of these common elements are then compared to each other, and this comparison yields a proximity value. This value is always between **0** and **1** and represents the extent to which the requests are similar.

This proximity value is then compared to a threshold value which you define. This threshold value sets the minimum proximity value which will result in the compared requests being considered similar.

In other words, when the proximity value between two changes is equal to or higher than the threshold, then the changes are considered to be similar for the purposes of the Similar Changes feature. Should the proximity value be less than the threshold, then the changes are not considered to be similar.

For example, if a comparison between the common elements of **Change A** and **Change B** yields a proximity value of **0.7**, and the defined threshold for minimum similarity is **0.5**, then **Change A** and **Change B** are considered to be similar, since their proximity value is higher than the minimum value defined for similarity.

Configuring Similarity

You can customize the way in which HP Release Control identifies and calculates similar changes in the <**similarity-settings**> section of the <**HP Release Control installation directory**>**conf****similarity.settings.**

```
<settings>
        <similarity-settings>
            <threshold>0.5</threshold>
            <fields>
                <field field-name="collision-severity"/>
                <numeric-fieldfield-name="calculated-risk"zero-distance="5"/>
                <text-field field-name="description"/>
                <implementor-set/>
                <CCI-set/>
                <DAA-set/>
            </fields>
        </similarity-settings>
</settings>
```

➤ For the threshold element, you enter a value between **0** and **1**. This value defines the minimum level of proximity between requests that can be considered similar, where **0** means the requests are not at all similar, and where **1** means perfect similarity. In order for two requests to be considered similar, their proximity value must meet or exceed this threshold.

- In the elements that appear under **fields,** you define which common elements HP Release Control compares between requests. The proximity value calculation takes all these elements into account, and the final proximity value is a composite of each element's level of proximity.
  - **field name.** You can enter any string, enumeration, boolean, and so on.
  - **numeric field.** You define the range in which numeric values between changes are to be considered similar. This element is divided into two parts:
    - **name.** You enter the name of any numeric field as defined in your system settings.
    - **zero-distance.** Once you enter a numeric field, the zero distance value is the value range either side of the proposed change's field value that is considered relevant when calculating proximity.

      For example, if the numeric field is **calculated risk** and the calculated risk value of the proposed change is **10**, and the zero distance is **5**, then only other changes with calculated risk values between **5** and **15** are considered relevant for the proximity value calculation.
  - **text field.** You can enter either the **summary** or the **description** fields.
  - **implementor.** This element is pre-defined and cannot be edited.
  - **CCI.** This element is pre-defined and cannot be edited.
  - **DAA.** This element is pre-defined and cannot be edited.

15

Configuring KPI Viewing

If HP Release Control is integrated with HP Business Availability Center 8.x, you can view Key Performance Indicators (KPIs) for the CIs impacted by the selected activity. To enable KPI viewing in HP Release Control, the KPIs need to be configured as federated in HP Business Availability Center.

To configure KPIs as federated in HP Business Availability Center:

1. In HP Business Availability Center, select **Admin** > **Universal CMDB**.
2. In the **Settings** tab, click **Federated CMDB**.
3. In the **Data Stores** tab, click the **New Data Store** button.
4. In the New Data Store dialog box, from the Adapter list, select **BACKPIsAdapter**.
5. In the Connection Properties section, enter the following details:
   - **Name.** Enter a logical name for the adapter.
   - **CustomerID.** Enter **1**.
   - **Host.** Enter the name of the HP Business Availability Center machine.

   Click **Next**.
6. Select **Real Time KPI** and click **Finish**.

Note: KPI viewing is enabled by default in HP Release Control. To disable this feature, go to the **<HP Release Control installation directory>\conf\mam-integration.settings** file, and set the **kpi-enable** element to **false.**

Part IV

Configuring Collaboration and Review Settings

16

Configuring the Automatic Creation of Action Items

By default, HP Release Control automatically creates action items from certain change requests and assigns these items to specific HP Release Control users.

You can modify the conditions for the automatic creation of action items in the **<HP Release Control installation directory>\conf\scripts.ext\change-flow.js** script, using the **addActionItemsOnChange** function.

By default, the **addActionItemsOnChange** function instructs HP Release Control to compare each new change request (that is not a surrogate request) of a specified status to the version of the request that was previously collected.

If the impact severity of a change was equal or greater than a specified severity and the calculated risk increased beyond a specified threshold, HP Release Control is instructed to create an action item for the users associated with the business CIs affected by the change request.

```
function addActionItemsOnChange(prevChange, newChange, actionItemsContext){
    if(prevChange != null || newChange.getChangeCategory() ==
CHANGECATEGORY_SURROGATE) return;

    statusIsPendingApproval = newChange.getField("status") ==
STATUS_PENDING_APPROVAL;
    threshold = 0;
    riskAboveThreshold = (newChange.getField("calculated-risk") > threshold);

    if(statusIsPendingApproval && riskAboveThreshold){
        users = newChange.getAffectedUsersAboveSeverityAsArray(SEVERITY_LOW);
        for(i=0; i<users.length; i++){
            assignee = users[i];
            actionItem = newChange.createActionItem(assignee);
            actionItem.setCreator("admin");
            actionItem.setAutoClose(true);
            actionItem.setDeadlineTimeStamp(newChange.getField("planned-start-time"));
            actionItem.setActionItemPriority(ACTIONITEMPRIORITY_NORMAL);
            actionItem.setSubject("Please check the impact on this change from your side");
            actionItemsContext.addActionItem(actionItem);
        }
    }
}
```

The following properties are assigned to the action item:

- **Assignee**. By default, the user associated with the business CIs affected by the change request.
- **Creator**. By default, the HP Release Control administrator.
- **Due date**. By default, the planned start time of the new change request.
- **Priority**. By default, normal level priority.

For an explanation of the objects that can be used in the **addActionItemsOnChange** function, refer to the **GenericRFC** class in the **API_Reference.chm** file, located in the **<HP Release Control installation directory>\documentation** folder.

17

Updating Service Desk Data from HP Release Control

This chapter describes how to configure HP Release Control to send updated ticket data back to the service desk application.

This chapter includes:

Updating Service Desk Data from HP Release Control

When HP Release Control receives tickets from a service desk application, changes can be made to the tickets. Some of these changes only affect the ticket within HP Release Control. Some of the changes can be exported back to the original service desk application and update the ticket there as well.

For this update in the original service desk application to occur, HP Release Control periodically performs a two-step check to determine if the user has permission to update the data in each situation. This check involves the following decision process:

1. HP Release Control runs the **sdOperations.js** script located in the **<HP Release Control installation directory>\conf\scripts.ext** directory. This script can disable the synchronization or allow it to proceed to the second part of the check. It can be customized by the user.
2. If the script allows the check to continue, HP Release Control integrates with the service desk to check if the user has permission to perform the given activity on the service desk server. If the service desk allows the synchronization, the activity is enabled and data can be passed from HP Release Control to the service desk.

Configuring the Data Update Process

As described in the section above, updating service desk data involves a two-step check. The user has the option to disable the second part of this check, leaving only the **sdOperations.js** script to determine whether the user has permission to update a particular item.

To disable the service desk check:

1. Locate and open your service desk integration file. For more information, see the section about service desk integration files in the *HP Release Control Deployment Guide*.
2. Locate the <**operations**> tag.

   For each child <**operation**> tag of name **X**, there is a parallel <**operation**> tag of name **canX**. For example, for the **approve** operation tag, there is also a **canApprove** operation tag.

```
<operations>
        <operation name="approve">
            <operation-type>approveOperation</operation-type>
            <connector>
                <connector-type>ServiceManagerChangeApprove</connector-type>
            </connector>
            <sender-properties>
                updateOperation=true
            </sender-properties>
        </operation>
            <operation name="canApprove">
            <operation-type>canApproveOperation</operation-type>
            <connector>
                <connector-type>ServiceManagerChangeCanApprove</connector-type>
            </connector>
      </operation>
```

3. Locate the **canX** operation tag of the operation you wish to disable. In the **operation-type** tag, change the value to **alwaysCanX**. For example, change **canApproveOperation** to **alwaysCanApproveOperation** as shown below:

```
<operation-type>alwaysCanApproveOperation</operation-type>
```

Request Approval

You can configure HP Release Control to allow users to approve change requests or retract the approval of change requests.

If you are working with any of the following service desk applications, the approval of requests within HP Release Control results in an updated status of the request within the service desk application:

- HP ServiceCenter 6.x / HP Service Manager 7.x
- HP Project and Portfolio Management 7.x / IT Governance Center Web Services 6.x

If you are not working with one of the above service desk applications, you can configure request approval in HP Release Control, but the approval status of the request will not be updated in the service desk application.

You configure request approval based on the service desk application you are using:

- If you are using HP Service Manager 7.x, request approval is configured as part of the HP Service Manager configuration process. For more information, see Chapter 3, "Configuring HP Service Manager/Center."
- If you are using HP ServiceCenter 6.x, see "Configuring Request Approval with HP ServiceCenter" on page 167.
- If you are using HP Project and Portfolio Management 7.x/ IT Governance Center Web Services 6.x, see "Configuring Request Approval with HP Project and Portfolio Management" on page 169.
- If you are using other service desk applications, see "Configuring Request Approval Without Updating the Service Desk" on page 172.

Note: To check whether your service desk application supports this feature, contact Customer Support.

Configuring Request Approval with HP ServiceCenter

This section describes how to configure change request approval if you are working with HP ServiceCenter 6.x.

Note: The procedures in this section should be completed as part of the HP ServiceCenter configuration process. For more information see "Configuring HP Service Manager/Center" on page 45.

To configure change request approval with HP ServiceCenter:

1. Assign the role of **Change Approver** to the users who are meant to approve requests. For details, see "Configuring User Settings" on page 196.
2. Configure both HP Release Control and HP ServiceCenter to check whether a request can be approved. For details, see "Enabling the Possibility of Request Approval" below.

Enabling the Possibility of Request Approval

Before performing a request approval or approval retraction operation, HP Release Control and your service desk application must determine that the request can, in fact, be approved (or approval retracted) at the current time by the current user.

You configure HP ServiceCenter to allow HP Release Control to check whether requests can be approved, and whether an approval can be retracted. This configuration should be performed by the HP ServiceCenter administrator.

Note: If you are using HP Service Manager, this procedure is performed automatically by the **sdiConfigurer.bat** utility.

To enable the possibility of request approval in HP ServiceCenter:

1 Load HP ServiceCenter's **can_approve_operations_62.unl** unload file, located in the **<HP Release Control installation directory>\bin\result \extensions** directory. (For details on loading unload files, refer to the HP ServiceCenter documentation.)

When you deploy this unload file, the **ccm.check.retract** and **ccm.check.approval** processes are created in HP ServiceCenter.

2 Associate a display action with each of the two new processes, **ccm.check.approval** and **ccm.check.retract**:

a Open the Document Engine in HP ServiceCenter by navigating to **Menu navigation** > **Utilities** > **Tools** > **Document Engine.**

b In the **Objects** menu, in the **File Name** box, type **cm3r**.

c In the **Object Info** tab, next to the **Default State** box, click the **Find** button and add the following values to the table.

Display Action	Process Name	Condition
checkapproval	ccm.check.approval	true
checkretract	ccm.check.retract	true

3 In WSDL Configuration, add the approval and retraction actions:

a Open the WSDL Configuration tool in HP ServiceCenter by navigating to **Menu navigation** > **Toolkit** > **WSDL Configuration.**

b In the **Name** box, type **cm3r**.

c Add the following actions:

Allowed Action	Action Name
checkapproval	CanApprove
checkretract	CanRetract

d Click **OK**

e Open the WSDL Configuration tool in HP ServiceCenter by navigating to **Menu navigation** > **Toolkit** > **WSDL Configuration.**

f In the **Name** box, type **cm3t.**

g Add the following actions:

Allowed Action	Action Name
checkapproval	CanApprove
checkretract	CanRetract

h Click **OK**

Configuring Request Approval with HP Project and Portfolio Management

This section describes how to configure change request approval if you are working with HP Project and Portfolio Management 7.x / IT Governance Center Web Services 6.x.

To configure change request approval with HP Project and Portfolio Management (IT Governance Center) Web Services:

1 Assign the role of **Change Approver** to the users who are meant to approve requests. For details, see "Configuring User Settings" on page 196.

2 The **sdOperations.js** script is located in the **<HP Release Control installation directory>\conf\scripts.ext** directory. It defines the rules for allowing/denying users permission to approve changes in the HP Project and Portfolio Management server. It is recommended that you configure this script to suit your needs.

3 Configure both HP Release Control and HP Project and Portfolio Management/IT Governance Center to perform request approval. For details, see "Enabling the Execution of Request Approval (HP Project and Portfolio Management)" on page 170.

Enabling the Execution of Request Approval (HP Project and Portfolio Management)

Before you configure request approval, make sure that:

- The user with which you instruct HP Release Control to connect to the HP Project and Portfolio Management/IT Governance Center database has write permissions to the database.
- Your HP Project and Portfolio Management/IT Governance Center Web Services workflow contains a transition from the **Approved** step to the **Pending Approval** step.

You configure HP Release Control to approve requests/retract approvals within the adapter configuration file.

To configure HP Release Control to approve/retract a request:

1. Open the adapter configuration file (by default, **itg-ws-adapter.settings** for HP Project and Portfolio Management / IT Governance Center Web Services).
2. Locate the **approve** and **retract** operations and ensure that the appropriate service desk application connectors are included in the appropriate **<connector-type>** elements:
   - To enable the approval of change requests, ensure that **<connector-type>itgApprove</connector-type>** is included in an **approve** operation
   - To enable the retraction of change request approvals, ensure that **<connector-type>itgRetract</connector-type>** is included in a **retract** operation

3 Define the following properties within the <**properties**> element:

Property Name	Description	Default Value
dbUrl (mandatory)	The URL of the HP Project and Portfolio Management/ IT Governance Center database.	—
username (mandatory)	The user name with which HP Release Control connects to the HP Project and Portfolio Management / IT Governance Center database.	—
password (mandatory)	The password with which HP Release Control connects to the HP Project and Portfolio Management / IT Governance Center database. **Note:** The password should be encrypted. For details on encrypting passwords, see Appendix A, "Password Encryption."	—
driverClassName (mandatory)	The name of the JDBC driver. Do not modify the default value.	**oracle.jdbc. OracleDriver**
sourceStepSequence (mandatory)	The source step number from which approval is performed. Either this or the **sourceStepName** must be provided. For sub-workflows, specify <parent workflow step>.<sub-workflow step>. For example, **5.5.**	—

Property Name	Description	Default Value
sourceStepName (mandatory)	The name of the source step from which approval is performed. Either this or the **sourceStepSequence** must be provided.	—
actionName (mandatory)	The action that must be performed within the HP Project and Portfolio Management/IT Governance Center application in order for the request to be approved.	—

4 To ensure that the updated approved requests/retracted approvals are of a high priority in the queue of requests being sent to HP Release Control, specify **updateOperation=true** within the **<sender-properties>** element.

5 Save the changes you made to the adapter configuration file.

6 Reload the adapter configuration file by clicking the **Reload Adapters** button in the Administrator module's **Fields** tab.

Configuring Request Approval Without Updating the Service Desk

This section describes how to configure change request approval if you are working with service desks other than HP Service Center 6.x / HP Service Manager 7.x or HP Project and Portfolio Management 7.x / IT Governance Center Web Services 6.x.

To configure change request approval:

1 Open the relevant service desk adapter configuration file.

2 Configure HP Release Control to check whether a request can be approved.

a In the adapter configuration file, include the following operation in the operations section:

```
<operation name="canApprove">
        <operation-type>alwaysCanApproveOperation</operation-type>
</operation>
```

b Configure the **canApprove** function in the <**HP Release Control installation directory**>**conf****scripts.ext****sdOperations.js** script. For example:

```
function canApprove(genericRFC, userLoginName) {

        var status = genericRFC.getField("status");
        return (status == STATUS_PENDING_APPROVAL);

}
```

For a detailed explanation of the objects that can be included in this function, refer to the **API_Reference.chm** file, located in the <**HP Release Control installation directory**>**documentation** folder.

3 Configure HP Release Control to check whether approval for a request can be retracted.

a In the adapter configuration file, include the following operation in the **operations** section:

```
<operation name="canRetract">
        <operation-type>alwaysCanRetractOperation</operation-type>
</operation>
```

b Configure the **canRetract** function in the <**HP Release Control installation directory**>**conf****scripts.ext****sdOperations.js** script. For example:

```
function canRetract(genericRFC, userLoginName) {

        var status = genericRFC.getField("status");
        return (status == STATUS_APPROVED);

}
```

For a detailed explanation of the objects that can be included in this function, refer to the **API_Reference.chm** file, located in the <**HP Release Control installation directory**>**documentation** folder.

4 Configure HP Release Control to perform request approval.

a In the adapter configuration file, include the following operation in the **operations** section:

```
        <operation name="approve">
            <operation-type>approveOperation</operation-type>
            <properties>
   refetchTicket=false
</properties>
            <connector>
                <connector-type>approveScriptingConnector</connector-type>
            <properties>
                scripts=approveRetractChange.js
                functionName=approve
</properties>
            </connector>
            <sender-properties>
                updateOperation=false
            </sender-properties>
        </operation>
```

b Configure the **approve** function in a script named **approveRetractChange.js**. For example:

```
function approve(ticket, userName, comment) {

        ticket.setField("status", STATUS_APPROVED);

}
```

c Save the script in the <**HP Release Control installation directory**>**conf**\<**adapter_name**>**.ext** directory.

For a detailed explanation of the objects that can be included in this function, refer to the **API_Reference.chm** file, located in the <**HP Release Control installation directory**>**documentation** folder.

5 Configure HP Release Control to retract approved requests.

a In the adapter configuration file, include the following operation in the **operations** section:

```
        <operation name="retract">
            <operation-type>retractOperation</operation-type>
            <properties>
   refetchTicket=false
</properties>
            <connector>
                <connector-type>retractScriptingConnector</connector-type>
            <properties>
                scripts=approveRetractChange.js
                functionName=retract
</properties>
            </connector>
            <sender-properties>
                updateOperation=false
            </sender-properties>
        </operation>
```

b Configure the **retract** function in a script named **approveRetractChange.js**. For example:

```
function retract(ticket) {

        ticket.setField("status", STATUS_PENDING_APPROVAL);

}
```

c Save the script in the <**HP Release Control installation directory**>**conf**\<**adapter_name**>.**ext** directory.

For a detailed explanation of the objects that can be included in this function, refer to the **API_Reference.chm** file, located in the <**HP Release Control installation directory**>**documentation** folder.

6 Save the adapter configuration file.

7 Reload the adapter configuration file by clicking the **Reload Adapters** button in the Administrator module's **Fields** tab.

8 Assign the role of **Change Approver** to the users who are meant to approve requests. For details, see "Configuring User Settings" on page 196.

Caution: Make sure that the approval status of the request is not overwritten in the service desk, when the service desk is synchronized with HP Release Control. You can do this by including the following function in the <**HP Release Control installation directory**>**conf****scripts.ext****change-flow.js** script:

```
function preChangeProcess(prevChange, newChange) {
   if (prevChange.getField("status") == STATUS_APPROVED) {
  newChange.setField("status", STATUS_APPROVED);
}
```

For a detailed explanation of the objects that can be included in this function, refer to the **API_Reference.chm** file, located in the <**HP Release Control installation directory**>**documentation** folder.

18

Configuring Notifications

This chapter describes how to configure the sending of notifications from HP Release Control.

This chapter includes:

About Configuring Notifications

By default, only automatic email notifications and not customized notifications are sent by HP Release Control. It is recommended, however, that you configure notifications to be sent to users who do not regularly work with HP Release Control and are therefore unlikely to view and monitor action items that are created as a result of an impact analysis. Using customized email notifications, you can inform these users of change requests that negatively affect the applications with which they are associated. You define the circumstances under which customized notifications should be sent as well as the notification recipients in the **<HP Release Control installation directory>\conf\scripts.ext\change-flow.js** script, using the **getUsersToNotify** function.

You enable/disable the notification feature and configure other notification properties in the **<notifications>** section of the **<HP Release Control installation directory>\conf\change-flow.settings** file.

You configure the format of the notifications being sent in the FTL files located in the **<HP Release Control installation directory>\conf\notifications.ext** directory. For more information, see "Configuring the Format of Emails" on page 219.

Configuring Notification Rules

You use the **getUsersToNotify** function in the **<HP Release Control installation directory>\conf\scripts.ext\change-flow.js** script to define the following:

- the circumstances under which notifications should be sent
- the recipients of the notifications
- the content of the notification messages

When enabled, the **getUsersToNotify** function, by default, instructs HP Release Control to compare each new change request of a specified status to the version of the request that was previously collected and ascertain whether the calculated risk increased beyond a specified threshold.

```
function getUsersToNotify(prevChange, newChange, notificationContext) {


    statusIsPendingApproval = (newChange.getField("status") ==
                        STATUS_PENDING_APPROVAL);

    message = "";
    riskStatusStr = "is ";

    riskIncreased = true;

    if (prevChange != null) {
        riskIncreased = (newChange.getField("calculated-risk") >
                    prevChange.getField("calculated-risk"));
        if (riskIncreased) {
            riskStatusStr = "has increased to ";
        }
    }

    threshold = 0;
    riskAboveThreshold = (newChange.getField("calculated-risk") > threshold);
```

Note: For details on risk calculations, see "Configuring Risk Analysis" on page 141.

If the calculated risk did increase beyond the specified threshold, the default version of the **getUsersToNotify** function instructs HP Release Control to notify all the users associated with the affected applications whose impact severity level exceeded the specified level.

```
 if (statusIsPendingApproval && riskIncreased && riskAboveThreshold) {
     message = "The current status of the request is " +
             newChange.getField("status").name +
             " and the calculated risk level of the request " +
             riskStatusStr +
             " " +
             newChange.getField("calculated-risk") +
             ".";
// Add affected users for this change request while Severity is greater than 0
(VERY_LOW).
// To get all affected users send -1 on: newChange.getAffectedusers()
notificationContext.addUsers(newChange.getAffectedUsersAboveSeverity(SEVERITY
_LOW));
```

If there are no users associated with these applications, the default version of the **getUsersToNotify** function instructs HP Release Control to notify the administrator.

```
 } else {
     notificationContext.addUsersByRole("Administrator");
     message = "HP Change Control Management has not identified specific users that"
+
             "will be notified regarding this request. " +
             "You are receiving this notification due to your role" +
             "as an HP Change Control Management administrator.\n" +
             message;
     }
```

For an explanation of the objects that can be used in the **getUsersToNotify** function, refer to the **notificationContext** and **GenericRFC** classes in the **API_Reference.chm** file, located in the **<HP Release Control installation directory>\documentation** folder.

Configuring Other Notification Properties

By default, the notification feature is enabled. You can disable this feature and modify the notification sender and frequency in the **<notifications>** section of the **<HP Release Control installation directory>\conf\change-flow.settings** file.

To disable the HP Release Control notification mechanism:

➤ Change the value of the **<send-notification-email-enabled>** element to **false**. When you change the value of this element, no notifications are sent by HP Release Control.

To modify the notification sender:

➤ Enter a different value for the **<notification-sender-email>** element.

To modify notification frequency:

➤ Change the value of the **<send-notifications-frequency>** element (in seconds) as required.

19

Configuring Post Implementation Review

This chapter describes how to configure settings related to the Post Implementation Review (PIR) feature.

This chapter includes:

About Configuring Post Implementation Review

The Post Implementation Review (PIR) feature allows the Change Reviewer to add review notes to any change request with **Evaluation and Closure** status. The review notes present the conclusions regarding the request and provide information about its overall success and satisfaction levels of relevant parties.

If you are working with HP Service Manager/ServiceCenter, you can synchronize PIR information directly to that application, and synchronize information from HP Service Manager / ServiceCenter to HP Release Control.

- To configure PIR enumeration fields, see "Configuring Enumeration Field Display Settings" on page 227.
- To configure HP Release Control to update HP Service Manager with PIR information, see "Updating HP Service Manager/ServiceCenter with Ticket Review Data" below.

Updating HP Service Manager/ServiceCenter with Ticket Review Data

You can configure HP Release Control to update HP Service Manager/ ServiceCenter with ticket review data. HP Release Control uses the **canUpdateReview** and **reviewUpdate** operations to enable this feature.

The **reviewUpdate** operation is responsible for the actual mapping of the review data. It includes the **updateOperations.js** script that maps the HP Release Control fields to the HP Service Manager/ServiceCenter fields. Specifically, it updates the outcome of the change or task, together with any review comments and the time of the review.

The **canUpdateReview** operation enables the feature in HP Release Control.

To enable updates to HP Service Manager:

1. Open the adapter configuration file (by default, **servicemanager-ws-adapter.settings**).
2. Ensure that the **reviewUpdate** operation exists under the <**operations**> element:

```
<operation name="reviewUpdate">
        <operation-type>reviewUpdateOperation</operation-type>
        <connector>
            <connector-type>ServiceCenterChangeUpdate</connector-type>
            <properties>
                scriptName=updateOperations.js
                methodName=updateChangeReview
            </properties>
        </connector>
    </operation>
```

where <**connector-type**> is defined as:

- **ServiceCenterChangeUpdate/ServiceManagerChangeUpdate** for top-level (parent) change requests
- **ServiceCenterTaskUpdate/ServiceManagerTaskUpdate** for second-level (child) change requests

and where the **updateOperations.js** script calls:

- the **updateChangeReview** method for top-level (parent) change requests
- the **updateTaskReview** method for second-level (child) change requests

3 If you are working with HP ServiceCenter, ensure that the **canUpdateReview** operation is defined under the <**operations**> element as follows:

```
<operation name="canUpdateReview">
    <operation-type>alwaysCanUpdateReviewOperation</operation-type>
</operation>
```

4 If you are working with HP Service Manager, ensure that the **canUpdateReview** operation is defined under the <**operations**> element as follows:

```
<operation name="canUpdateReview">
    <operation-type>canUpdateReviewOperation</operation-type>
  <connector>
     <connector-type>ServiceManagerChangeCanUpdate</connector-type>
  </connector>
</operation>
```

5 Save the adapter configuration file, and restart the HP Release Control service.

20

Configuring Latent and Detected Changes

HP Release Control contains all the changes that are scheduled to take place in your environment.

If you are working with HP Universal CMDB, you can configure it to periodically discover actual changes to your environment and send data about these changes to HP Release Control.

The latent change feature enables you to determine whether changes discovered in your environment (**discovered changes**) correspond to changes that were already scheduled in HP Release Control (**scheduled changes**).

This chapter includes:

Understanding Latent and Detected Changes

Caution: There are different ways that you can work with the latent change feature. This section assumes that the latent change feature is fully activated (**latent-and-detected** mode). For more information about the different work modes, see "Configuring Latent Change Feature Properties" on page 190.

When a change is discovered, HP Release Control tries to match the discovered change with scheduled changes according to the following criteria:

- **Time period.** HP Release Control checks whether the discovered change took place during the same time period as a scheduled change.

  Regarding the time period of the scheduled change, HP Release Control first checks the actual time of the scheduled change (this is established by the service desk or the Traffic Control module). If there is no actual time recorded, it checks the planned time.

- **CCI/Grouper CI.** If the discovered change took place during the same time period as a scheduled change, HP Release Control checks whether changed CI (CCI) in the discovered change is the same as the scheduled change. If the CCI's are not the same, HP Release Control checks to see if they are linked to a common Grouper CI (for example, the same host).

- **Change type.** If the discovered change and a scheduled change share the above criteria (time and Grouper CI), HP Release Control checks whether the discovered change and the scheduled change are of the same change type. The change type can be one that involves adding either hardware or software.

  The type of the discovered change is determined by the **change-type** category (**HW_ADD** or **SW_ADD** within the **mam-integration.settings** file) in which the CIT of the discovered change is included. The type of the scheduled change is determined by the information in the scheduled change's **change-types-orig** field, which can contain the value of either **HW_ADD** or **SW_ADD**.

Note:

- To enable HP Release Control to use the change type criterion, you need to have a field in your service desk application in which you identify the change request's change type. You then need to map this field to the possible values—**HW_ADD** or **SW_ADD**—in the **change-types-orig** field. For more information about converting and mapping service desk application fields, see the section about configuring and converting requests in the *HP Release Control Deployment Guide*.
- To enable HP Release Control to check whether changed CIs (CCIs) in the discovered change and in the scheduled change are linked to a common CIT, you must ensure that at least one of the following attributes is selected for each CIT within HP Universal CMDB: **Change Monitored**, **Comparable**, **Asset Data**.

Handling the Discovered Change

HP Release Control handles the discovered change in one of the following ways, depending on the extent to which the above matching criteria were met:

- **HP Release Control displays the change as a detected change.**

  When a discovered change matches a scheduled change according to all of the above criteria (time, CCI/grouper CI, and change type), it is defined by HP Release Control as a **detected change**. Detected changes are displayed with the corresponding change request in the Analysis module's Detected Changes tab.

➤ **HP Release Control displays the change as a latent change.**

When a discovered change does not match any scheduled change, or if it only matches the scheduled change according to some of the above criteria, it is defined by HP Release Control as a **latent change**.

Note: The exception to this rule is when the change type is unknown. For more information, see **HP Release Control disregards the change** below.

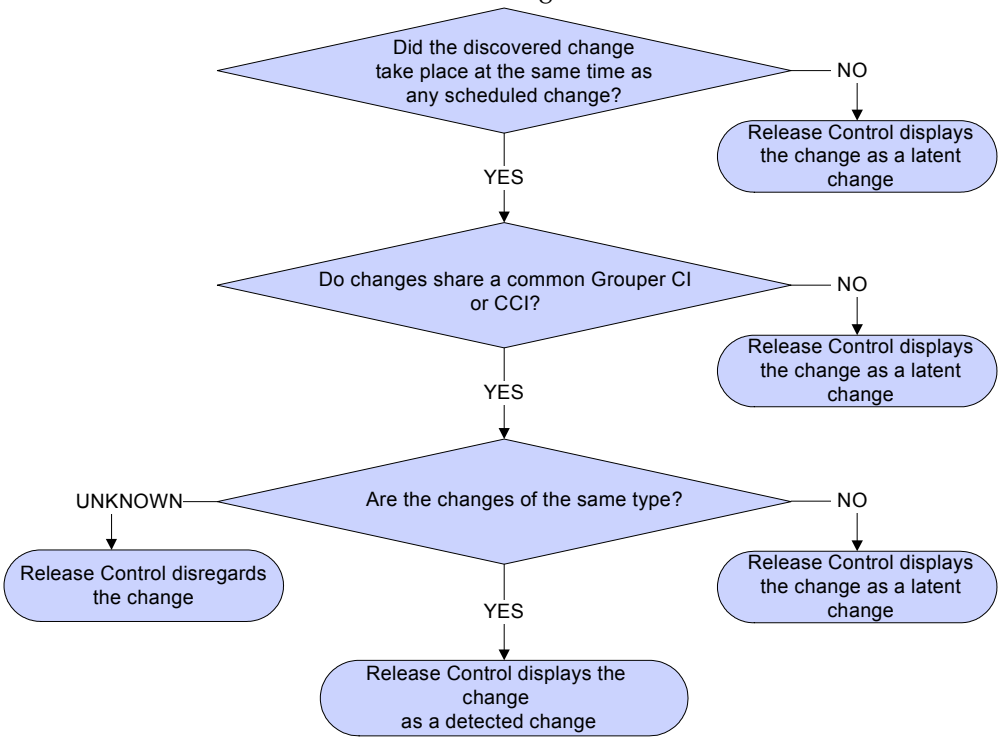
For example, if the discovered change took place during the same period as the scheduled change but they do not share a common Grouper CI, the discovered change is defined as latent.

Latent changes are displayed as separate changes in the Analysis module's Change Requests pane.

➤ **HP Release Control disregards the change.**

If the discovered change matches the scheduled change according to the first two criteria (time and CCI/Grouper CI), but the scheduled change does not include information regarding its **change type** (meaning that the change type is unknown), HP Release Control will disregard the discovered change and the change will not be displayed.

The following flow chart summarizes the way in which HP Release Control handles a discovered change:



Example

Assume, for example, that **NewChange** is the name of a discovered change that was detected by HP Universal CMDB and **CCMrequest1**, **CCMrequest2**, and **CCMrequest3** are all the scheduled changes included in HP Release Control.

HP Release Control tries to match the discovered change, **NewChange**, with existing scheduled changes (**CCMrequest1**, **CCMrequest2**, and **CCMrequest3**) according to the criteria described above.

If **NewChange** and **CCMrequest2** took place over the same time period, HP Release Control checks whether **NewChange** and **CCMrequest2** have identical CIs. If they do not have identical CI's, HP Release Control checks to see if they link to a common Grouper CI. If they do, HP Release Control checks the change type.

- If **NewChange** and **CCMrequest2** have the same change type (both involve adding hardware), **NewChange** is defined as a **detected change**.
- If **NewChange** and **CCMrequest2** have different change types (one involves adding hardware and one involves adding software), **NewChange** is defined as a **latent change**.
- If HP Release Control cannot identify the change type of **CCMrequest2**, then **NewChange** is disregarded and is not displayed anywhere.

Configuring Latent Change Feature Properties

You configure the latent change feature in the **<latent-changes>** section of the **HP Release Control installation directory>\conf\mam-integration.settings** file.

The following is an example of the code displaying the configurable elements:

```
<latent-changes-mode>disabled</latent-changes-mode>
   <!-- get detected changes every night at 4 AM -->
<detect-changes-schedule>0 0 4 * * ?</detect-changes-schedule>
<detect-changes-duration-in-hours>24</detect-changes-duration-in-hours>
<detect-changes-recovery-duration-in-hours>720
</detect-changes-recovery-duration-in-hours>
<latent-change-level>1</latent-change-level>
<latent-change-ref-id>
   <initial-counter-value>1</initial-counter-value>
   <format>L-{0,number,#0000000000.###}</format>
```

- **<latent-changes-mode>.** You choose how to work with the latent change feature by defining a value for this element. You can define one of the following values:

Value	Description
disabled	The latent change feature is inactivated. HP Release Control does not receive information about new changes in your environment. This is the default setting.

Value	Description
latent-and-detected	The latent change feature is fully activated. Latent and detected changes are displayed according to the criteria described in "Understanding Latent and Detected Changes" on page 185.
latent-consider-change-types	The latent change feature is partially activated. Detected changes are ignored and latent changes are displayed. Latent changes detected in your environment are displayed according to the criteria described in "Understanding Latent and Detected Changes" on page 185.
latent-ignore-change-types	The latent change feature is partially activated. Detected changes are ignored and latent changes are displayed. In this mode, the **change type** criteria is not taken into account when identifying latent changes. The difference between **latent-ignore-change-types** mode and **latent-consider-change-types** mode can be illustrated in the following example: If a discovered change matches one of the scheduled changes according to the first two criteria (time and CCI/Grouper CI) but the change types are different, then: ➤ in **latent-ignore-change-types** mode, the change would not be defined as latent. ➤ in **latent-consider-change-types** mode, the change would be defined as latent.

- **<detect-changes-schedule>.** Define the schedule for HP Release Control's request of information from HP Universal CMDB about newly discovered changes. This value is entered as a cron expression.
- **<detect-changes-duration-in-hours>.** Define the block of time for which HP Release Control requests information from HP Universal CMDB about newly discovered changes.

- **<detect-changes-recovery-duration-in-hours>.** When the HP Release Control server starts up, it searches for cases in which there were problems encountered during the calculation of detected changes (for example, if the server stopped during the calculation process). In this element, you define how far back in time HP Release Control should search for such problem cases. The default setting is one month.
- **<latent-change-level>.** Latent changes are displayed as separate changes in the Analysis module. Define whether you want latent changes to be displayed as top-level (parent) change requests or second-level (child) requests.
- **<latent-change-ref-id>.** Latent changes are displayed as separate changes in the Analysis module. Define a format for the request ID assigned to the latent changes by defining a value for the following sub-elements:
  - **<initial-counter-value>.** The number that will be included in the Request ID for the first latent change recorded in your system.
  - **<format>.** The format of the latent change request ID.
- **<detected-changes-query>.** HP Release Control uses the **ccmDetectedChangesRule** TQL query to describe the types of CIs which should be checked for changes. Each CI type must be linked to its Grouper CI as well.

Note: All nodes in the TQL must be set to visible (property visible = true).

For more information about TQL queries, refer to the HP Universal CMDB documentation.

Part V

User Management

21

Configuring User Settings

This chapter describes how to configure user settings.

This chapter includes:

Configuring Users

You configure user settings for new HP Release Control users, edit the settings of existing users, and delete users in the Administrator module's Users tab.

This section includes:

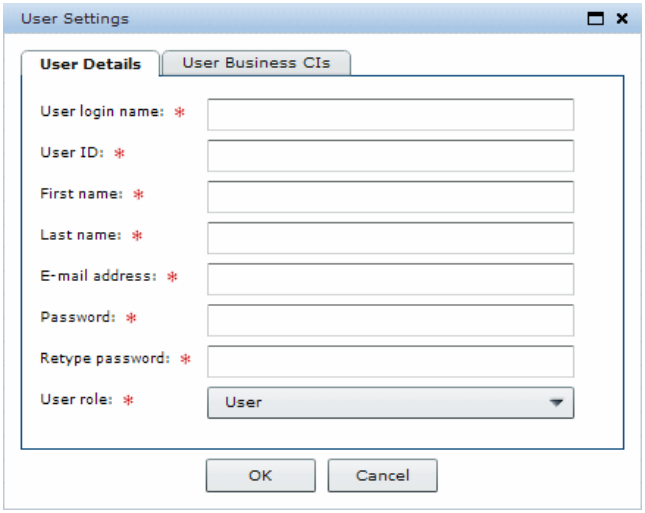
Configuring User Settings

You define a new user by configuring settings—including basic user details and associated business CIs—for the user.

Note: If you are working in identity management mode, you cannot add users in the Administrator module. For details on working in identity management mode, see "Using Identity Management" on page 204.

To configure user settings:

1 In the Administrator module's **Users** tab, click the **New** button in the top left corner. The User Settings dialog box opens.



2 Enter the following user settings:

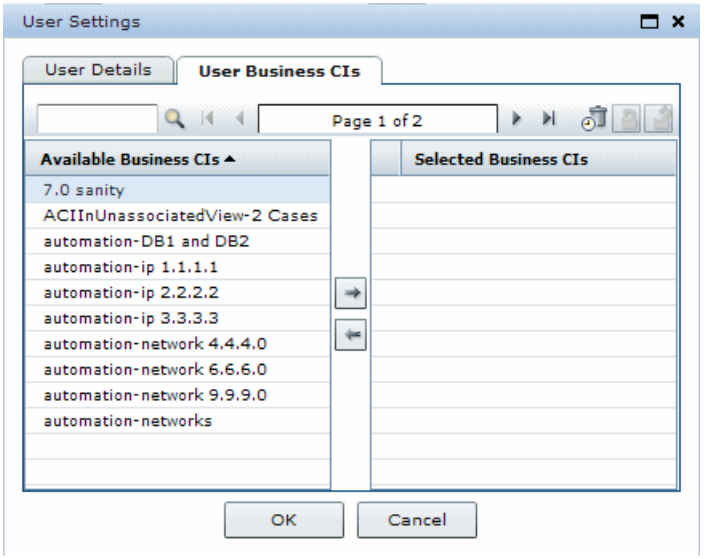
Column	Description
User login name	The user name by which the user will be able to log in to HP Release Control.
User ID	The user's login ID, where applicable.

Column	Description
First name	The first name of the user you are defining.
Last name	The last name of the user you are defining.
Email address	The email address of the user you are defining. This is the email address to which notifications will be sent for this user.
Password	The password by which the user will be able to log in to HP Release Control.
Retype password	Confirms the password entered in the previous box.

3 From the **User role** box, select one of the following options:

Role	Permissions
Administrator	Can perform all functions
Change Approver	Can approve change requests or retract an approved change request
Change Manager	Can create and send CAB minutes and invitations
Change Reviewer	Can create and edit Post Implementation Reviews (PIR), and send PIR minutes and invitations
Guest	None
NOC	Can perform any action in the Director module, such as changing the state of a change request, dismissing alerts, and rescheduling change requests
Similarity Teacher	Can use the Similar Changes feature to teach similarity
User	Can perform all functions other than those specified in other roles

4 To associate business CIs with the user you are defining, click the **User Business CIs** tab.



5 In the **Available Business CIs** list, select the business CIs you want to associate with the user. If the list of available business CIs is lengthy, you can use the search box to display only those business CIs that match the text you enter in the search box. In addition, you can use the **First**, **Previous**, **Next**, and **Last** buttons to locate a business CI. You can select multiple business CIs using the CTRL key.

6 Click the right arrow to move the business CIs to the **Selected Business CIs** list.

7 To ensure that the user will not be able to remove the association with a specific business CI, select the business CI and click the **Enforce Business CI** button.

To restore the user's ability to remove the association with this business CI, select the business CI and click the **Stop Enforcing Business CI** button.

8 Click **OK** to save your settings and close the User Settings dialog box. The new user is added to the HP Release Control database and is listed in the Users tab.

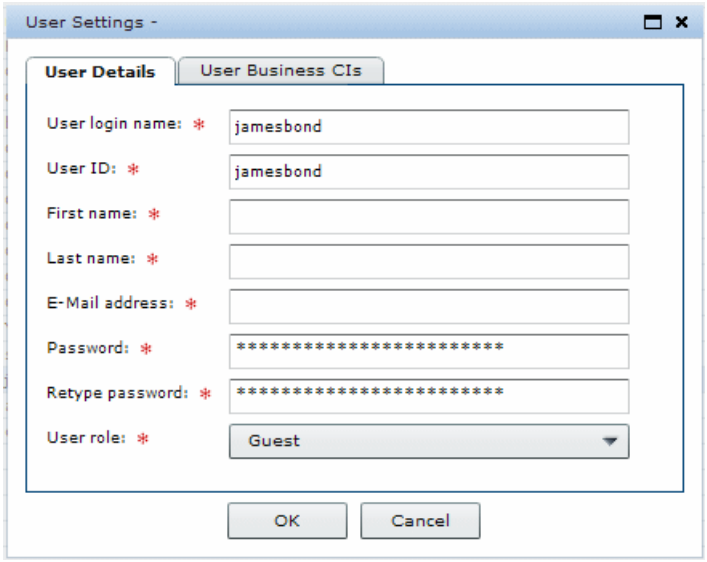
Modifying User Settings

As an administrator, you can modify the settings of an existing HP Release Control user.

To modify user settings:

1 In the Administrator module's **Users** tab, select the user whose settings you want to modify. If the list of users is lengthy, you can use the search box and/or the **First**, **Previous**, **Next**, and **Last** buttons to locate a user.

2 Click the **Edit** button in the top left corner. The User Settings – <Name of User> dialog box opens.



3 Modify the user details and the business CIs associated with the user as required. For a description of user settings, see "Configuring User Settings" on page 196.

Note: If you are working in identity management mode, you cannot modify the user's login name, password, first name, last name, or email address. For details on working in identity management mode, see "Using Identity Management" on page 204.

---

4 Click **OK** to save your changes and close the User Settings – <Name of User> dialog box.

Deleting Users

You can delete any previously defined HP Release Control users.

To delete users:

1 In the Administrator module's **Users** tab, select the users you want to delete and click the **Delete** button in the top left corner.

2 Click **Yes** to confirm deletion. HP Release Control deletes the users from the database.

Configuring User Name and Password Constraints

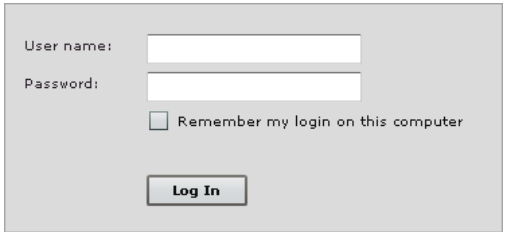
You can configure the following HP Release Control business CI user name and password constraints and properties in the **<HP Release Control installation directory>\conf\ analysis-app-module.settings** file:

- **minimum length.** Specify the minimum number of characters the user name/password can contain. By default, a user name/password must contain at least one character.
- **maximum length.** Specify the maximum number of characters the user name/password can contain. This number must be greater than 25, and is set to 50 by default.

- **pattern.** Using regular expressions, specify the characters that each user name/password can contain. For example, use the following expression to indicate that a user name/password can be any upper-case or lower-case letter, as well as any digit: ^[A-Z,a-z,0-9]$
- **pattern error message.** Specify the type of error message to be displayed if the user name/password contains a character that is not allowed. You can enter the error text itself here, or **properties-file** if you want to reference a properties file for the error message. If you reference a properties file, the error message text itself should be written in the **onyxCommonResources.properties** file.

Configuring User Login Settings

When users log in to HP Release Control from the opening page, they can select **Remember my login on this computer** so that the next time they log in from the same computer, they do not need to enter a user name and password.



You can disable the **Remember my login on this computer** option in the **<HP Release Control installation directory>\conf\ security.settings** file by setting the value of the **<remember-me-enabled>** element to **false** and then restarting the HP Release Control server.

```
<settings>
    <session-settings version="3.0">
        <remember-me-enabled>false</remember-me-enabled>
    </session-settings>
</settings>
```

The **Remember my login on this computer** option no longer appears on the opening screen.

To restore the **Remember my login on this computer** option, set the value of the <**remember-me-enabled**> element to **true** and restart the HP Release Control server.

22

User Authentication

This chapter describes the possible methods of user authentication in HP Release Control.

This chapter includes:

About HP Release Control User Authentication

You can configure HP Release Control to work in one of the following user authentication modes:

- **Identity management mode.** HP Release Control works with an identity management system that authenticates all users using Lightweight Directory Access Protocol (LDAP).
- **LDAP mode.** HP Release Control works directly with the Lightweight Directory Access Protocol (LDAP) server for user authentication. User information is stored in the LDAP information directory and an LDAP server is used to process queries and updates to this directory.
- **Regular mode.** HP Release Control does not work with an identity management system or LDAP, and HP Release Control authenticates all users.

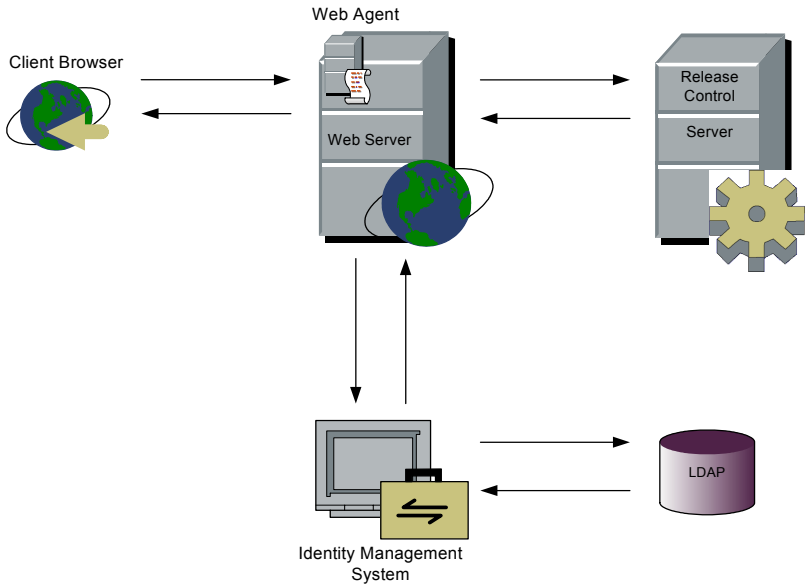
Using Identity Management

Identity management systems enable organizations to maintain user account information in order to control login access to applications. If an identity management system is in place and a user attempts to access an application, the identity management system first authenticates the user by requesting credentials, such as a user name and password. If the user is authenticated, the identity management system authorizes the appropriate level of access to the application based on the user's identity and permissions. In this manner, critical data is protected with appropriate authorizations, while end-user identity information is properly stored.

HP Release Control supports a variety of identity management systems. The configuration samples in this document use the CA SiteMinder 6.0 identity management system.

HP Release Control's Identity Management Mode Architecture

The following diagram illustrates HP Release Control's identity management mode architecture.



To work with identity management in conjunction with HP Release Control, you must instruct HP Release Control to use a Web server. During the HP Release Control installation process, you can instruct HP Release Control to use either an Apache or a Microsoft IIS Web server. For details, see the *HP Release Control Deployment Guide*.

The identity management Web agent is installed on the Web server and used as the single access point for all Web clients. The Web agent intercepts all incoming requests and ensures that they are authenticated. Only authenticated requests are then transferred to HP Release Control.

Configuring HP Release Control to Work in Identity Management Mode

To work with HP Release Control in conjunction with an Identity Management System such as CA SiteMinder, you must configure both HP Release Control and the Identity Management System. This section uses CA SiteMinder as an example, but the same concepts can apply to a variety of Identity Management Systems.

The HP Release Control identity management mode configuration process includes the following:

- Configuring HP Release Control to Work with an Identity Manager
- Configuring an Identity Manager to Work with HP Release Control
- Adding Your Organization's Administrator to HP Release Control

Configuring HP Release Control to Work with an Identity Manager

To work with HP Release Control in conjunction with CA SiteMinder, the HP Release Control administrator must perform the following procedure.

To configure HP Release Control to work with CA SiteMinder:

1. Copy the files located in the **<HP Release Control installation directory>\examples\identity-management-examples\Site-Minder\CCM** \ directory to the HP Release Control installation directory.
2. If your organization has a logout page, ask the CA SiteMinder administrator to provide you with an HP Release Control logout URL. In the **<HP Release Control installation directory>\conf\ security.settings** file, set the **logout-url** field to the value provided.
3. Restart the HP Release Control service.

Configuring an Identity Manager to Work with HP Release Control

To work with CA SiteMinder in conjunction with HP Release Control, the CA SiteMinder administrator must:

- install and configure the Web agent

- configure personalization
- configure the logout page

Installing and Configuring the Web Agent

Install the Web agent on the HP Release Control server machine and configure the agent to protect the HP Release Control resource. Only users who are authorized to work with HP Release Control should be allowed access to the HP Release Control resource.

For details on installing the Web agent and configuring the agent to protect resources, refer to the *eTrust SiteMinder Web Agent Installation Guide*, available from CA.

Configuring Personalization

Configure CA SiteMinder to add the following headers to the HTTP header request that is returned following a successful authentication:

- **uid.** Containing the user's login name.
- **firstName.** Containing the user's first name.
- **lastName.** Containing the user's last name.
- **eMail.** Containing the user's email address.

Configuring the Logout Page

If your organization does not have a logout page, CA SiteMinder should be configured to use the HP Release Control logout page, **ccmLogout.html**, located under **/ccm/imresources** in the Resource Access tree.

Adding Your Organization's Administrator to HP Release Control

By default, HP Release Control includes one user, **admin**, with administrative privileges. This user, however, does not exist in the LDAP information directory. Your organization's real HP Release Control administrator, whose properties are stored in the LDAP directory, does not initially exist in HP Release Control and must be added using the following bootstrap procedure.

To add your organization's administrator to HP Release Control:

1. Set the HP Release Control authentication mode to **IMMode** (in the **<HP Release Control installation directory>\conf\ security.settings** file) and restart the HP Release Control service.
2. Log in to HP Release Control (http://<server name>/ccm) using the identity management credentials of your organization's administrator. Your organization's administrator is added to HP Release Control as a regular user (**User** role).
3. Set the HP Release Control authentication mode to **DBMode** (in the **<HP Release Control installation directory>\conf\ security.settings** file) and restart the HP Release Control service.
4. Log in to HP Release Control (http://<server name>:<Tomcat server port>/ccm) using **admin** as the user name and password.
5. Assign your organization's administrator the role of **Administrator** (in the Administration module's Users tab – see the "Configuring Users" on page 195 for details).
6. Optionally, change the **admin** user's password.
7. Return the HP Release Control authentication mode to **IMMode** and restart the HP Release Control service.

Note:

- You can close the Tomcat server port (by default, 8080) once you have performed the above procedure. For details, contact HP Professional Services.
- It is recommended that you do not remove the **admin** user from HP Release Control. If you did remove the **admin** user, you can restore this user by making sure the server is running, changing the command line directory to **<HP Release Control installation directory>\bin,** and running the following: **addAdminUser.bat.**

Working in Identity Management Mode

When you work in identity management mode, your identity management system authenticates all users. If a user has been successfully authenticated, the identity management system returns the user name, first name, last name, and email address user properties in the HTTP header request. HP Release Control checks whether this user already exists in HP Release Control. If so, the user's first name, last name, and email address are updated, if necessary. If not, the user is added to HP Release Control as a regular user (**User** role), with the properties returned from the identity management system.

Note:

- The created user is unable to log in to HP Release Control using the regular authentication mode until the HP Release Control administrator provides the user with an HP Release Control password. For details, see "Using the Regular Authentication Mode" on page 214.
- If you want to perform an operation that is user-centric (such as assigning an action item to a user) before the user exists in HP Release Control, you can add the user to HP Release Control using the user importer utility. For details on this utility, see "User Importer" on page 285.

When working in identity management mode, the following user and HP Release Control administrator restrictions exist:

- Users are unable to modify their user names, passwords, first names, last names, or email addresses.
- The HP Release Control administrator is unable to add users to HP Release Control using the Administration module.
- The HP Release Control administrator is unable to update the user name, password, first name, last name, or email address of any user within HP Release Control.

All of the above functions must be performed in the LDAP directory.

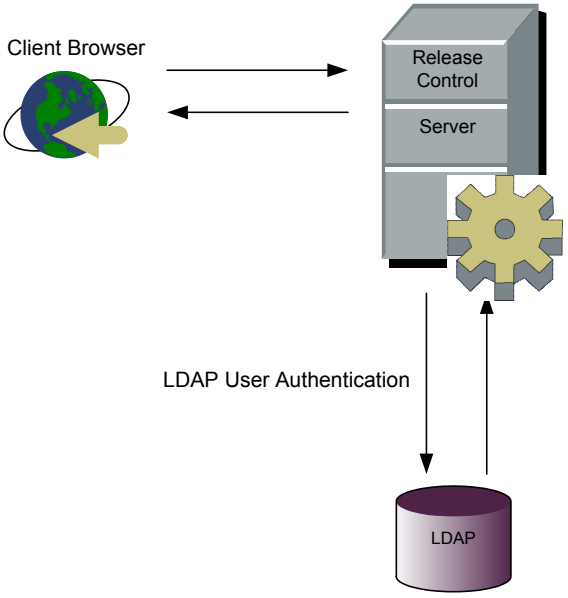
It is possible, however, to add users to HP Release Control using the user importer utility. For details on this utility, see "User Importer" on page 285.

Using LDAP Authentication

You can configure HP Release Control to use LDAP for user authentication. HP Release Control will automatically take the user login information from the LDAP server. Since HP Release Control and LDAP are synchronized, any user information that changes in LDAP will be reflected in HP Release Control the next time a user logs in. When you configure LDAP authentication, you map the LDAP user groups to HP Release Control user roles.

HP Release Control's LDAP Authentication Architecture

The following diagram illustrates HP Release Control's LDAP Authentication mode architecture.



Configuring the LDAP Connection Properties

To work with LDAP authentication in HP Release Control, you must set the LDAP parameters in the **security.settings** and **ldap.properties** files.

security.settings

After you set up the LDAP server, copy the **<HP Release Control installation directory>\examples\ldap-examples\security.settings** file to the **<HP Release Control installation directory>\conf** directory, and configure the following settings:

- **authentication_mode.** Set the authentication mode to **LDAPMode.**
- **User Login Information.** Specify the user login information required to connect to the LDAP server: **FirstName, LastName, Email**.

For example:

```
<authentication-mode>LDAPMode</authentication-mode>
<firstName-header>first_name</firstName-header>
<lastName-header>last_name</lastName-header>
<eMail-header>mail</eMail-header>
```

Map the LDAP user groups to roles in HP Release Control as follows:

- **Group.** In each Group section, specify the **group-name** of the LDAP user group and the corresponding HP Release Control **roles**. The roles can be a single role, or a list of roles separated by a comma.
- **synchronize-roles.** Indicate whether to synchronize the group mapping if a definition changes.
  - Use **true** to specify that if a user changes to a different LDAP group, they will automatically be mapped to new corresponding HP Release Control roles.
  - Use **false** to specify that users should keep their original roles, even if they change groups. In this case a user can only change roles using the HP Release Control client.

➤ **default_roles.** Specify which roles to map to a user if they do not belong to any of the groups defined in the **groups** section. The LDAP authentication will allow all users with a role to access to HP Release Control. Use this setting with caution, because if you set default_roles, then all users will be granted access to HP Release Control.

In the following example, there are two LDAP groups. **Admin** is mapped to the HP Release Control **ONYX_ROLE_ADMIN** role. **General** is mapped to the HP Release Control **ONYX_ROLE_USER** role. **Synchronize-roles** is **true**, so if a user changes roles, he is automatically mapped to the new corresponding LDAP group.

```
<!-- Configure the mapping of groups from LDAP to roles in CCM -->
        <ldap-settings>
            <synchronize-roles>true</synchronize-roles>
            <default-roles></default-roles>
            <groups>
                <group>
                    <group-name>Admin</group-name>
                    <roles>ONYX_ROLE_ADMIN</roles>
                </group>
                <group>
                    <group-name>General</group-name>
                    <roles>ONYX_ROLE_USER</roles>
                </group>
            </groups>
        </ldap-settings>
```

ldap.properties

The HP Release Control installation provides two sample **ldap.properties** files. Both of these files contain detailed instructions for setting the connection between HP Release Control and the LDAP server.

If you are working with LDAP Active Directory, then copy the **<HP Release Control installation directory>\examples\ldap-examples\ldap.properties.AD** file to **<HP Release Control installation directory>\conf\ldap.properties** and set the necessary LDAP server information.

If you are working with LDAP SUN One, then copy the **<HP Release Control installation directory>\examples\ldap-examples\ldap.properties.SO** file to **<HP Release Control installation directory>\conf\ldap.properties** and set the necessary LDAP server information.

Note: If the LDAP server is configured to work over SSL, make sure to set **enableSSL = true** in the **ldap.properties** file.

Using the Regular Authentication Mode

As an alternative to using the HP Release Control's identity management or LDAP user authentication solutions, you can use HP Release Control's regular authentication mode.

To revert to the regular authentication mode:

1. If you previously closed the Tomcat server port (by default, 8080), reopen it.
2. Set the HP Release Control authentication mode to **DBMode** (in the **<HP Release Control installation directory>\conf\security.settings** file) and restart the HP Release Control service.
3. Log in to HP Release Control (http://<server name>:<Tomcat server port>/ccm) using **admin** as the user name and password.
4. Add users as required, providing these users with an initial password. You can also configure passwords for the users added while working in identity management mode. These users will be able to log in to HP Release Control using HP Release Control's regular authentication mode.

Once the identity management solution has been restored, you can resume working in identity management mode by setting the HP Release Control authentication mode to **IMMode** in the **<HP Release Control installation directory>\conf\security.settings** file and accessing HP Release Control via the following URL: http://<server name>/ccm. You can then disable the DB authentication mode by closing the Tomcat server port.

Part VI

System Preferences

23

Configuring System Preferences

This chapter describes how to configure system preferences.

This chapter includes:

Configuring the Format of Emails

You configure the format of the emails that HP Release Control sends in the **ftl** files, located in the **<HP Release Control installation directory>\conf\notifications.ext** directory.

- **mailSubject.ftl.** Defines the subject line of an email. By default, HP Release Control displays **<request-id> – <request summary>** (for example, **C-10020 – Upgrade database server**) as the subject line of the notification.
- **mailbody-text.ftl.** Defines the content of a notification sent in text format.

- **mailbody-html.ftl.** Defines the content of a notification sent in HTML format.
- **user-mailbody-text.ftl.** Defines the content of the email that a user sends by clicking the **Send Email** button in the Change Requests pane.
- **user-mailbody-html.ftl.** Defines the content of the email (in HTML format) that a user sends by clicking the **Send Email** button in the Change Requests pane.
- **free-text-only-text.ftl.** Defines the content of the email that a user sends by clicking the **Send Email** button in the Collaboration tab's Discussion view.
- **free-text-only-html.ftl.** Defines the content of the email (in HTML format) that a user sends by clicking the **Send Email** button in the Collaboration tab's Discussion view.
- **user-action-item-text.ftl.** Defines the content of the email that a user sends by clicking the **Forward by Email (FYI)** button in the Action Items pane.
- **user-action-item-html.ftl.** Defines the content of the email (in HTML format) that a user sends by clicking the **Forward by Email (FYI)** button in the Action Items pane.
- **subscribe-ai-modified-textbody.ftl.** Defines the content of the email sent to a user who subscribed to receive notification of updates to an action item.
- **subscribe-ai-modified-htmlbody.ftl.** Defines the content of the email (in HTML format) sent to a user who subscribed to receive notification of updates to an action item.
- **subscribe-ai-modified-subject.ftl.** Defines the subject line of the email sent to a user who subscribed to receive notification of updates to an action item.
- **subscribe-cr-modified-htmlbody.ftl.** Defines the content of the email (in HTML format) sent to a user who subscribed to receive notification of updates to a change request.
- **subscribe-cr-modified-subject.ftl.** Defines the subject line of the email sent to a user who subscribed to receive notification of updates to a change request.

➤ **subscribe-cr-modified-textbody.ftl.** Defines the content of the email sent to a user who subscribed to receive notification of updates to a change request.

By default, the above files make use of the following HP Release Control objects:

Object	Description
notificationRuleSummary	References the message included in the **change-flow.js** script's **getUsersToNotify** function explaining why the user is receiving a notification.
freeTextBody	The text entered by the user when sending an email from the Change Requests pane of the HP Release Control application.
ScriptingActionItem	The action item object for which the notification is being sent. Using this object, you can reference all of the action item properties. For details of the methods that can be used for this object, refer to the **ScriptingActionItem** class in the **API_Reference.chm** file, located in the **<HP Release Control installation directory>\documentation** folder.
request	The request object for which the notification is being sent. Using this object, you can reference all of the request fields. For details of the methods that can be used for this object, refer to the **GenericRFC** class in the **API_Reference.chm** file, located in the **<HP Release Control installation directory>\documentation** folder.
affectedCIs	Returns a list of the CIs that are impacted by a change request.

Object	Description
viewCis	Returns information about CIs in the context of an impact analysis of a specific change request. For details of the methods that can be used for this object, refer to the **CI** class in the **API_Reference.chm** file, located in the **<HP Release Control installation directory>\documentation** folder.
affectedViews	Returns a list of the business CIs that are impacted by a change request.
viewInfo	Returns information about business CIs that are associated with the affected users, in the context of an impact analysis of a specific change request. For details of the methods that can be used for this object, refer to the **ViewInfo** class in the **API_Reference.chm** file, located in the **<HP Release Control installation directory>\documentation** folder.

Notes:

- The FTL files are written using FreeMarker syntax. For details on using FreeMarker, refer to http://freemarker.sourceforge.net/docs/index.html.
- For a detailed explanation of the objects that can be used in the FTL files, refer to the **API_Reference.chm** file, located in the **<HP Release Control installation directory>\documentation** folder.
- The HP Release Control fields that can be used in the FTL files are those that are defined in the Fields tab of the Administration module. For more information, see "Configuring Change Request Field Settings" on page 29.

Configuring Log File Properties

The **<HP Release Control installation directory>\conf\ ccmlog4j.properties** file contains a list of log file definitions, some of which you may want to modify.

The Tomcat server log files are located in the **<HP Release Control installation directory>\tomcat\logs\stdout-date.log** file.

The HP Release Control log files are located in the **<HP Release Control installation directory>\logs** directory. For a description of each of the log files contained in this directory, see Appendix D, "Log Files."

Modifying the HP Release Control Console Display

By default, when the Tomcat server is running, HP Release Control will not display error messages on the console. All messages will be directed to the **<HP Release Control installation directory>\logs\ccm_general.log** file. This controls the size of the Tomcat server **stdout.log** file.

To change this setting, modify the following line at the top of the **ccmlog4j.properties** file:

```
log4j.rootCategory=WARN, ccm_general_fileout, stdout
```

Modifying the Types of Messages Displayed

The following three types of log message commands can be used:

- **WARN.** Warning and error messages are displayed.
- **INFO.** Info messages that record the processing activity that the system performs are displayed, in addition to warning and error messages.
- **DEBUG.** All types of log messages are displayed.

Modifying File Size and Backup Policy

By default, the maximum size of a log file is set to 4000 KB. To change this setting for all log files, modify the following line at the top of the **ccmlog4j.properties** file:

```
def.file.max.size=4000KB
```

By default, there are 10 backup log files at any given time. To change this setting for all log files, modify the following line at the top of the **ccmlog4j.properties** file:

```
def.files.backup.count=10
```

Modifying Time Zones

By default, log messages are recorded using the time zone that is configured for the HP Release Control server.

To use a different time zone, in the **ccmlog4j.properties** file, set the value of the **CCMTimeZone** property to the appropriate time zone. If the value of this property is not set, the default time zone is used.

For a list of GMT time zones for locations throughout the world, see Appendix B, "GMT Time Zones."

Configuring Calendar Settings

By default, the Calendar view in the Analysis module displays Monday as the first day of the week and the color of the impact severity level as the color of the change request heading. However, you can modify these settings in the **<calendar-settings>** section of the **<HP Release Control installation directory>\conf\analysis-app-module.settings** file.

For example, if you would like to display Sunday as the first day of the week, you would change the value of the **<start-day-of-week>** element from **2** to **1**:

```
<start-day-of-week>1</start-day-of-week>
```

You can also associate the header color with a field other than the impact-severity field. For example, you could associate the header color with the **contact-person** field (using the name of the field that you defined in the Fields tab) and map different contact people to different colors, as follows:

```
<header-line-color>
            <data-field-name>contact-person</data-field-name>
            <data-type>enumeration</data-type>
            <values>
                <map-value source="Steve" target="yellow"/>
                <map-value source="David" target="0x00ff00"/>
            </values>
            <unknown-value>0xffffff</unknown-value>
        </header-line-color>
```

Note: The <**unknown-value**> element defines the color to be displayed when the value of the field does not match any of the mapped values.

Alternatively, you can modify the default colors displayed in the header for each impact severity level. For example, you could associate the impact severity level of **High** with the color purple and the impact severity level of **Medium** with the color blue, as the following lines demonstrate:

```
<header-line-color>
            <data-field-name>impact-severity</data-field-name>
            <data-type>enumeration</data-type>
            <values>
                <map-value source="High" target="purple"/>
                <map-value source="Medium" target="blue"/>
            </values>
            <unknown-value>0xffffff</unknown-value>
        </header-line-color>
```

Note: The colors you define for the calendar header will also be used in the Timeline views.

Configuring Dashboard Settings

The **<HP Release Control installation directory>\conf\dashboard.settings** file maps the two types of roles in HP Release Control—**user** and **administrator**—to the **users** and **administrators** Dashboard groups, respectively, and defines the privileges granted to each group. This file also contains other definitions related to the display of Dashboard pages and portlets.

Note: The definitions in this file should not be modified.

The **<HP Release Control installation directory>\conf\Dashboard_Objects_Export.xml** file contains definitions for the HP Release Control Default Page in the Dashboard. If you changed the **Pending Approval** or **Closed** status in the **<HP Release Control installation directory>\conf\enumerations.settings** file, you must update the **Dashboard_Objects_Export.xml** file with the alternative status or statuses that you are using.

To update the Closed status:

1 Locate the following line within the **Dashboard_Objects_Export.xml** file:

```
[CLOSED][Closed]
```

Note that there are two occurrences of this line in the file.

2 Replace **[CLOSED]** with the alternative status defined in the **<HP Release Control installation directory>\conf\enumerations.settings** file. For details on configuring the **enumerations.settings** file, see the section about customizing HP Release Control fields in the *HP Release Control Deployment Guide*.

3 Replace **[Closed]** with the label you assigned to the above status in the **<HP Release Control installation directory>\conf\enumeration-labels.properties** file. For details on configuring the **enumeration-labels.properties** file, see "Configuring Enumeration Field Display Settings" on page 227.

To update the Pending Approval status:

1 Locate the following line within the **Dashboard_Objects_Export.xml** file:

```
[PENDING_APPROVAL][Pending_Approval]
```

Note that there are two occurrences of this line in the file.

2 Replace **[PENDING_APPROVAL]** with the alternative status defined in the **<HP Release Control installation directory>\conf\ enumerations.settings** file. For details on configuring the **enumerations.settings** file, see the section about customizing HP Release Control fields in the *HP Release Control Deployment Guide*.

3 Replace **[Pending_Approval]** with the label you assigned to the above status in the **<HP Release Control installation directory>\conf\ enumeration-labels.properties** file. For details on configuring the **enumeration-labels.properties** file, see "Configuring Enumeration Field Display Settings" below.

After you have updated the **Dashboard_Objects_Export.xml** file with the alternative status or statuses that you are using, you must run the **populate_dashboard.bat** command from the **<HP Release Control installation directory>\tomcat\webapps\ccm** command line directory. Note that when you run this command, any previous Dashboard data that you configured is automatically deleted.

Configuring Enumeration Field Display Settings

The **<HP Release Control installation directory>\conf\ enumeration-labels.properties** file contains a default application display mapping scheme for the configured enumeration fields. You can modify the way in which the HP Release Control application displays each of the enumeration fields listed in this file.

For example, you may want to display the status **Closed** as **Completed**. To do so, you would change the line:

```
StatusEnum.CLOSED=Closed
```

to:

```
StatusEnum.CLOSED=Completed
```

You can also modify the icon color that corresponds to each severity level. For example, to display a red icon rather than an orange icon for a severity level of **High**, you would change the line:

```
SeverityEnum.High.color=orange
```

to:

```
SeverityEnum.High.color=red
```

Note: You cannot modify the color icons themselves; red, orange, yellow, green_yellow, green, and gray are the only colors available.

By default, top-level or parent change requests are referred to as **changes** and second-level or child change requests are referred to as **tasks** in the HP Release Control application. Other request hierarchy levels are referred to as **unknown**. You can modify this terminology by changing the following lines in the **enumeration-labels.properties** file:

```
LevelEnum.1=Change
LevelEnum.2=Task
LevelEnum.Level.UNKNOWN=Unknown
```

Configuring Localization Settings

By default, the HP Release Control location setting is set to the United States and English is the default language setting. You can modify these settings in the **<name>country</name>** and **<name>language</name>** sections of the **<HP Release Control installation directory>\conf\appinfra.settings** file.

```
<property>
        <name>country</name>
        <value>US</value>
</property>
<property>
        <name>language</name>
        <value>en</value>
</property>
```

For example, if you would like to change the country and language settings to Japan and Japanese respectively, you would change the **US** and **en** values to **JP** and **ja** respectively.

Configuring Alert Settings

This section describes the configuration of the **alerts-config.settings** file where you can configure the following settings for alerts:

- "Alert Engine Run Interval" on page 230
- "First Run of Alert Engine" on page 232
- "Change-Modify Time Window for Emergency/Modified Activity Alerts" on page 232
- "Alert Behavior" on page 235

Caution: You must restart the HP Release Control service for these configuration changes to take effect.

Alert Engine Run Interval

HP Release Control refreshes alerts in the Director module using the alert engine defined in the <**HP Release Control installation directory**>**conf****alerts-config.settings** file. By default, the alert engine is enabled and runs every minute.

To change the rate at which the engine runs:

1 In the **alerts-config.settings** file, locate the <**cron-expression**> element.

```
<alerts-config version="4.0-local-build">
        <default-config>
            .
            <!-- use this option to enable the alert engine every minute-->
            <cron-expression>0 0/1 * * * ?</cron-expression>
```

By default, the alert engine is configured to run after an interval of 1 minute. This is indicated by the **minutes** field of the cron expression, **0/1**, where 1 is the interval (in minutes) after which the engine runs. (For more information about cron expressions, see http://quartz.sourceforge.net/javadoc/org/quartz/CronTrigger.html.)

Use the following examples as a guideline for changing the run interval:

- To run the engine every 5 minutes, change the minutes field to **0/5**.
- To run the engine every 30 minutes, change the minutes field to **0/30**.

2 Save the **alerts-config.settings** file.

3 To apply the changes, you must restart the HP Release Control service.

To disable the alert engine:

1 In the **alerts-config.settings** file, locate the following code:

```
<alerts-config version="4.0-local-build">
        <default-config>
            .
            .
            <!-- use this option to disable the alert engine-->
            <!-- <cron-expression>-1</cron-expression> -->

            <!-- use this option to enable the alert engine every minute-->
            <cron-expression>0 0/1 * * * ?</cron-expression>
```

2 Uncomment the expression that disables the alert engine, and comment out the code that enables it, as follows:

```
<alerts-config version="4.0-local-build">
        <default-config>
            .
            .
            <!-- use this option to disable the alert engine-->
           <cron-expression>-1</cron-expression>

            <!-- use this option to enable the alert engine every minute-->
            <!-- <cron-expression>0 0/1 * * * ?</cron-expression> -->
```

3 Save the **alerts-config.settings** file.

4 To apply the changes, you must restart the HP Release Control service.

First Run of Alert Engine

The first run of the Alert Engine is very heavy on the system, calculating alerts, by default, 2 days (2880 minutes) retroactively. You can change this setting so that the Alert Engine runs on fewer change requests, that is, over a shorter retroactive time interval.

To modify this setting:

1 In the **alerts-config.settings** file, locate the <**fuse-duration**> element.

```
<alerts-config version="4.0-local-build">
        .
        .
          <fuse-duration>2880</fuse-duration>
```

2 Define a new retroactive time interval, in minutes.

3 Save the **alerts-config.settings** file.

4 To apply the changes, you must restart the HP Release Control service.

Change-Modify Time Window for Emergency/Modified Activity Alerts

Emergency Activity alerts and Activity Modification alerts are generated for all activities whose schedules intersect the **change-modify time window** defined in the **alerts-config.settings** file.

More specifically:

- An Emergency Activity alert is generated if a new activity is created that is scheduled to start within the change-modify time window.
- An Activity Modification alert is generated if a change is made to an activity whose schedule intersects with the change-modify time window.

The **change-modify time window** can be defined as a window of time surrounding or close to the current time. By default, the change-modify time window is defined as 12 hours (720 min) behind the current time to 24 hours (1440 min) ahead of the current time.

To modify the change-modify time window:

1 In the **alerts-config.settings** file, locate the <**change-modify-time-window**> element.

```
<alerts-config version="4.0-local-build">
        .
      <!-- This configuration purpose is to decide whether to generate alerts due to
change modification in the given time window:
            1. Emergency Change Alert
            2. Modified Change Alert -->
            <change-modify-time-window>
                <min>-720</min>
                <max>1440</max>
            </change-modify-time-window>
```

2 Define a time interval as follows (see examples below):

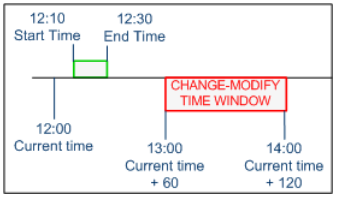
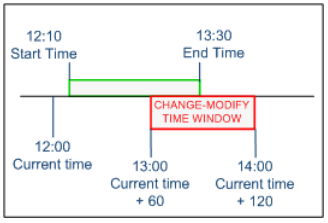
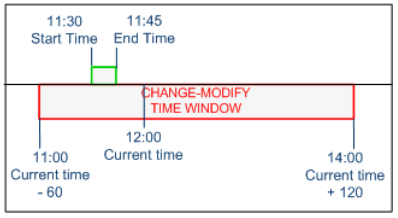
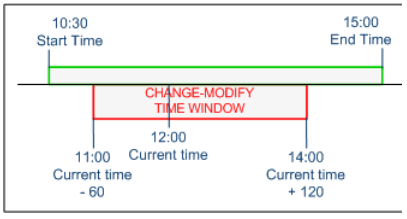
- <**min**>**.** The number of minutes before (negative value) or after (positive value) the current time, representing the beginning of the time window.
- <**max**>**.** The number of minutes before (negative value) or after (positive value) the current time, representing the end of the time window.

3 Save the **alerts-config.settings** file.

4 To apply the changes, you must restart the HP Release Control service.

Examples

The following examples illustrate minimum and maximum values for the time window, and where alerts will or will not be generated.

Scenario 1- No alert generated ➤ Emergency Activity insterted at: 12:00 ➤ Time window: min = +60; max = +120 ➤ Activity Start: 12:10; Activity End: 12:30	
Scenario 2 - Alert generated ➤ Activity modified at: 12:00 ➤ Time window: min = +60; max = +120 ➤ Activity Start: 12:10; Activity End: 13:30	
Scenario 3 - Alert generated ➤ Emergency activity insterted: 12:00 ➤ Time Window: min = -60; max = +120 ➤ Activity Start: 11:30; Activity End: 11:45	
Scenario 4 - Alert generated ➤ Activity modified at: 12:00 ➤ min = -60; max = +120 ➤ Activity Start: 10:30; Activity End: 15:00	

Alert Behavior

You can enable or disable alerts, and define the number of minutes before or after events that you want alerts to be generated.

Each alert is defined in an <**alert**> sub-element, which specifies the type of alert, whether the alert is enabled or not, and if so, the amount of time before or after the event that the alert is to be generated.

For example, the code below indicates that if an activity's implementation is more than 15 minutes late to finish, HP Release Control generates a **ChangeEndLateAlert** alert.

```
<alerts-config version="4.0-local-build">
        .
        </alerts>
           <alert>
              <alert-type>ChangeEndLateAlert</alert-type>
              <alert-enabled>true</alert-enabled>
              <notification-offset>15</notification-offset>
           </alert>
           .
           .
        </alerts>
```

To configure an alert's behavior:

1. In the **alerts-config.settings** file, locate the <**alerts**> element and then the <**alert**> sub-element of the alert you want to modify.
2. Modify the alert's definition as follows:
   - In the <**notification-offset**> attribute, specify the number of minutes before or after the event that the alert is to be generated.
   - To disable the alert, set <**alert-enabled**> to **false**.
3. Save the **alerts-config.settings** file.
4. To apply the changes, you must restart the HP Release Control service.

Customizing Reports

This section describes how to customize the reports generated by HP Release Control in the Analysis module. HP Release Control uses JasperReports as the report engine.

The report template files are located in the **<HP Release Control installation directory>/conf/reports.ext** folder. For a description of these reports, see "Report Templates" below.

You use the iReport tool to edit these report templates. You can download the latest version of the iReport tool from http://sourceforge.net/projects/ireport/.

Notes:

- You can use value expressions to customize your reports. For more information, see "Value Expressions" on page 238.
- After editing the reports, there is no need to restart the HP Release Control server.
- To verify your editing changes, you can generate the report in the Analysis module.

Report Templates

The report template files are located in the **<HP Release Control installation directory>/conf/reports.ext** folder.

The following table describes the report template uses for the reports generated in the Analysis module Calendar view:

Report Template	Function
calendar.changes-report.pdf.jrxml	Information included in the header and footer in PDF or HTML reports.
calendar.week..jrxml	The display of the week in PDF or HTML reports. For example: Week: Oct 20, 2008 - Oct 26, 2008.
calendar.changes-report.days-subreport.pdf.jrxml	The display of the day in PDF or HTML reports. For example: Wednesday 10/22/08.
calendar.changes-report.tickets-subreport.pdf.jrxml	The content of the actual change request in PDF or HTML reports.

The following table describes the report template uses for the reports generated in the Analysis module List view:

Report Template	Function
grid.change-single-pager-report.pdf.jrxml	Template for generating a one page PDF or HTML report.
grid.changes-report.pdf.jrxml	Template for generating first level changes in a PDF or HTML list report.
grid.changes-report.tasks-subreport.pdf.jrxml	Template for generating second level changes in a PDF or HTML list report.
grid.changes-report.xls.jrxml	Template for generating a list report in Excel format.

Value Expressions

You can define value expressions using report parameters, variables, and fields, and you can use Java expressions to customize your report.

Ticket Field

In JasperReports, there is a preconfigured **ticket** field that contains the most newly created request for change (a wrapper of the **GenericRFC** object). To obtain a value for one of the change request fields, use the following expression:

```
$F{Ticket}.getFieldLabel(<“field name”>)
```

For example:

```
$F{Ticket}.getFieldLabel(<“summary”>)
```

$F{Ticket} returns the wrapped **GenericRFC** object. For more complex expressions, you can use any of the methods included in the **GenericRFC** class of the HP Release Control API. For information on the **GenericRFC** class, refer to the **API_Reference.chm** file, located in the **<HP Release Control installation directory>\documentation** folder.

Java Expressions

You can use Java expressions to customize your reports**.** For example, if the UI displays **N/A** for blank values, it is likely that you will want to display N/A in the report as well. To do so, you can use the following expression:

```
(((String)$F{Ticket}.getFieldLabel(<field name>)).length() > 0) ? $F{Ticket}.getFieldLabel(<field name>) : $P{N/A}
```

In the above example, **$P{N/A}** is a parameter that contains a string value, **N/A**, to be displayed when data is not available. The string value can be changed as required.

Part VII

Special Integration with Other Products

24

HP Release Control Federation Adapter

This chapter provides information on the HP Release Control Federation adapters. The adapters are compatible with HP Universal CMDB, version 7.5 or later.

This chapter includes:

About the Release Control Federation Adapters

The HP Release Control Federation adapter supports the retrieval of data from HP Release Control. Every request to HP Release Control to calculate a federated query is made through this adapter.

There are two types of HP Release Control Federation adapters:

- **Change Federation adapter.** See "About the Change Federation Adapter" below.
- **KPI Federation adapter.** See "About the KPI Federation Adapter" on page 244.

About the Change Federation Adapter

The Change Federation adapter supports the **Planned Change** CI type. You use **service desk** links to create a query.

The adapter ID for the Change Federation adapter is **CcmChangeAdapter**.

The following use cases describe how the adapter can be employed:

- A user needs to display **planned changes to any CI** within a specific time frame.
- A user needs to display **planned changes to specified system CIs**.

  In this case, HP Universal CMDB retrieves changes that directly change system CIs and not changes that indirectly affect system CIs.
- A user needs to display **planned changes to a specified business CI**.

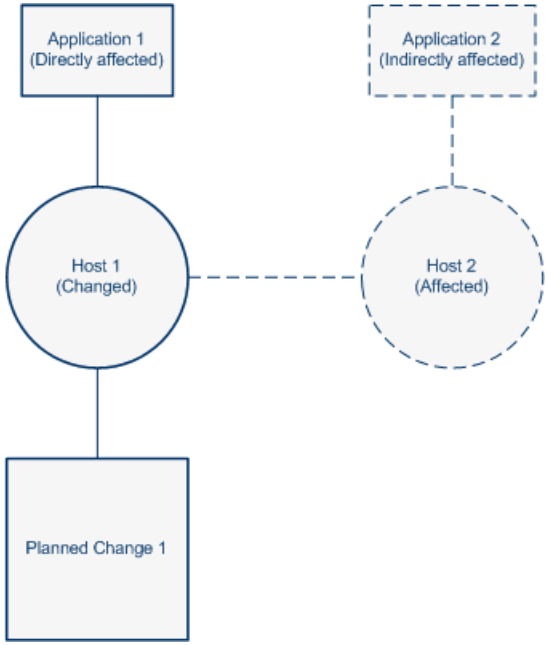
  In this case, HP Universal CMDB retrieves changes that directly affect business CIs and not changes that indirectly affect business CIs.

In all of the above cases, HP Universal CMDB retrieves parent changes and independent tasks. HP Universal CMDB does not retrieve tasks that are included in a parent request.

Example

The following example illustrates some of the use cases. Assume there is one planned change in HP Release Control, **Planned Change 1.**
Planned Change 1 will be performed on **Host 1**. **Application 1** runs on **Host 1** and is therefore directly affected by the change.

Host 2 is connected to **Host 1** and may be affected by **Planned Change 1** but no actual change is made to **Host 2**. **Application 2** runs on **Host 2** and may be indirectly affected by the change.



If the user runs a query to retrieve planned changes to **Host 1** or **Application 1,** HP Universal CMDB will display **Planned Change 1**, because this change directly affects those CIs.

If the user runs a query to retrieve planned changes to **Host 2** or **Application 2,** HP Universal CMDB will not display any changes because there are no changes that directly affect those CIs.

About the KPI Federation Adapter

The KPI Federation adapter supports the **Real Time KPI** CI type. You use **KPI of** links to create a query.

When this adapter is configured, you can view KPIs (Key Performance Indicators) in the HP Business Availability Center Dashboard that indicate the number of planned/actual changes that have taken place on the relevant CIs during the last 24 hours.

The adapter ID for the KPI Federation adapter that displays information about **planned** changes is **RCKpiPlannedChangeAdapter**.

The adapter ID for the KPI Federation adapter that displays information about **actual** changes is **RCKpiActualChangeAdapter**.

Configuring the Federation Adapters

This section describes how to configure the HP Release Control Federation adapter to work with HP Universal CMDB.

For more information see the *HP Universal CMDB Model Management* guide.

To configure the adapter:

1 Deploy the following file in the HP Universal CMDB Package Manager (In the HP Universal CMDB go to **Settings** > **Package Manager)**:

- **<Release Control installation directory>\conf\uCmdb -<version_number>-extensions\federation\<adapter_name>.zip**
- where <adapter_name> is th ename of the relevant adapter, for example, **CcmChangeAdapter.zip**.

2 Restart the HP Universal CMDB server or reload the relevant adapter in the HP Universal CMDB jmx-console as follows:

a To open the HP Universal CMDB jmc-console, type the following URL:

```
http://<HP Universal CMDB server name>:8080/jmx-console
```

b Enter your user name and password.

c Locate the **service=FCmdb Config Services link** and click it.

d Go to the **Load or reload (and start) adapter code base** section and enter the following:

- **CustomerID.** the ID of the customer
- **adapterID.** the ID of the federated adapter. For example, **CcmChangeAdapter**.

e Click Invoke to reload the adapter.

3 In the HP Universal CMDB go to **Settings** > **Federated CMDB** and configure the relevant adapter. Enter the following required details:

- **Name.** The logical name of the adapter.
- **Host.** The URL of HP Release Control.
- **Port.** The port used by the Tomcat server. If no value is entered, 8080 is used as the default port. To use a different port, enter a value.
- **User.** The user name of an administrator user in HP Release Control.
- **Password.** The password of the administrator user specified above.

4 If you are configuring the Change Federation adapter, see "Advanced Configuration for the Change Federation Adapter" below.

Advanced Configuration for the Change Federation Adapter

This section includes advanced configuration information for the Change Federation adapter.

Retrieving Planned Change Attributes

HP Universal CMDB contains a list of the **planned change** attributes selected in the **CI Type Manager Attributes** tab. HP Universal CMDB retrieves **planned change** attributes from HP Release Control using the following rule:

HP Universal CMDB converts all underscores (_) in the attribute names and converts them to hyphens (-) and searches through the HP Release Control fields for matching fields. The list of fields in HP Release Control is located in the Administrator module **Fields** tab.

In addition, specific attribute properties are mapped to specific fields in the **convertfields.properties** file, located in the **CcmChangeAdapter** directory. You can map additional attributes to fields HP Release Control in this file.

Adding Custom Fields to the Federation Adapter

This section explains how to add custom fields to the Federation adapter.

To add new custom fields to the Federation adapter:

1. In HP Release Control, add the relevant fields in the Administrator module **Fields** tab. For more information about adding custom fields, see "Creating or Modifying Change Request Fields" on page 31.
2. In HP Universal CMDB, go to the **planned change** CI type and add the new attribute names.
   - ➤ Use the same name for the attribute as you used for the custom field that you created in HP Release Control. However, if you used a hyphen (-) in the field name, substitute the hyphen for an underscore (_) in the name of the attribute.
   - ➤ If you want to use an attribute name that is different from the custom field name, you can map the attribute name to a specific field name in the **convertfields.properties** file, located in the **CcmChangeAdapter** directory.

25

Linking to HP Release Control Interfaces from Other Applications

This chapter contains information about creating links to HP Release Control from other applications. You can create a link to the whole application or to specific areas of the application.

For example, assume that you are working in your service desk and you are trying to decide what start time to assign to a ticket. You can create a link from within your service desk to open the HP Release Control Calendar and view the scheduled changes for the relevant time frame.

Notes:

- If you do not have LW-SSO installed, you will be prompted for your HP Release Control credentials when you access these links.
- If you are fully integrated with HP Service Manager 7.11 (webtier), these links are pre-configured in HP Service Manager.

This chapter includes:

Linking to the HP Release Control Application

You can create a customized link to the HP Release Control application to be used from outside of HP Release Control. The link can be customized to display the relevant view using the filter, timestamp, and perspective of your choice.

To create a link to the HP Release Control application:

From an internet browser, enter the following URL, customized according to the table below:

```
http://localhost:8080/ccm?requestOrigin=EXTERNAL&<customizable parameters>
```

Caution: The URL must contain at least one **filterName** or **field-<field name>** parameter.

For guidelines about rules and syntax regarding the URLs, see “Rules and Syntax” on page 255.

For guidelines about locating the enumeration values for the relevant fields see “Field Parameter Values” on page 255.

The following table describes the available parameters for the URL:

Parameter	Description
filterName	Filters the requests displayed in HP Release Control according to the specified filter name. **Notes:** ➤ You can further refine the filter by defining **field-<field name>** parameters, as described below. ➤ The filter names are defined in the HP Release Control Analysis or Director module.
field-<field name>	Filters the requests displayed in HP Release Control according to the field values defined in this parameter. For example, **field-status=APPROVED,CLOSED.** **Notes:** ➤ All field names must start with the **field-** prefix. ➤ Fields used in this parameter must be defined as filterable in HP Release Control. ➤ Field names should be written as they appear in the **fields.settings**. ➤ If you specified a filter in the **filterName** parameter, the **field-<field name>** parameter, further refines this filter. ➤ If the field name (**field-<field name>)** also exists in the filter (**filterName)**, the value in the **field-<field name>** parameter will overwrite the value in the filter. ➤ You can specify multiple **field-<field name>** parameters. For information about where to find allowed values for the fields used in this parameter, see “Field Parameter Values” on page 255.

Parameter	Description
perspective	The view in which the Analysis module will open. You can set the following values: ➤ **RFCViewer.** Opens the List view (Default) ➤ **timeLine.** Opens the Timeline view ➤ **calendar.** Opens the Calendar view
timestamp	The date on which you want the calendar to open. The date is represented as a timestamp in milliseconds. **Notes**: ➤ If no timestamp is defined, the default date is the current date. ➤ If the current or specified date is not within the time range of the specified filter, the date closest to the start or end of the filtered time is displayed.

Example

In the following example, a link is created to the HP Release Control application. HP Release Control opens in the Calendar view on the specified date. HP Release Control displays only the requests with a status of APPROVED or CLOSED and a risk level between 20-80.

```
http://localhost:8080/ccm?requestOrigin=EXTERNAL&filterName=any&
field-calculated-risk=20,80&field-status=APPROVED,CLOSED&perspective=calendar&
timestamp=1225648800000
```

Linking to HP Release Control Calendar

You can create a customized link to the HP Release Control Calendar. When you access the Calendar using this link, you can view the scheduled change requests, search for specific change requests, view change request details, and so forth. However, access to other areas of the HP Release Control is limited. For example, you cannot set filters or user preferences and you cannot access the various change analysis tabs.

To create a link to the HP Release Control Calendar:

From an internet browser, enter the following URL, customized according to the table below:

```
http://localhost:8080/ccm/calendar.html?requestOrigin=EXTERNAL&<customizable parameters>
```

Caution: The URL must contain at least one **filterName** or **field-<field name>** parameter.

For guidelines about rules and syntax regarding the URLs, see “Rules and Syntax” on page 255.

For guidelines about locating the enumeration values for the relevant fields see “Field Parameter Values” on page 255

The following table describes the available parameters for the URL:

Parameter	Description
filterName	Filters the requests displayed in HP Release Control according to the specified filter name. **Notes:** ➤ You can further refine the filter by defining **field-<field name>** parameters, as described below. ➤ The filter names are defined in the HP Release Control Analysis or Director module.
field-<field name>	Filters the requests displayed in HP Release Control according to the field values defined in this parameter. For example, **field-status=APPROVED,CLOSED.** **Notes:** ➤ All field names must start with the **field-** prefix. ➤ Fields used in this parameter must be defined as filterable in HP Release Control. ➤ Field names should be written as they appear in the **fields.settings**. ➤ If you specified a filter in the **filterName** parameter, the **field-<field name>** parameter, further refines this filter. ➤ If the field name (**field-<field name>)** also exists in the filter (**filterName)**, the value in the **field-<field name>** parameter will overwrite the value in the filter. ➤ You can specify multiple **field-<field name>** parameters. For information about where to find allowed values for the fields used in this parameter, see "Field Parameter Values" on page 255.
timestamp	The date on which you want the calendar to open. The date is represented as a timestamp in milliseconds. **Notes**: ➤ If no timestamp is defined, the default date is the current date. ➤ If the current or specified date is not within the time range of the specified filter, the date closest to the start or end of the filtered time is displayed.

Example

In the following example, a link is created to the HP Release Control Calendar. The Calendar opens on the specified date and displays only the requests with a status of APPROVED or CLOSED and a risk level between 20-80.

```
http://localhost:8080/ccm/calendar.html?requestOrigin=EXTERNAL&filterName=any
&field-calculated-risk=20,80&field-status=APPROVED,CLOSED&timestamp=1225648
800000
```

Linking to the Assess Tab

You can create a link to the HP Release Control Assess tab for a single change request. The Assess Tab contains information about impact analysis, collisions, risk analysis, similar changes, and time period conflicts.

When you access the Assess tab using this link, you can view all the change analysis information for the specified request, but you cannot access other areas of HP Release Control.

To create a link to the Assess tab:

From an internet browser, enter the following URL:

```
http://<HP Release Control Server Name: Port>/ccm/assess.html?refId=<service desk
ID>
```

where **service desk ID** is the ID of the ticket as defined in the service desk application.

For example:

```
http://localhost:8080/ccm/assess.html?refId=C-00000006
```

Note: If you are working with more than one service desk application, you can use the **serviceDesk** parameter, to specify the name of the service desk. For example, if two tickets from two different service desks both have the same ID, the **serviceDesk** parameter can serve as a discriminator. The name of the service desk is at it appears in the Analysis module details tab.

Linking to a Single Change Request

You can create a link to a single change request in HP Release Control. HP Release Control opens displaying the specified change request.

When you access HP Release Control using this link, you can access all other areas of HP Release Control.

To create a link to a single change request in HP Release Control:

From an internet browser, enter the following URL:

```
http://localhost:8080/ccm?requestOrigin=EXTERNAL&requestedChangeID=<service desk ID>
```

where **service desk ID** is the ID of the ticket as defined in the service desk application.

For example:

```
http://localhost:8080/ccm?requestOrigin=EXTERNAL&requestedChangeID=C-00000006
```

Rules and Syntax

The following list contains various rules, tips, and syntax requirements regarding the URLs.

- Enumeration values are case sensitive.
- Boolean values are in the form of **true** and **false** respectively.
- Date constraints are not supported.
- Multiple values should be delimited by a comma (,) with no white space between values.
- Fields with a BETWEEN operator must contain two unequal values.
- Ensure that filter values are the correct type. For example, if you enter a single value for a field that requires a numeric-range the application will return an exception.

Field Parameter Values

This section describes where to find the allowed values for fields used in the **field-<field name>** parameter. Values are defined in:

- The HP Release Control database or configuration files.
- The service desk application
- The HP Universal CMDB.

Some of the configurable values are defined in the **<HP Release Control installation directory>\conf\enumerations.settings** file. In these cases, the allowed values are the **name** elements of the relevant **enum-type** element.

For example, for the **priority** field, the relevant **enum-type** element in the **enumerations.settings** file is **Priority**:

```
<enum>
    <enum-type>Priority</enum-type>
    <default-name>NORMAL</default-name>
    <unknown-name>UNKNOWN</unknown-name>
    <entry>
            <id>27</id>
            <name>LOW</name>
            <value>0</value>
    </entry>
    <entry>
            <id>28</id>
            <name>NORMAL</name>
            <value>1</value>
    </entry>
    <entry>
            <id>29</id>
            <name>HIGH</name>
            <value>2</value>
    </entry>
    <entry>
            <id>30</id>
            <name>IMMEDIATE</name>
            <value>3</value>
    </entry>
    <entry>
            <id>31</id>
            <name>UNKNOWN</name>
            <value>-1</value>
    </entry>
</enum>
```

In this example, the allowed values, would be:

- LOW
- NORMAL
- HIGH
- IMMEDIATE
- UNKNOWN

The following table describes the allowed values for the fields:

Field Name	Corresponding Enumeration Value
abnormal-cause	Name of time period rule in Administrator module Time Periods tab.
application	Business CI IDs (as defined in HP Universal CMDB)
category	Values as defined in the service desk ticket.
change-type	➤ REGULAR ➤ LATENT ➤ SURROGATE ➤ AUTOMATED
collision-severity	➤ NONE ➤ VERY_LOW ➤ LOW ➤ MEDIUM ➤ HIGH ➤ CRITICAL
collision-type	➤ CCI_CCI ➤ CCI_ACI ➤ ACI_ACI ➤ IAA_IAA ➤ IAA_DAA ➤ DAA_DAA ➤ IMPLEMENTOR
creating-service-desk	Values as defined in the service desk ticket.
impact-severity	**<enum-type>Severity</enum-type>** in **enumerations.settings**.
implementation-outcome	**<enum-type>Implementation</enum-type>** in **enumerations.settings**.
implementors	Values as defined in the service desk ticket.

Field Name	Corresponding Enumeration Value
lastImpact-cis-label	System CI labels (as defined in HP Universal CMDB)
lastImpact-cis-refId	System CI IDs (as defined in HP Universal CMDB)
opinion-type	**<enum-type>Opinion</enum-type>** in **enumerations.settings**.
priority	**<enum-type>Priority</enum-type>** in **enumerations.settings**.
review-customer-satisfaction	**<enum-type>CustomerSatisfaction</ enum-type>** in **enumerations.settings**.
review-planning-satisfaction	**<enum-type>PlanningSatisfaction</enum-type>** in **enumerations.settings**.
status	**<enum-type>Status</enum-type>** in **enumerations.settings**.
subcategory	Values as defined in the service desk ticket.
ticket-level	**<enum-type>Level</enum-type>** in **enumerations.settings**.

Part VIII

Appendices

A

Password Encryption

All HP Release Control passwords may be encrypted, if required. This chapter describes how to encrypt passwords.

To encrypt a password:

1 Ensure that your HP Release Control installation directory contains a **security** directory that includes the following files:

- private_key.txt
- public_key.txt

If these files do not exist, then run the following in the **<HP Release Control installation directory>\bin** directory:

```
GenerateKeys.bat
```

2 In the **<HP Release Control installation directory>\bin** directory, run the following:

```
EncryptPassword.bat <options> <password to encrypt>
```

The command line <options> can be:

Option	Description
-f <file> **--password-file <file>**	Encrypt the passwords in the specified plain-text password file.
-p <password> **--password <password>**	Encrypt a single plain-text password.

Option	Description
--keys-path <path>	Use the encryption keys located at the specified path. If this option is not specified, the default key location is **<ccm-installation>\security.**
-h **--help**	Print this message.

For example, to encrypt a single password, run the following:

```
EncryptPassword.bat -p <password to encrypt>
```

3 Copy and paste the generated encrypted password (**{ENCRYPTED}** **<encrypted password>**) into the appropriate HP Release Control configuration file.

To encrypt all the passwords in a file:

1 Ensure that the each password in the file is on a separate line, as in the following example:

```
<password1>
<password2>
<password3>
```

2 In the **<HP Release Control installation directory>\bin** directory, run the following:

```
EncryptPassword.bat -f <file name>
```

A file with the same name and the extension **.enc** is created. This file includes an encrypted password for each password included in the original file.

3 Copy and paste each generated encrypted password (**{ENCRYPTED}** **<encrypted password>**) into the appropriate HP Release Control configuration file.

B

GMT Time Zones

The following list describes GMT time zones for locations throughout the world.

(GMT -11) Pacific/Niue
(GMT -11) MIT
(GMT -10) Pacific/Tahiti
(GMT -10) Pacific/Honolulu
(GMT -10) America/Adak
(GMT -9) Pacific/Marquesas
(GMT -9) America/Anchorage
(GMT -8) Pacific/Pitcairn
(GMT -8) America/Tijuana
(GMT -8) PST
(GMT -7) America/Phoenix
(GMT -7) America/Edmonton
(GMT -7) America/Denver
(GMT -6) America/Belize
(GMT -6) Pacific/Galapagos
(GMT -6) America/Tegucigalpa
(GMT -6) America/Costa_Rica
(GMT -6) Pacific/Easter
(GMT -6) America/Chicago
(GMT -5) America/Porto_Acre
(GMT -5) America/Guayaquil
(GMT -5) America/Cayman
(GMT -5) America/Panama
(GMT -5) America/Indianapolis
(GMT -5) America/Nassau
(GMT -11) Pacific/Apia
(GMT -11) Pacific/Pago_Pago
(GMT -10) Pacific/Fakaofo
(GMT -10) HST
(GMT -10) Pacific/Rarotonga
(GMT -9) Pacific/Gambier
(GMT -9) AST
(GMT -8) America/Vancouver
(GMT -8) America/Los_Angeles
(GMT -7) America/Dawson_Creek
(GMT -7) PNT
(GMT -7) America/Mazatlan
(GMT -7) MST
(GMT -6) America/Regina
(GMT -6) America/Guatemala
(GMT -6) America/El_Salvador
(GMT -6) America/Winnipeg
(GMT -6) America/Mexico_City
(GMT -6) CST
(GMT -5) America/Bogota
(GMT -5) America/Jamaica
(GMT -5) America/Managua
(GMT -5) America/Lima
(GMT -5) IET
(GMT -5) America/Montreal

(GMT -5) America/Havana
(GMT -5) America/Grand_Turk
(GMT -5) EST
(GMT -4) America/Anguilla
(GMT -4) America/Aruba
(GMT -4) America/La_Paz
(GMT -4) America/Dominica
(GMT -4) America/Grenada
(GMT -4) America/Guyana
(GMT -4) America/St_Lucia
(GMT -4) America/Montserrat
(GMT -4) PRT
(GMT -4) America/St_Vincent
(GMT -4) America/St_Thomas
(GMT -4) Antarctica/Palmer
(GMT -4) America/Cuiaba
(GMT -4) Atlantic/Stanley
(GMT -4) America/Asuncion
(GMT -3) America/St_Johns
(GMT -3) America/Fortaleza
(GMT -3) America/Paramaribo
(GMT -3) America/Buenos_Aires
(GMT -3) America/Godthab
(GMT -3) America/Sao_Paulo
(GMT -2) America/Noronha
(GMT -1) Atlantic/Jan_Mayen
(GMT -1) America/Scoresbysund
(GMT +0) Africa/Ouagadougou
(GMT +0) Africa/Accra
(GMT +0) Africa/Conakry
(GMT +0) Atlantic/Reykjavik
(GMT +0) Africa/Casablanca
(GMT +0) Africa/Nouakchott
(GMT +0) Africa/Freetown
(GMT +0) Africa/Sao_Tome
(GMT +0) GMT
(GMT -5) America/Port-au-Prince
(GMT -5) America/New_York
(GMT -4) America/Antigua
(GMT -4) America/Curacao
(GMT -4) America/Barbados
(GMT -4) America/Manaus
(GMT -4) America/Santo_Domingo
(GMT -4) America/Guadeloupe
(GMT -4) America/St_Kitts
(GMT -4) America/Martinique
(GMT -4) America/Puerto_Rico
(GMT -4) America/Port_of_Spain
(GMT -4) America/Tortola
(GMT -4) America/Caracas
(GMT -4) Atlantic/Bermuda
(GMT -4) America/Halifax
(GMT -4) America/Thule
(GMT -4) America/Santiago
(GMT -3) CNT
(GMT -3) America/Cayenne
(GMT -3) America/Montevideo
(GMT -3) AGT
(GMT -3) America/Miquelon
(GMT -3) BET
(GMT -2) Atlantic/South_Georgia
(GMT -1) Atlantic/Cape_Verde
(GMT -1) Atlantic/Azores
(GMT +0) Africa/Abidjan
(GMT +0) Africa/Banjul
(GMT +0) Africa/Bissau
(GMT +0) Africa/Monrovia
(GMT +0) Africa/Timbuktu
(GMT +0) Atlantic/St_Helena
(GMT +0) Africa/Dakar
(GMT +0) Africa/Lome
(GMT +0) UTC

(GMT +0) Atlantic/Faeroe
(GMT +0) Europe/Dublin
(GMT +0) Europe/London
(GMT +1) Africa/Porto-Novo
(GMT +1) Africa/Kinshasa
(GMT +1) Africa/Libreville
(GMT +1) Africa/Niamey
(GMT +1) Africa/Ndjamena
(GMT +1) Africa/Algiers
(GMT +1) Europe/Tirane
(GMT +1) Europe/Brussels
(GMT +1) Europe/Prague
(GMT +1) Europe/Copenhagen
(GMT +1) Europe/Gibraltar
(GMT +1) Europe/Rome
(GMT +1) Europe/Luxembourg
(GMT +1) Europe/Monaco
(GMT +1) Africa/Windhoek
(GMT +1) Europe/Oslo
(GMT +1) Europe/Stockholm
(GMT +1) Europe/Paris
(GMT +2) Africa/Bujumbura
(GMT +2) Africa/Lubumbashi
(GMT +2) Africa/Blantyre
(GMT +2) Africa/Kigali
(GMT +2) Africa/Mbabane
(GMT +2) Africa/Harare
(GMT +2) Africa/Johannesburg
(GMT +2) Europe/Minsk
(GMT +2) Europe/Tallinn
(GMT +2) ART
(GMT +2) Europe/Athens
(GMT +2) Asia/Amman
(GMT +1) Europe/Vilnius
(GMT +2) Europe/Chisinau
(GMT +2) Europe/Kaliningrad
(GMT +0) Atlantic/Canary
(GMT +0) Europe/Lisbon
(GMT +1) Africa/Luanda
(GMT +1) Africa/Bangui
(GMT +1) Africa/Douala
(GMT +1) Africa/Malabo
(GMT +1) Africa/Lagos
(GMT +1) Africa/Tunis
(GMT +1) Europe/Andorra
(GMT +1) Europe/Vienna
(GMT +1) Europe/Zurich
(GMT +1) Europe/Berlin
(GMT +1) Europe/Madrid
(GMT +1) Europe/Budapest
(GMT +1) Europe/Vaduz
(GMT +2) Africa/Tripoli
(GMT +1) Europe/Malta
(GMT +1) Europe/Amsterdam
(GMT +1) Europe/Warsaw
(GMT +1) Europe/Belgrade
(GMT +1) ECT
(GMT +2) Africa/Gaborone
(GMT +2) Africa/Maseru
(GMT +2) Africa/Maputo
(GMT +2) Africa/Khartoum
(GMT +2) Africa/Lusaka
(GMT +2) CAT
(GMT +2) Europe/Sofia
(GMT +2) Asia/Nicosia
(GMT +2) Africa/Cairo
(GMT +2) Europe/Helsinki
(GMT +2) Asia/Jerusalem
(GMT +2) Asia/Beirut
(GMT +2) Europe/Riga
(GMT +2) Europe/Bucharest
(GMT +2) Asia/Damascus

(GMT +2) Europe/Kiev
(GMT +2) EET
(GMT +3) Africa/Djibouti
(GMT +3) Africa/Addis_Ababa
(GMT +3) Africa/Nairobi
(GMT +3) Asia/Kuwait
(GMT +3) Asia/Qatar
(GMT +3) Africa/Dar_es_Salaam
(GMT +3) Asia/Aden
(GMT +3) Asia/Riyadh
(GMT +2) Europe/Simferopol
(GMT +3) Asia/Tehran
(GMT +4) Asia/Dubai
(GMT +4) Asia/Muscat
(GMT +4) Indian/Mahe
(GMT +4) NET
(GMT +4) Asia/Aqtau
(GMT +4) Asia/Kabul
(GMT +4) Asia/Tbilisi
(GMT +5) Indian/Maldives
(GMT +5) Asia/Ashkhabad
(GMT +5) Asia/Karachi
(GMT +5) Asia/Bishkek
(GMT +5) Asia/Yekaterinburg
(GMT +5) IST
(GMT +6) Antarctica/Mawson
(GMT +6) Asia/Colombo
(GMT +6) BST
(GMT +6) Asia/Novosibirsk
(GMT +6) Asia/Rangoon
(GMT +7) Asia/Jakarta
(GMT +7) Asia/Vientiane
(GMT +7) VST
(GMT +7) Asia/Krasnoyarsk
(GMT +8) Australia/Perth
(GMT +8) Asia/Hong_Kong
(GMT +2) Europe/Istanbul
(GMT +3) Asia/Bahrain
(GMT +3) Africa/Asmera
(GMT +3) EAT
(GMT +3) Indian/Comoro
(GMT +3) Indian/Antananarivo
(GMT +3) Africa/Mogadishu
(GMT +3) Africa/Kampala
(GMT +3) Indian/Mayotte
(GMT +3) Asia/Baghdad
(GMT +3) Europe/Moscow
(GMT +3) MET
(GMT +4) Indian/Mauritius
(GMT +4) Indian/Reunion
(GMT +4) Asia/Yerevan
(GMT +4) Asia/Baku
(GMT +4) Europe/Samara
(GMT +5) Indian/Kerguelen
(GMT +5) Indian/Chagos
(GMT +5) Asia/Dushanbe
(GMT +5) Asia/Tashkent
(GMT +5) PLT
(GMT +5) Asia/Aqtobe
(GMT +5) Asia/Calcutta
(GMT +5) Asia/Katmandu
(GMT +6) Asia/Thimbu
(GMT +6) Asia/Dacca
(GMT +6) Asia/Almaty
(GMT +6) Indian/Cocos
(GMT +7) Indian/Christmas
(GMT +7) Asia/Phnom_Penh
(GMT +7) Asia/Saigon
(GMT +7) Asia/Bangkok
(GMT +8) Antarctica/Casey
(GMT +8) Asia/Brunei
(GMT +8) Asia/Ujung_Pandang

(GMT +8) Asia/Macao
(GMT +8) Asia/Manila
(GMT +8) Asia/Taipei
(GMT +8) CTT
(GMT +8) Asia/Irkutsk
(GMT +9) Asia/Pyongyang
(GMT +9) Pacific/Palau
(GMT +9) JST
(GMT +9) Australia/Darwin
(GMT +9) Australia/Adelaide
(GMT +10) Australia/Hobart
(GMT +10) Pacific/Truk
(GMT +10) Pacific/Saipan
(GMT +10) Australia/Brisbane
(GMT +10) Australia/Sydney
(GMT +10) Australia/Lord_Howe
(GMT +11) Pacific/Efate
(GMT +11) SST
(GMT +11) Asia/Magadan
(GMT +12) Pacific/Kosrae
(GMT +12) Pacific/Majuro
(GMT +12) Pacific/Funafuti
(GMT +12) Pacific/Wallis
(GMT +12) Antarctica/McMurdo
(GMT +12) Pacific/Auckland
(GMT +12) Pacific/Chatham
(GMT +13) Pacific/Tongatapu
(GMT +14) Pacific/Kiritimati
(GMT +8) Asia/Kuala_Lumpur
(GMT +8) Asia/Singapore
(GMT +8) Asia/Shanghai
(GMT +8) Asia/Ulan_Bator
(GMT +9) Asia/Jayapura
(GMT +9) Asia/Seoul
(GMT +9) Asia/Tokyo
(GMT +9) Asia/Yakutsk
(GMT +9) ACT
(GMT +9) Australia/Broken_Hill
(GMT +10) Antarctica/DumontDUrville
(GMT +10) Pacific/Guam
(GMT +10) Pacific/Port_Moresby
(GMT +10) Asia/Vladivostok
(GMT +10) AET
(GMT +11) Pacific/Ponape
(GMT +11) Pacific/Guadalcanal
(GMT +11) Pacific/Noumea
(GMT +11) Pacific/Norfolk
(GMT +12) Pacific/Tarawa
(GMT +12) Pacific/Nauru
(GMT +12) Pacific/Wake
(GMT +12) Pacific/Fiji
(GMT +12) Asia/Kamchatka
(GMT +12) NST
(GMT +13) Pacific/Enderbury
(GMT +13) Asia/Anadyr

C

Preconfigured Change Request Fields

This appendix lists HP Release Control's default set of preconfigured change request fields, which includes two types of fields: predefined fields and custom fields. The data for these fields can originate from the service desk or from HP Release Control.

This appendix includes:

Predefined Fields

Predefined fields are non-editable fields based on ITIL standards, which are common to most service desk applications. The following **Predefined** fields are included in HP Release Control:

Name	Description
actual-end-time	The actual change activity's completion time.
actual-start-time	The actual change activity's start time.
approved-groups	A list of the user groups who have already approved the change request.
approvals-required	A list of the user groups who can only approve a change after user groups in the Current Pending list have already approved or disapproved.
calculated-risk	The risk value calculated for the change request.

Name	Description
collision-severity	The collision severity level evaluated for the request.
contact-email	The email of the contact person designated as responsible for the change request's creation.
contact-location	The location of the contact person designated as responsible for the change request's creation.
contact-person	Name of the contact person designated as responsible for the change request's creation.
contact-phone	The phone number of the contact person designated as responsible for the change request's creation.
creating-service-desk	The service desk on which this change request was created.
creation-time	The time at which the change request was created.
current-pending-groups	a list of user groups whose approval is still required.
description	A description of the change request.
down-end-time	The end of the down time period during change implementation.
down-start-time	The beginning of the down time period during change implementation.
ignore-detection	Indicates whether HP Release Control should try to detect the change request or skip its detection during the detection stage.
impact-severity	The impact severity level evaluated for the request.
implementation-outcome	A report of the change implementation. The implementor submits this report.
implementors	A list of users assigned to implement the change.
internal-id	An ID value used internally by HP Release Control.

Name	Description
is-abnormal	Used to determine if a change request is considered normal in terms of the time period in which it was or should be implemented.
lastImpact-cis-label	A list of all CIs involved in the impact analysis calculation for the relevant change request.
last-impact-time	The last time the change request's impact was calculated.
last-update-time	The last time the change request was updated.
number-of-comments	The number of comments created for the change request.
origin-url	A URL address that points to the original change request in the service desk application.
planned-end-time	The change activity's planned end time.
planned-start-time	The change activity's planned start time.
priority	A priority assigned to the request by the user creating the request.
request-id	An ID value that originated in the service desk application.
review-comments	Comments about the change request. Submitted during post implementation review.
review-customer-satisfaction	The customer (the person who opened the request ticket) satisfaction for the change request. Submitted during post implementation review.
review-outcome	The change request's outcome. Submitted during post implementation review.
review-planning-satisfaction	The level of planning satisfaction for the change request. Submitted during post implementation review.
review-time	The time the change request was reviewed (post implementation review).

Name	Description
source-itil-entity	The ITIL entity out of which the change request was created (incident, problem, requirement).
subcategory	Elaborates on the **category** field, and describes the type of change request in further detail.
status	The current status of the change request.
summary	A short summary of the change request.
ticket-level	The hierarchy level of the change request. This information originates from service desk.
user-estimated-risk	The risk level of the change request as evaluated by the creating user.

Custom Fields

Custom fields are editable fields that are recommended for use in order to optimize HP Release Control analysis features. The following **Custom** fields are included in HP Release Control:

Name	Description
category	The category describing the type of change request.
changed-ci-list	The list of CIs that are part of the planned change stored by CI name. Submitted by the user who creates the change.
changed-ci-id-list	The list of CIs that are part of the planned change stored by HP Universal CMDB ID. Submitted by the user who creates the change.
departments-involved	The number of different departments from which the change implementors emanate.
emergency	Indicates that the change request is handled according to the Emergency Change procedure.
implementor-experience	The implementor's level of experience regarding the work involved in the change.

Name	Description
involved-users	The number of users using the business CIs involved in the change.
initiated-by	The person initiating the request (first level change requests only).
is-backout-possible	Indicates whether there is a valid backout plan.
is-outage-planned	Indicates whether an outage is planned as part of the change.
is-sox-app-involved	Indicates whether a SOX application is involved in the change.
is-tested	Indicates whether the change was tested in a testing environment.
new-deployment	Indicates whether the change is a deployment of new hardware, a major feature, or a business CI.
opened-by	The person initiating the request (second level change requests only).
past-experience	The success ratio of similar changes in the past.
recent-incidents	Indicates whether a business CI involved in the change had major incidents within the two previous weeks.
request-end-date	The latest date by which to implement the request.
scheduled-downtime-end	The change activity's planned downtime end time.
scheduled-downtime-start	The change activity's planned downtime start time.
subcategory	Elaborates on the **category** field, and describes the type of change request in further detail.
site-location	The location of the site where the change will take place. Can be used in collision calculation.
sla-status	Indicates whether the SLA of a business CI involved in the change is close to being breached.

Name	Description
technology-experience	The amount of time (in quarters) that has transpired since the technology involved in the change was introduced to the organization.
urgency	The urgency assigned to the request by the request initiator.
vip-users	Indicates whether there are any VIP users using business CIs involved in the change.

D

Log Files

This appendix describes the log files available in HP Release Control. These log files are located in the **<HP Release Control installation directory>\logs** directory.

The following table describes each of the HP Release Control log files:

Log name	Usage
ccm_axis	Log file for Axis Open Source, which facilitates Web service communication between a service desk application and HP Release Control.
ccm_c3p0	Log file for the interactions with the database involving the **c3p0** database connection pool.
ccm_client	Log file for requests initiated from the user interface or from Web services.
ccm_cmdb	Log file for the module responsible for interfacing with HP Universal CMDB.
ccm_datamodel	Log file for most of the interactions between HP Release Control and the database.
ccm_general	Log file for the HP Release Control console messages that were formerly displayed in the Tomcat console.
ccm_genericinfra	Log file for infrastructure utilities such as settings and scripting.
ccm_hibernate	Log file for the interactions with the database involving the **hibernate** object to database mapper.
ccm_infra	Log file for infrastructure utilities that depend on the database and enumerations.

Log name	Usage
ccm_services	Log file for HP Release Control server requests. Contains information regarding the change request analysis process (for example, impact and collision analysis), notification deliveries, and risk recalculations, as well as other data.
ccm_reporting	Log file for the HP Release Control reporting module.
ccm_sdi	Log file for the Service Desk Integration module (SDI). Contains information on the process of collection and conversion of change requests, until they reach the CCM_QUEUED_CHANGES input queue of the HP Release Control platform.
ccm_security	Log file for security infrastructure issues.
ccm_dashboard	Log file for the dashboard module.
ccm_jobs	Log file containing information regarding job details in the system.

When you are investigating an incident, it is recommended that you begin by looking through the log files for the Service Desk Integration module (**ccm_sdi**) or for the HP Release Control server requests (**ccm_services**), depending on which part of the change request process you want to investigate.

Note: You configure the log file properties in the **<HP Release Control installation directory>\conf\ccmlog4j.properties** file. This file contains a list of log file definitions that you can modify. For more information about configuring the log file properties, see "Configuring Log File Properties" on page 223.

E

Database Configuration and Maintenance

This appendix provides important guidelines for configuring and maintaining both Microsoft SQL Server and Oracle Server databases.

This appendix includes:

Guidelines for MS SQL Server Databases

It is recommended that you design a maintenance plan, update index statistics, and activate the snapshot isolation feature for the MS SQL Server database as described below.

Data and Index Page Reorganization

The HP Release Control database may become fragmented after processing a certain number of requests. To prevent fragmentation from seriously affecting client-side performance, it is recommended that you design a maintenance plan that causes the indexes on the database tables to be dropped and recreated.

To create a maintenance plan:

1. Open the MS SQL Server Enterprise Manager.
2. Under the relevant MS SQL Server registration, select **Management**.

3. Right-click **Database Maintenance Plans** and select **New Maintenance Plan**. The Database Maintenance Plan Wizard opens to guide you through the required definition parameters.
4. Choose the database for which you want to create a maintenance plan and click **Next**.
5. Select the **Reorganize data and index pages** check box and choose the **Change free space per page percentage to** option.
6. Set the free space per page to **10** percent and click **Next**.
7. Accept all the other default settings in the wizard and save your maintenance plan.

Note: After the maintenance plan has been executed, statistics should be updated.

Updating Statistics

MS SQL Server 2000 allows statistical information regarding the distribution of values in a column to be created. This statistical information can be used by the query processor to determine the optimal strategy for evaluating a query. When an index is being created, MS SQL Server automatically stores statistical information regarding the distribution of values in the indexed columns. The query optimizer in MS SQL Server uses these statistics to estimate the cost of using the index for a query. As the data in a column changes, index and column statistics can become out-of-date and cause the query optimizer to make less than optimal decisions regarding the processing of a query.

It is recommended that you update index statistics to provide the query optimizer with up-to-date information about the distribution of data values in the tables. With more information about the data stored in the database, the query optimizer is able to make better judgments about the best way to access data.

By default, the **auto update statistics** database option is enabled, but if this option has been disabled, it is strongly recommended that you create an automatic task to update statistics for the database on a daily basis, as the data is frequently changed. The job should execute the **sp_updatestats** API against the specific database.

Activating Snapshot Isolation

We strongly recommend using the snapshot isolation feature in SQL Server 2005. To do this, execute the following command once after creating the database:

```
alter database <ccm_database_name> set read_committed_snapshot on
```

For more information about the SQL Server snapshot isolation feature, see http://msdn.microsoft.com/en-us/library/tcbchxcb(VS.80).aspx.

Guidelines for Oracle Server Databases

It is recommended that you set cache attributes and collect statistics for the Oracle Server database as described below.

Setting Cache Attributes

Set the **cache\nocache** attribute of the **CCM_CHANGES** table to **cache** by executing the following statement:

```
alter table CCM_CHANGES cache;
```

Gathering Statistics

It is recommended that you gather statistics once a day. To do so effectively, perform the steps in the following procedure.

To gather statistics once a day:

1 Turn on the **MONITORING** flag to the tables in the HP Release Control schema by executing the following:

```
exec dbms_stats.alter_schema_tab_monitoring('<name of oracle schema>',TRUE);
```

2 Create the following job to collect statistics on a daily basis at midnight:

```
declare
    job_num number;
begin
    dbms_job.submit(job_num,'dbms_stats.gather_schema_stats
    (ownname=>"<name of oracle schema>", options=>"GATHER AUTO",
    cascade=>TRUE);', sysdate+1/1440,'trunc(sysdate+1)');
    commit;
end;
/
```

Caution:

- The **job_queue_processes** parameter must be set to a positive value to allow the job to be executed.
- As of Oracle 10g, the statistics gathering process is automated by default. There is an automatic job named **GATHER_STATS_JOB** running on a daily basis and there is therefore no need to perform the actions described in the above procedure.

Database Pool Configuration Settings

You can modify the database pool configuration settings for an MS SQL or Oracle Server database or user schema, if required. For details on configuring database pool settings, refer to the following URL: http://www.mchange.com/projects/c3p0/index.html

By default, HP Release Control does not log MS SQL or Oracle Server database statements. To modify this default setting, ensure that the following line in the **<HP Release Control installation directory>\conf\ccmlog4j.properties** file is not commented out:

```
log4j.logger.org.hibernate.SQL=debug
```

F

Utilities

This appendix describes a number of HP Release Control utilities that are available.

Note: If you are have upgraded HP Release Control but want to run a utility from a previous installation, you must change the **CCM_HOME** variable by entering **set CCM_HOME=<previous installation directory>** from the command line before running the utility.

This appendix includes:

Change Cleaner

The change cleaner utility enables you to count or remove HP Release Control database change requests. You can also count or remove change requests until a specified date.

To count or remove requests in the database:

1. Make sure the server is running.
2. In the Command Prompt window, change the command line directory to: **<HP Release Control installation directory>\bin**.
3. Run the following command:

```
ChangeCleaner.bat <options>
```

You can use the following command line <options>:

Option	Description
-c **--count**	Counts the number of changes.
-cb <yyyy-MM-dd> **--count-before <yyyy-MM-dd>**	Counts the number of changes before the specified date.
-cf <filter-name> **--count-filter <filter-name>**	Counts number of changes that are included in the specified filter. See "Specifying a Filter: Notes and Limitations" below.
-h **--help**	Prints this message.
-ra **--remove-all**	Removes all changes from the database.
-rb <yyyy-MM-dd> **--remove-before <yyyy-MM-dd>**	Removes changes before the specified date.
-rf <filter-name> **--remove-filter <filter-name>**	Removes the changes and dependent tasks that are included in the specified filter. See "Specifying a Filter: Notes and Limitations" below.

For example, to remove the changes planned or implemented before the 20th of September 2008, run the following command:

```
ChangeCleaner.bat -rb 2008-09-20
```

Specifying a Filter: Notes and Limitations

Using the change cleaner utility, you can count or remove all change requests included in a specified filter using the **-cf**, **--count-filter**, **rf**, or **--remove-filter** options. The following notes and limitations apply to these options:

- The filters are defined in the HP Release Control Analysis or Director module.
- You can only specify filters created by users with the administrator role.
- If the same filter name has been used for more than one filter, you cannot specify that filter name.
- The **Hierarchy level** in the filter you specify needs to be defined as C**hanges and Independent Tasks**.
- Filter that depend on the context of the user are not supported. (For example, **Requests affecting my business CIs**).

User Importer

The user importer utility enables you to import a list of defined users and user properties from a CSV file to HP Release Control.

To import users via this utility:

1. Make sure the server is running.
2. In the Command Prompt window, change the command line directory to: **<HP Release Control installation directory>\bin**
3. Run the following command:

```
ImportUsers.bat <options>
```

The command line <options> can be:

Option	Description
--list-charsets	Since you can use this utility to import files from a variety of character sets, use this option to see a list of the available character sets. You can then use the **--charset** option to specify a character set.
--charset <charset>	Specify the character set of the file (useful for Asian languages). If this option is not specified, the default file character set is UTF-8.
-f <file> **--file <file>**	Imports the file specified in <file>.
-r <level> **--report-level <level>**	Specify the level of error reporting for the import, where <level> can be 0 - no reporting, 1 - report errors, 2 - report warnings, 3 - report all. If this option is not specified, the default level is 1 - report errors.
-h **--help**	Prints this message.

The following is an example of a CSV file with one user:

```
USERNAME,PASSWORD,FIRST_NAME,LAST_NAME,EMAIL,BUSINESS_ID
jdoe,jdoe,John,Doe,jon.doe@hp.com,jdoe
```

Updating User Details

The **business ID** and **username** fields are unique identifiers. There cannot be two different users in HP Release Control with the same business ID or the same user name.

The **business ID** field is also the business key. To update the details of an existing user, import a user with the same business ID and change the relevant details.

For example, assume there is a user John Doe, with business ID **123** and username **john_doe**. If you want to change John Doe's user name to **johnd,** import a user with business ID **123** and user name **johnd**. John Doe's user name will now be updated to **johnd**. However, if the user name **johnd** already exists in HP Release Control, the user will not be updated.

File Locator

The file locator utility enables you to locate HP Release Control configuration files, log files, and/or files that were modified following installation.

To use the file locator utility:

1 Change the command line directory to **<HP Release Control installation directory>\bin**.

2 Run the following command:

```
LogGrabber.bat <options>
```

The command line <options> can be:

Option	Description
-c **--conf**	Locate configuration files.
-l **--logs**	Locate log files.
-m **--modified**	Locate files that were modified following installation.
-h **--help**	Print this message.

To locate a combination of the above, combine the above commands. For example, to locate configuration, log, and modified files, run:

```
LogGrabber.bat -clm
```

Populate Batch File

The populate batch file enables you to create tables in the HP Release Control database.

Note: This utility deletes any data that was previously stored in the database.

To use the populate batch file:

1. Change the command line directory to **<HP Release Control installation directory>\bin**.
2. Run the following command:

```
Populate.bat i
```

Queue Manager

The queue manager utility enables you to manage the change requests that are waiting to enter HP Release Control from the service desk application.

To use the queue manager utility:

1. Make sure the server is running.
2. Change the command line directory to **<HP Release Control installation directory>\bin**.
3. Run the following command:

```
QueueManager.bat <options>
```

The command line <options> can be:

Option	Description
-l **--list**	List all the change requests in the queue.
--remove all	Delete all change requests in the queue.
--remove first	Delete the first change request in the queue.
-h **--help**	Print this message.

For example, to delete the first change request in the queue, run:

```
QueueManager.bat --remove first
```

Web Server Configurer

The Web server configure utility enables you to modify your Web server installation.

To use the Web server configure utility:

1. Change the command line directory to **<HP Release Control installation directory>\bin**.
2. Run the following command:

```
WebServerConfigurer.bat <options>
```

The command line <options> can be:

Option	Description
config apache <port> <apache home directory>	Configure an Apache Web server. Specify the Apache configuration options: **<port>** - the port used by the Apache Web server. **<apache home directory>** - the Apache Web server installation directory.
config IIS, <port> <version> <RC Website>	Specify the configuration options for an IIS server: **<port>** - the port used by the server. The default port is 80. **<version>** - Web server version, either 5 or 6. **<RC Website>** - the Web site defined for Release Control. In a new IIS installation, the Release Control default site is called **Default Web Site**.
remove-config	Configures HP Release Control to work without a Web server. This command will not uninstall the Web server. **Note:** In the **<HP Release Control installation directory>\conf\server.settings** file, the HP Release Control port number in the **server-address** property will be reset to the Tomcat default port (8080). Ensure that the HP Release Control and Tomcat port number are the same.

For example:

➤ To install an Apache server using port 80, run:

```
WebServerConfigurer.bat install apache 80 "C:\Apache Software
Foundation\Apache 2.2"
```

➤ To configure an IIS server version 5 using port 80 and the default Web site, run:

```
WebServerConfigurer.bat config IIS 80 5 "Default Web Site"
```

➤ To remove the Web server configuration, run:

```
WebServerConfigurer.bat remove-config
```

G

Ticket Processing Error Handling

This appendix describes the way in which HP Release Control handles errors during the conversion and analysis of change request tickets.

This appendix includes:

Error Handling during Change Request Conversion

Change requests are converted from their service desk application formats to a generic format using service desk application-specific adapters. (For more information, see the section about converting HP Release Control requests in the *HP Release Control Deployment Guide*.)

During the conversion process, HP Release Control may encounter errors with a ticket in the service desk. When an error is detected in one of the tickets, HP Release Control handles these errors as follows:

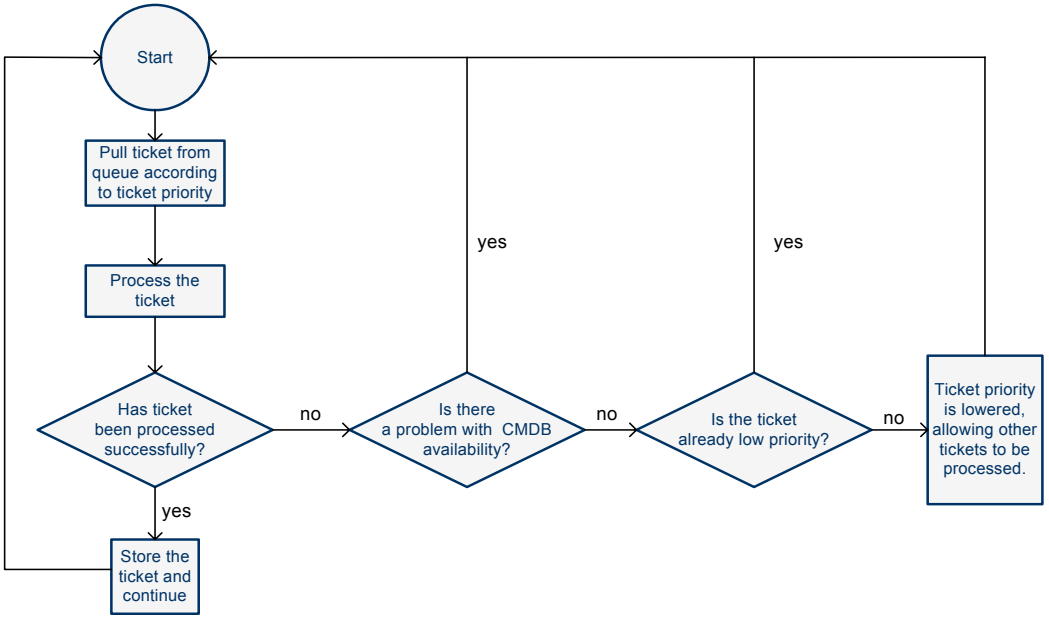
- **If all of the tickets in the service desk are being converted (initial load)**, a message is written to the **ccm_sdi** log file and the conversion process is stopped.
- **If only updated tickets are being converted (polling),** HP Release Control skips over the problematic ticket and continues converting the remaining tickets. A message is written to the **ccm_platform** log.

You can configure HP Release Control to send email notifications when an error occurs during the processing of change request tickets. For more information, see "Configuring Email Notification of Errors" on page 295.

Error Handling during Change Request Analysis

HP Release Control analyzes change requests, performing calculations such as impact, risk and collision analysis (For more information, see Chapter 9, "Before Configuring Change Request Analysis").

During the analysis process, HP Release Control may encounter errors with a ticket in the service desk. The following diagram describes the process of error handling during the analysis of change request tickets.



As illustrated in the above diagram, if there is a specific problem with one of the tickets that is not related to a CMDB configuration issue, the priority of the ticket is lowered. The ticket is moved to the end of the queue, enabling other tickets with higher priority to be processed first.

You can configure HP Release Control to send email notifications when an error occurs during the processing of change request tickets. For more information, see "Configuring Email Notification of Errors" on page 295.

Configuring Email Notification of Errors

You can configure HP Release Control to send email notification when an error occurs during the processing of change request tickets.

To receive email notification for errors during ticket processing:

1 Open the **HP Release Control\Conf\ccmlog4j.properties** file for editing.

2 Configure HP Release Control to send email notifications for errors.

- To receive email notifications about errors during **ticket conversion**, uncomment the following line:

```
log4j.logger.sdi_admin=info, ccm_cp_email
```

- To receive email notifications about errors during **ticket processing**, uncomment the following line:

```
log4j.logger.change_process=info, ccm_cp_email
```

3 Configure the email properties in the following section:

```
log4j.appender.ccm_cp_email=org.apache.log4j.net.SMTPAppender
log4j.appender.ccm_cp_email.from=
log4j.appender.ccm_cp_email.SMTPHost=
log4j.appender.ccm_cp_email.SMTPUsername=
log4j.appender.ccm_cp_email.SMTPPassword=
log4j.appender.ccm_cp_email.to=
log4j.appender.ccm_cp_email.subject=CCM Change Process Problem
log4j.appender.ccm_cp_email.evaluatorClass=com.mercury.onyx.genericinfra.utils.logs
.CountingTriggeringEventEvaluator
log4j.appender.ccm_cp_email.layout=org.apache.log4j.HTMLLayout
log4j.appender.ccm_cp_email.layout.title=CCM Change Process Problem
```

Index

E

F

G

H

I

K

L

M