Release Control

Software Version: 9.60

For the supported Windows® and Linux® operating systems

User Guide

Document Release Date: January 2018
Software Release Date: January 2018

MICRO FOCUS®

Legal Notices

Warranty

Restricted Rights Legend

Copyright Notice

Trademark Notices

Disclaimer

Certain versions of software and/or documents ("Material") accessible here may contain branding from Hewlett-Packard Company (now HP Inc.) and Hewlett Packard Enterprise Company. As of September 1, 2017, the Material is now offered by Micro Focus, a separately owned and operated company. Any reference to the HP and Hewlett Packard Enterprise/HPE marks is historical in nature, and the HP and Hewlett Packard Enterprise/HPE marks are the property of their respective owners.

Documentation Updates

To check for recent updates or to verify that you are using the most recent edition of a document, go to: https://softwaresupport.softwaregrp.com.

This site requires that you register for a Software Passport and to sign in. To register for a Software Passport ID, click **Register for Software Passport** on the Micro Focus Support website at https://softwaresupport.softwaregrp.com.

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

Support

Visit the Micro Focus Support site at: https://softwaresupport.softwaregrp.com.

This website provides contact information and details about the products, services, and support that Micro Focus offers.

Micro Focus 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 website to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up 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 a Software Passport user and to sign in. Many also require a support contract. To register for a Software Passport ID, click **Register for Software Passport** on the Micro Focus Support website at https://softwaresupport.softwaregrp.com.

To find more information about access levels, go to: https://softwaresupport.softwaregrp.com/web/softwaresupport/access-levels.

Integration Catalog accesses the Micro Focus Integration Catalog website. This site enables you to explore Micro Focus Product Solutions to meet your business needs, includes a full list of Integrations between Micro Focus Products, as well as a listing of ITIL Processes. The URL for this website is https://softwaresupport.softwaregrp.com/km/KM01702731.

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Contents

Welcome to This Guide

Welcome to the *Release Control User Guide*, which explains how to use and configure Release Control software. Release Control provides a common platform of decision support for Change Advisory Board members and implementation teams during the release life cycle. Release Control analyzes each change request in the system and provides real-time information and alerts during implementation. In addition, 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: Introduction
  Describes the various components of the Release Control application.
- Part II: User Settings
  Describes how to view and configure user properties and Analysis module settings for the current Release Control user.
- Part III: Analyzing Changes
  Describes the different change request views and change request information displayed across the various tabs in the Analysis module, and how to filter change requests, action items, and activities.
- Part IV: Monitoring and Implementing Activities
  Describes the Director module where you can monitor the status of change requests scheduled for implementation, the Implementor module where you manage the activities you are implementing, and how you can communicate between them.

- Part V: Dashboard
  Describes how to work with the Release Control Dashboard, which displays change request data in real time using graphical displays.
- Part VI: Administration
  Describes how to configure the various parts of the Release Control system.
- Part VII: Appendices
  Describes Release Control log files, database configuration and maintenance, Release Control utilities, and error handling during the change request conversion process.

Who Should Read this Guide

This guide is intended for members of the Change Advisory Board and others involved in the change process who are responsible for assessing the business impact of change requests on your organization's IT environment and approving or rejecting the proposed changes, and for the change implementors and NOC users who are responsible for implementing the changes and for monitoring the implementation progress.

Release Control Documentation

Release Control comes with the following documentation:

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

- in PDF format in the Release Control installation package
- in PDF format by selecting **Help > Documentation Library** from the Release Control application

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

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

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

Release Control Release Notes provides information on what's new in the current version of the product as well as comprehensive information on known problems and limitations. The Release Notes is available in HTML format in the Release Control installation package.

> **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

Software Support accesses the Micro Focus 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 > Software Support**.

Most of the support areas require that you register as a Software Passport user and sign in. Many also require a support contract. To find more information about access levels and register for a Software Passport user ID, go to the Micro Focus Software Support website as well.

Software Web Site accesses the Micro Focus Software website. This site provides you with the most up-to-date information on Micro Focus Software products. This includes new software releases, seminars and trade shows, customer support, and more. Choose **Help > Software Web Site**.

Part I: Introduction

Introduction to Release Control

This chapter includes:

Concepts

- Overview of Release Control

Reference

- Accessing Release Control

Concepts

Overview of Release Control

In a typical release life cycle, after a change enters the system, the change goes through an **approval**, **implementation**, and **review** phase. Release Control supports each one of these phases in the release life cycle.

Approval

During the approval phase, the **Analysis module** provides a detailed analysis of each change request in the system. Change Advisory Board (CAB) members can view information such as the potential impact of the change and the possible risk involved in implementation. The CAB uses this information to make more informed and accurate decisions regarding the approval of planned changes.

In addition, the **collaboration feature** enables CAB members to provide feedback about planned changes, approve or deny the change requests, or retract the approval.

Implementation

During implementation, the **Director and Implementor modules** provide real-time information regarding change activities. Implementors and release teams are able to monitor the status of all change activities on a 24-hour timeline view. They receive alerts about issues such as scheduling, collisions, and delays, and use the implementation guidelines that were drawn up in the Analysis module during the approval phase.

Review

After implementation, the **Post Implementation Review (PIR) feature** provides a platform for reviewers to present their conclusions regarding the implemented change. Using information collected during the implementation phase, reviewers provide feedback about the overall success of the change and satisfaction levels of relevant parties.

Management and Administration

During the entire release life cycle, IT managers use the Release Control **Dashboard module** to view graphic displays of change request and activity data in real time. Release Control uses the **Administration module** to configure the Release Control properties and perform administration tasks in the system.

Reference

Accessing Release Control

You can access Release Control using a Web browser from any computer with a network connection (intranet or Internet) to the Release Control server. For details on Web browser requirements, see "Server System Requirements" in the *Release Control Deployment Guide*.

To access the Release Control login page and log in to Release Control:

1. In the Web browser, enter the URL http://<server_name>:<Tomcat server port>/ccm if you are not working with an identity management system, or http://<server_name>/ccm if you are working with an identity management system, where **server_name** is the name or IP address of the Release Control server.
2. Enter the login parameters (user name and password) of a user defined by the administrator and assigned to you, and click **Log In**. After logging in, the user name appears in the top right-hand corner of the screen. In a new installation, a user called **admin** with an **admin** password is created and can be used for initial access to the system.
3. Configure the user authentication mode, as described in Release Control User Authentication Overview.

To log out of Release Control:

When you have completed your session, click **Logout** in the top right-hand corner of the screen.

Part II: User Settings

User Preferences

This chapter includes:

Concepts

- User Preferences Overview

Reference

- User Preferences User Interface

Concepts

User Preferences Overview

Release Control enables you to view and configure user properties for the current Release Control user, select the business CIs you want to associate with the current user and configure the settings for the Analysis module.

For more information on configuring user settings, see User Configuration.

Reference

User Preferences User Interface

This chapter includes:

- Business CIs Pane
- Details Pane
- Grid Display Pane

- Quick Filter Display Pane
- User Workspace Pane

Business CIs Pane

This pane enables you to associate business CIs with the current user.

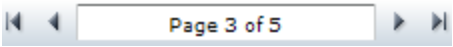
Associating a business CI with a user causes the user to receive notifications when a change is scheduled which impacts the business CI. Although the administrator is responsible for the initial association of business CIs with users, you can associate or remove business CI associations from the current user.

For details on how to define a new user by configuring settings—including basic user details and associated business CIs—for the user, see User Configuration.

To access	Select **Preferences** > **User Preferences** > **Business CIs**.

User interface elements are described below:

UI Elements (A-Z)	Description
	Show/Hide Obsolete. Toggle between hiding and displaying the obsolete CIs.
	Find. Search for a specific business CI by entering the name or part of a name in the search box. The search returns all business CIs that contain the entered string somewhere in the name. Click the **Find** button to run the search.
	Move the selected business CIs from the **Available Business CIs** list to the **My Business CIs** list. The business CI is associated with the current user
	Move the selected business CIs from the **My Business CIs** list to the **Available Business CIs** list. The business CI is not associated with the current user. **Note:** You can remove the association of a business CI with the current user only if the administrator did not require the user to view data for the business CI by enforcing the business CI for the user.
<View other pages>	To view other pages, use the left and right arrows. The number between the left and right arrows indicate which page is currently being displayed. For example, 3 of 5 means that the 3rd page out of 5

UI Elements (A-Z)	Description
	is being displayed. 
Available Business CIs	The business CIs in this list that are not associated with the current user.
My Business CIs	The business CIs in this list that are associated with the current user.

Details Pane

This pane enables you to view and modify the properties of the current Release Control user that were configured by the administrator.

To access	Select **Preferences** > **User Preferences** > **Details**.
Important Information	If you are working in identity management or LDAP mode, you cannot change the user's password.
See also	• Release Control User Authentication Overview • User Configuration

User interface elements are described below:

UI Elements (A-Z)	Description
Password	To change the user's password, type in a new password. This is the password by which the user logs in to Release Control. **Note:** If you are working in identity management or LDAP mode, you cannot change the user's password.
Retype password	Retype the password to confirm the password entered in the **Password** box. **Note:** If you are working in identity management or LDAP mode, you cannot change the user's password.

Grid Display Pane

This pane enables you to configure the change request fields for which you want to view data in Release Control.

To access	Select **Preferences** > **User Preferences** > **Analysis** > **Grid Display**.
Important Information	• The change request fields for which you want to view data in Release Control are defined in the Administrator module. For details, see Fields Pane. • A user-specific configuration defined in the Grid Display pane overrides the current configuration in the Administrator module. This definition applies only to the machine on which the specific user used to configure the change request fields.
See also	Change Requests — List View

User interface elements are described below:

UI Elements (A-Z)	Description
	Restore to Defaults. Restore the default fields as defined in the Administrator module.
	Find. Search for a specific column by entering the name or part of a name in the search box. The search returns all columns that contain the entered string somewhere in the name. Click the **Find** button to run the search.
	Add. Move the selected columns from the **Available Columns** list to the **Selected Columns** list. The columns appear in the Change Request pane.
	Remove. Move the selected fields from the **Selected Columns** list to the **Available Columns** list. The columns do not appear in the Change Request pane.
	Use the up and down arrows to determine the order in which the columns appear in the Change Request pane.
<View other pages>	To view other pages, use the left and right arrows. The number between the left and right arrows indicate which page is currently being displayed. For example, 3 of 5 means that the 3rd page out of 5 is being displayed. Page 3 of 5

UI Elements (A-Z)	Description
Available Columns	The list of available columns. **Note:** You can select multiple columns using the CTRL key.
Selected Columns	Displays the fields that appear in the Change Request pane. **Note:** You can select multiple columns using the CTRL key.

Quick Filter Display Pane

This pane enables you to define which fields appear in the Filters pane in the Analysis module. For details, see Filters Pane.

To access	• **In User Preferences:** Select **Preferences** > **User Preference** > **Quick Filter Display**. • **In the Administrator module:** Select **Configuration** tab > **Fields**. In the Available fields pane, click the **Manage Quick Filter Display** button to open the Quick Filter Display dialog box.
Important Information	• The results of modifications you make appear immediately in the Filters pane. • By default, the fields that are displayed in the Filters pane are defined by the administrator in **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Fields** > **Available Fields** pane > **Manage Quick Filter Display** button. • A user-specific configuration defined in the Quick Filter Display pane overrides the administrator's current configuration for this user.
See also	Filters Pane

User interface elements are described below:

UI Elements (A-Z)	Description
	Restore to Defaults. Restore the default fields as defined in the Administrator module.
	Find. Search for a specific field by entering the name or part of a name in the search box. The search returns all fields that contain the entered string somewhere in the name. Click the **Find** button to run the search.

UI Elements (A-Z)	Description
	Move the selected field from the **Available Fields** list to the **Selected Fields** list. The fields appear in the quick filter pane.
	Move the selected fields from the **Selected Fields** list to the **Available Fields** list. The fields do not appear in the quick filter pane.
	Use the up and down arrows to determine the order in which the fields appear in the quick filter pane.
<Viewing other pages>	To view other pages, use the left and right arrows. The number between the left and right arrows indicate which page is currently being displayed. For example, 3 of 5 means that the 3rd page out of 5 is being displayed. Page 3 of 5
Available Fields	The list of available quick filter fields. **Note:** You can select multiple fields using the Ctrl key.
Selected Fields	Displays the fields that appear in the quick filter pane. **Note:** You can select multiple fields using the Ctrl key.

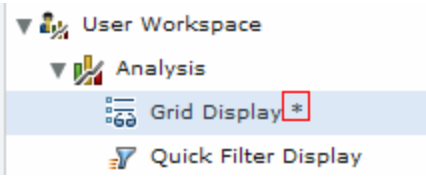
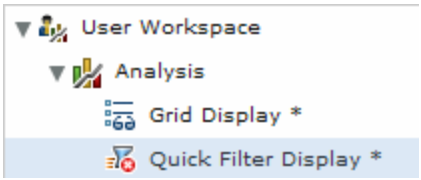
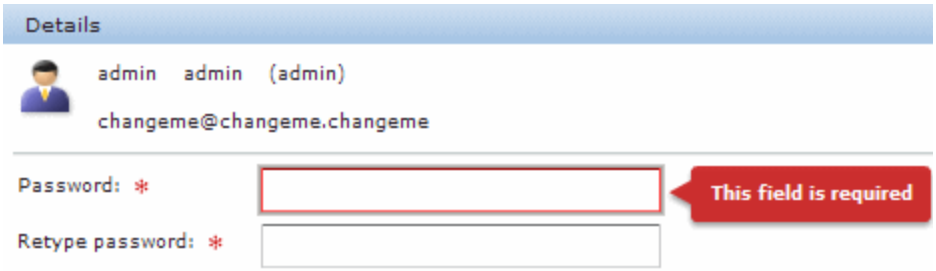
User Workspace Pane

This pane enables you to configure user properties for the current Release Control user.

To access	Select **Preferences** > **User Preferences** > **User Workspace**.
Important Information	If you are working in identity management or LDAP mode, you cannot change the user's password.
See also	• Release Control User Authentication Overview • User Configuration

User interface elements are described below:

UI Elements (A-Z)	Description
<User preferences	The selected option appears in the right pane. The following indicators appear: • If a change occurs in the selected option, an asterisk (*) appears to the right of

UI Elements (A-Z)	Description
tree in the left pane>	the selected option in the tree.  • If an invalid action has been taken, an appears attached to theicon at the left of the selected option in the tree.  Examples of invalid actions are: • The **Password** box in the Details pane is empty • The **Selected Fields** list in the Quick Filter Display pane contains no selected fields In such cases, a red frame appears around the relevant box to indicate that an invalid action has been taken. You can also hold the pointer over the red frame to display a description of the invalid action. 
Auto detect language settings	Select this option to instruct Release Control to use the default language configured for your machine. To use a different language, clear the **Auto detect time language settings** option and select the required language. If the selected language is not supported, Release Control uses the default language in the **System language** box in **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Server**. **Default:** Selected
Auto detect	Select this option to instruct Release Control to use the time zone that is

UI Elements (A-Z)	Description
time zone settings	configured for the Release Control server. To use a different time zone, clear the **Auto detect time zone settings** option and select the required time zone from the **Time zone** list. > **Note:** This option is disabled if the **Force client time zone** check box in **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Server** pane is selected. **Default:** Selected
Landing Page	Select the current module as the landing page. Navigate to the module to which you want Release Control to open and click **Use Current Page**. If you select to use the Analysis module as your landing page, Release Control also: • Opens the last displayed view. For example, **List** or **Calendar** format. For details, see Change Requests Toolbar Options. • Opens the last displayed filter in the Change Requests pane, including an unsaved filter. > **Note:** If the last displayed filter was the result of a Search for Request ID search, the Any filter is displayed. However, if the **Default changes filter name** box (select **Administrator** > **Configuration** tab > **Server**) contains a value other than **empty** (the **Any** filter), then Release Control displays the filter that appears in the **Default changes filter name** box. For details about filtering change requests, see Filtering Change Requests and Activities.
Last Visited Page	Release Control opens to the last module that was displayed before logging out. If the Analysis module was the last module to be displayed, Release Control also: • Opens the last displayed view. • Opens the last displayed filter in the Change Requests pane. For more information, see **Landing Page** above. > **Note:** By default, Release Control opens to the last page that was open.
Notify me on updates to items in	Enables you to receive notifications when certain modifications are made to your favorite change requests and action items.

UI Elements (A-Z)	Description
my Favorites list	

Part III: Analyzing Changes

Analysis Module

This chapter includes:

Concepts

Tasks

Reference

Concepts

Analysis Module Overview

The Analysis module displays a detailed analysis of each change request that has entered the system.

Change Advisory Board (CAB) members can view information such as the potential impact of the change and the possible risk involved in implementation. The CAB uses this information to make more informed and accurate decisions regarding the approval of planned changes.

In addition, the collaboration feature enables CAB members to provide feedback about planned changes, approve or deny the change requests. or retract the approval.

Release Control enables you to configure the settings for the Analysis module. For details, see User Preferences.

Action Items

Action items are tasks that one user can send another regarding a specific change request. The user to whom the action item is assigned—known in Release Control as the assignee—can choose to perform the task assigned to him or return the action item to its creator. If the assignee chooses to perform the task, he informs the creator that the action item is done once the work has been completed. The creator of the action item then closes the item or reopens it, as required.

When the assignee receives an action item for whose completion he must involve other users, the assignee can create one or more derived action items from the action item he was assigned. However, these action items are not directly associated with the original action item and their statuses do not impact upon the status of the original action item. The status of the original action item does not change until the original item's assignee informs the creator that the item is done.

To monitor specific action items, you can add the items to your **Favorites** list. You can also subscribe to receive email notifications when modifications are made to action items. In addition, you can forward an action item by email to other users for them to review the item or comment on it.

> **Notes:**
>
> - A change request can have multiple action items associated with it, but an action item can be associated with only one change request.
> - By default, Release Control automatically creates action items for certain change requests. For details, see Configure the Automatic Creation of Action Items.

Action items can be viewed in two places within the Analysis module:

- In the Action Items pane. You use the Action Items pane to view all the action items in your system, or those that meet certain filter criteria. For details, see Action Items Pane.
- In the Action Items view of the Collaboration tab. You use the Collaboration tab to view the action items associated with a specific change request. For details, see Collaborate > Action Items Tab.

Impact Analysis

Impact analysis calculates the effects of change requests on CIs. Both the CI details, and their relationships are imported from Universal CMDB. For information on how to set up and configure Release Control to calculate impact analysis, see Impact Analysis Rules Pane.

Release Control enables you to view the impact analysis calculation results for a change request in the Assess > Impact tab. The Assess > Impact tab displays the business and system CIs that are affected by the change request. This includes general information about the affected business or system CIs and an indication of the severity of the impact of the change request. For details, see Assess > Impact Tab.

Risk Analysis

For each change request, 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 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 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 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

Factor Name	Weight
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 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

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 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 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

Factor Name	Factor Score	Weight	Weighted Value
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.

To view the risk analysis for a change request, see Assess > Risk Tab.

Modeling Studio Integration Overview

> **Note:** This feature is relevant only if you are connected to Universal CMDB version 8.01 or later.

Impact analysis calculation results are based on the CIs that appear in the Impact CIs, Affected by, or Affects panes in the Assess > Impact tab. If there are CIs that should have been included in the calculation but do not appear in the Assess > Impact tab, or, CIs that do appear in the Impact tab but should not have been included in the calculation, the impact analysis calculation results are rendered inaccurate. For details about how to configure impact analysis, see Impact Analysis Rules Pane.

Release Control enables you to change the impact analysis calculation results for the change request by modifying the relevant business CI model in the Modeling Studio in Universal CMDB, directly from Release Control.

For example, if a host appears in the Impact CIs pane, but in actuality no longer exists in the model, it is still included in the impact results since Universal CMDB was not updated with this change. The impact analysis results are therefore inaccurate. For details, see the Assess > Impact Tab.

Viewing the Updated Results

Once Universal CMDB is updated with the required change, the impact analysis calculation results are updated. In the Impact CIs pane in the Assess > Impact tab, the updated results do not appear until the next time Release Control performs impact calculation. To see updated results, you can run a simulation in the Change Planner and view the simulation results in the Change Planner details pane. For details, see Change Planner Dialog Box.

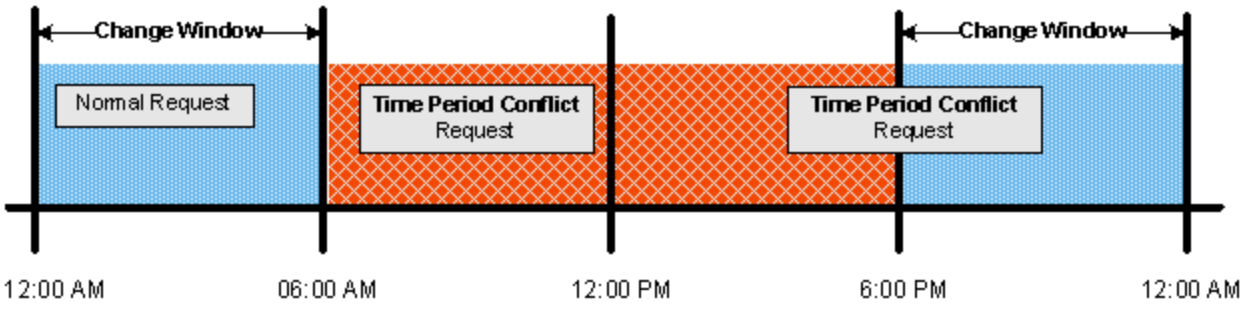
Time Periods

Time periods define when changes may and may not be implemented. The types of time periods are:

- **Change Window.** A period of time in which requests may be implemented.
- **Blackout.** A period of time in which requests may not be implemented.
- **Neutral to Changes.** A period of time indicating an external event, such as a holiday, which has no direct bearing on request implementation.

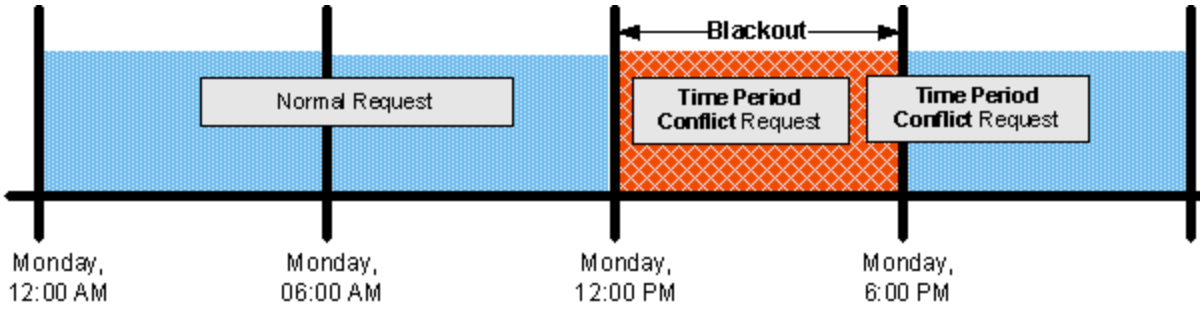
For example, to ensure that your company's service level agreements are upheld, you may define a **Change Window** time period such that changes to your corporate Web site may only take place from 12:00 AM to 6:00 AM or from 6:00 PM to 12:00 AM. For details on the recommended procedure for defining time periods, see Define Time Periods.

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. For details about viewing Time Period Conflicts, see Assess > Time Period Conflicts Tab.



Likewise, you may define a **Blackout** time period such that changes to the Web site may not take place on Mondays 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.



For details on how to configure time periods, see Time Periods Tab.

Change Request Collisions

Release Control automatically identifies change requests involving common key elements that are scheduled to take place at the same time or adjacent to one another, causing **change request collisions**.

> **Note:** All references to change requests in this chapter relate to change requests associated with action items as well.

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.

This section also includes:

- Collision Proximity Levels
- Causes of Collision
- Collision Severity

Collision Proximity Levels

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

details, see Configuring Collision Proximity Levels.

Causes of Collision

For information on the causes of change request collisions, see Configuring Collisions Severity Levels.

Collision Severity

For information on how Release Control determines the severity of a collision, see Calculating Change Request Collisions.

You change the severity level definitions in the **change-flow.settings** configuration file (**<Release Control installation directory>\conf**). For more information, see Collisions Pane.

For information about viewing collision details, see Assess > Collisions Tab.

Similar Changes

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 feature is based on an adaptive algorithm developed by software Labs. A user with the Similarity Teacher role can tune this algorithm by adding, deleting, or confirming similar changes.

In other words, by tuning the similarity algorithm, the Similarity Teacher actually modifies the way Release Control calculates similarity between change requests, thereby yielding more meaningful results in the future.

For more information about similar changes, see Assess > Similar Changes Tab.

Detected and Latent Changes

By default, Release Control contains all the changes that are *scheduled* to take place in your environment. However, you can configure the Universal CMDB to periodically search for *actual* changes to your environment and send data about these changes to Release Control. For details, see Configuring Latent and Detected Changes.

> **Note:** This feature may not be available in your Release Control application. For more information,

> contact your Release Control administrator.

This section also includes:

- Understanding Scheduled and Discovered Changes
- Viewing Detected Changes
- Viewing Latent Changes

Understanding Scheduled and Discovered Changes

You can use Release Control to view data for two types of changes:

- **Discovered changes.** Actual completed changes discovered in your environment by the Universal CMDB.
- **Scheduled changes.** All changes scheduled to take place in your environment that are contained in Release Control.

Release Control matches all **discovered changes** with **scheduled changes** according to certain criteria. Depending on how the changes match up, each discovered change is then classified as either a **detected change** or as a **latent change**.

Viewing Detected Changes

When a discovered change matches a scheduled change according to all of the matching criteria, Release Control defines the change as a **detected change**. For details on how to view detected changes, see Review > Verifications Tab.

Viewing Latent Changes

When a detected change does not match any scheduled change, or matches only according to some of the matching criteria, Release Control defines the change as a **latent change**.

Latent changes are displayed as separate changes in the Change Requests List View, along with all the other change requests. A latent change is indicated by the **Latent** icon and the words **Latent change** in the List view's **Summary** column. For details on how to view detected changes, see Review > Verifications Tab.

You can work with the latent change feature in different ways. This section assumes that the latent change feature is fully activated. For more information about the different latent change modes, see Latent Changes Pane.

Tasks

Resolve Open Issues Before the Change Advisory Board (CAB) Meeting

This task describes how to identify change request collisions associated with changes scheduled to be discussed during the next CAB meeting. Then, it describes how to resolve the problems prior to the meeting, so that the CAB discussion can focus only on issues which cannot be resolved offline.

Step 1: View the Change Requests to be discussed at the CAB meeting

As the Change Manager for your company, you select **Module** > **Analysis** > **Change Requests** and then click **Select Filter**. Select the **Next CAB Meeting** filter to view the change requests that are scheduled to be discussed at the next CAB meeting.

For more information about filtering change requests, see Change Request Filter Dialog Box.

Step 2: Sort the Change Requests by Collision Severity

In the Change Requests pane, you click the header of the **Collision Severity** column to sort the change requests by severity. The colliding change requests appear at the top of the list and the changes having the highest severity appear first.

For more information about change request collision, see Change Request Collisions.

Step 3: Create an Action Item

You create an action item for each colliding change to request that the collisions be resolved before the next CAB meeting.

In the Change Requests pane, you select the change request for which you want to create a new action item, and then click the **Collaborate** > **Action Items**tab. You then click the **New Action Item** button to open the Add Action Item dialog box and assign the action item to the relevant person.

For more information on how to create an action item, see Add/Edit Action Item Dialog Box.

Use the Change Planner to Reschedule a Change

Step 1: Select a New Schedule in the Change Planner

Select **Module** > **Analysis** > **Change Requests** and click the **Plan Selected Change** button to open the Change Planner. In the Scheduling pane, use the calendars in the **Planned start** and **Planned end** boxes to set a new schedule. For details, see Scheduling Pane.

Step 2: Run a simulation in the Change Planner

In the Change Planner, click the **Run Simulation** button to run the simulation.

Step 3: View the summary information

In the Change Planner, click the **Preview** tab to display the:

- Current planned times of the change compared with the simulated time.
- Summary of the current analysis results compared with the simulated analysis results. For more information on the Preview tab, see Preview Tab.

Step 4: View the Impact Analysis of the simulation

In the Change Planner, click the **Impact** tab to display the impact analysis of the simulation. For more information about viewing impact analysis results and the filter options, see Impact Tab.

Step 5: View the Collision Analysis of the simulation

In the Change Planner, click the **Collisions** tab to display the collision analysis of the simulation. For more information about viewing collision analysis results and the filter options, see Collisions Tab.

Step 6: View the Time Periods Conflicts Analysis of the simulation

In the Change Planner, click the **Time Periods Conflicts** tab to display the time period conflicts analysis of the simulation. For more information about viewing time period conflicts analysis results and the filter options, see Time Period Conflicts Tab.

Step 7: View the risk analysis of the simulation

In the Change Planner, click the **Risk** tab to display the risk analysis of the simulation. For more information about viewing time risk results, see Risk Tab.

Step 8: Save the updated schedule

Save the updated schedule to your service desk. For details, see Change Planner Dialog Box.

Change the Impact Analysis Calculation Results - Delete a CI

This task describes how to change the impact analysis calculation results for a change request by deleting the relevant business CI model in the Modeling Studio in Universal CMDB, directly from Release Control.

This task includes the following steps:

Step 1: Review Impact Analysis calculation results

Step 2: Remove the TestBusiness CI from the Impact CIs pane

Step 3: View the simulation results

Step 1: Review Impact Analysis calculation results

Assume that you are a member of the Change Advisory Board and are responsible for reviewing the impact analysis calculation results for the deployment of a new webmail server.)

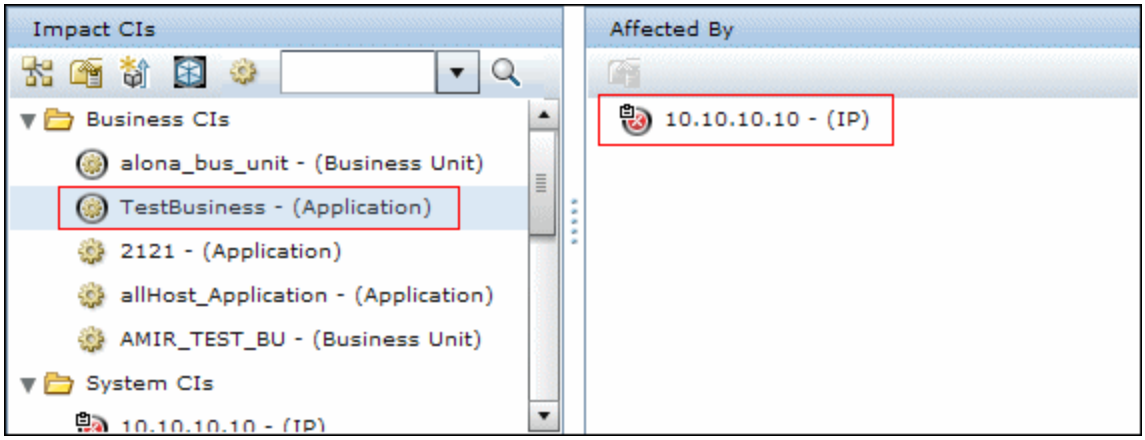
In the Change Requests pane, you select the required change request. Then you click the **Plan Selected Change** button to open the Change Planner. You click the **Impact** tab to review the impact analysis calculation results for the change request. For more information about viewing impact analysis results, see Assess > Impact Tab.

You see the **TestBusiness** CI that appears in the Impact CIs pane and recall that the **TestBusiness** CI no longer exists in the model. The **TestBusiness** CI still appears in the Impact CIs pane and is therefore included in the impact results since Universal CMDB was not updated with this change.

The impact analysis results are therefore inaccurate.

Example of a redundant CI in the impact CIs pane:

To render the impact analysis results accurate, you need to remove the **TestBusiness** CI from the Impact CIs pane so that the impact analysis results are calculated without it.

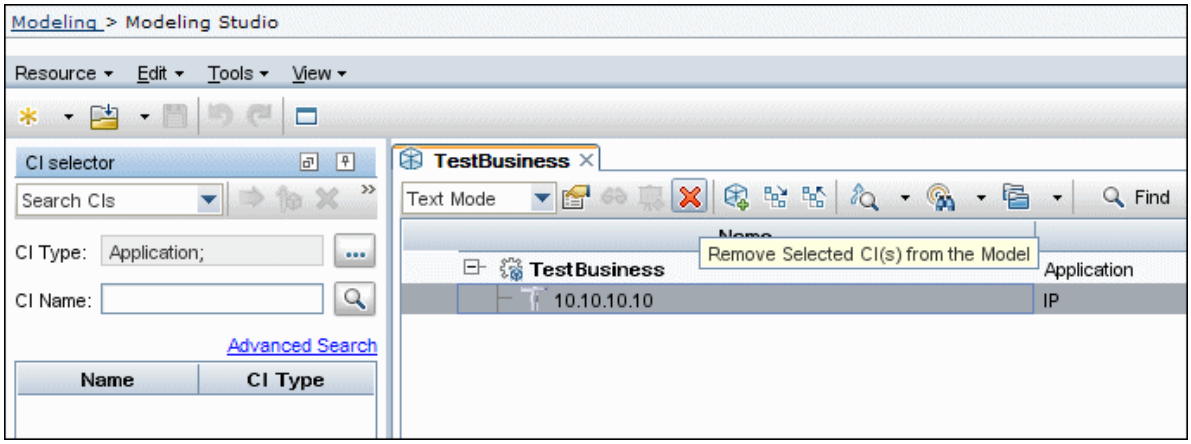


Step 2: Remove the TestBusiness CI from the Impact CIs pane

You select the **TestBusiness** CI in the Impact CIs pane and then click **Update Model** to open the Modeling Studio in Universal CMDB. The business CIs of the selected model appear in the Editor pane. You want to delete the CI that affects the **TestBusiness** CI, which in this case is the **10.10.10.10** CI, so that the **TestBusiness** CI no longer appears in the Impact CIs pane as an impact CI. For details on the **Update Model** button, see Update Model.

Example of how to delete a CI from the model:

In Modeling Studio, you select the **10.10.10.10** CI and click the **Remove Selected CIs from the Model** button. Then, to save the changes you made, you click the **Save** button in the Modeling Studio toolbar.

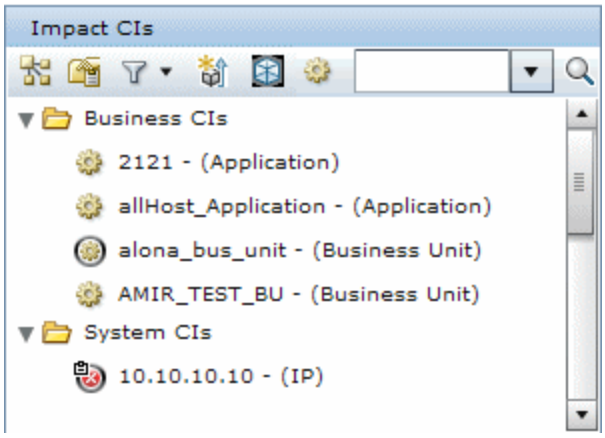


Step 3: View the simulation results

In the Change Planner, you click the **Run Simulation** button to run the Change Planner simulation. For details on the Change Planner, see Change Planner Dialog Box.

Example showing the TestBusiness CI removed from the Impact CIs pane:

The **TestBusiness** CI has been removed from the Impact CIs pane and is no longer calculated as part of the impact analysis results.



Change the Impact Analysis Calculation Results - Add a CI

This task describes how to change the impact analysis calculation results for a change request by adding the required business CI model from the Modeling Studio in Universal CMDB, directly from Release Control.

This task includes the following steps:

Step 1: Review Impact Analysis calculation results

Step 2: Add the Criticality_App CI to the Affects pane

Step 3: View the Simulation Results

Step 1: Review Impact Analysis calculation results

As a member of the Change Advisory Board, you are responsible for reviewing the impact analysis calculation results for the deployment of a new webmail server.

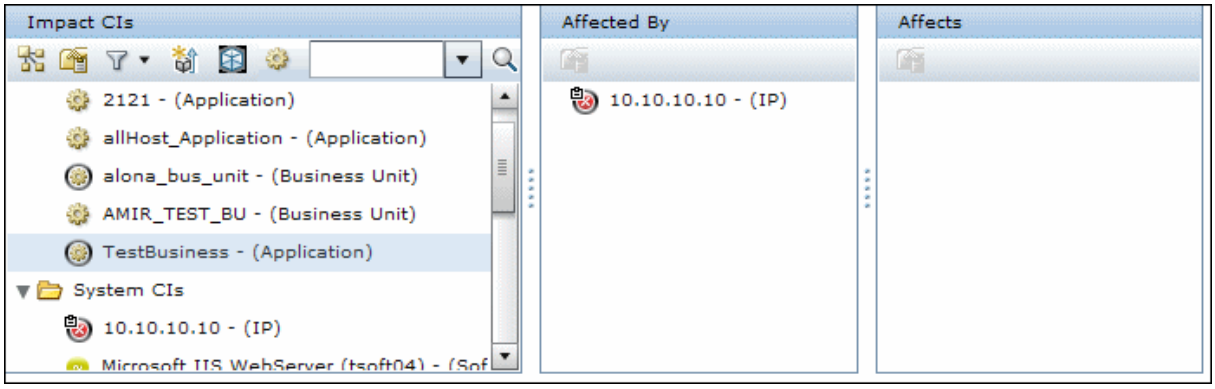
In the Change Requests pane, you select the required change request. Then you click the **Plan Selected Change** button to open the Change Planner. You click the **Impact** tab to review the impact analysis calculation results for the change request. For details on the Impact tab, see Assess > Impact Tab.

You notice that the **TestBusiness** CI that appears in the Impact CIs tab should impact another CI - **Criticality_App**, but the **Criticality_App** CI does not appear in the Affects pane. The **Criticality_App** CI is not included in the impact results since Universal CMDB was not updated with this change.

The impact analysis results are therefore inaccurate.

Example of a missing CI in the Impact CIs tab:

To render the impact analysis results accurate, you need to add the **Criticality_App** CI to the Affects pane so that the **Criticality_App** CI is included in the calculation.



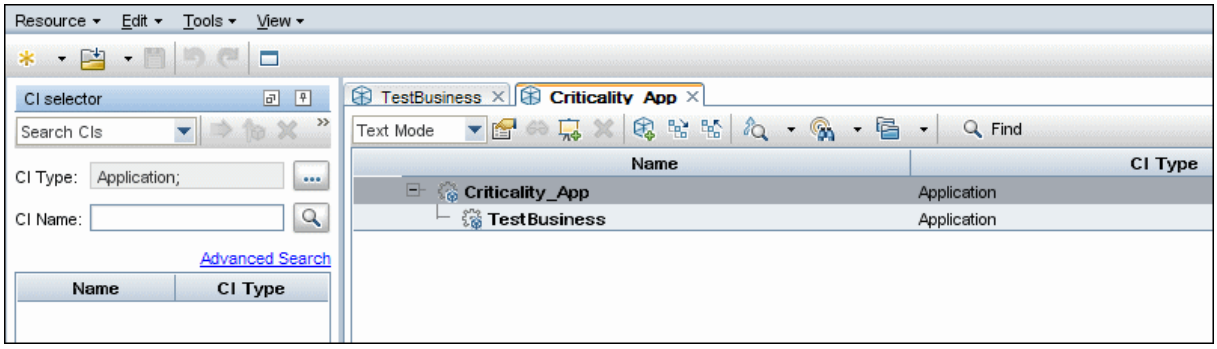
Step 2: Add the Criticality_App CI to the Affects pane

You select the **TestBusiness** CI in the Impact CIs pane and then click the **Add CI to Model** button to open Modeling Studio in Universal CMDB. The **TestBusiness** CI appears in the CI Selector. You want to add the **Criticality_App** CI to the model. For details on the **Add CI to Model** button, see Add CI to Model.

> **Note:** If you are using Universal CMDB 9.0, the CI Selector works only if the Release Control and Universal CMDB servers are under the same domain.

Example of how to add a CI to the model:

In Modeling Studio, you click the drop-down arrow next to the **Open** button and select **Open Model**. The Open Model dialog box opens. You select the **Criticality_App** CI and click **OK**. The **Criticality_App** CI appears above the **TestBusiness** CI to show that the **TestBusiness** CI impacts the **Criticality_App** CI. Then, to save the changes you made, you click the **Save** button in the Modeling Studio toolbar.

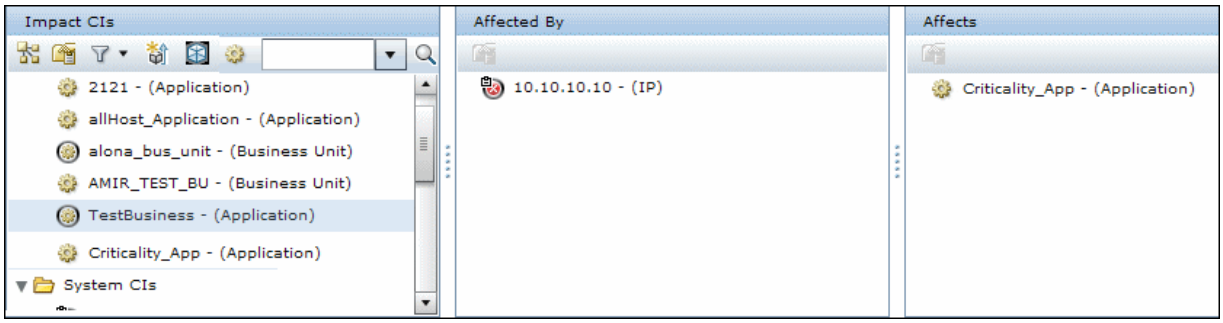


Step 3: View the Simulation Results

In the Change Planner, you click the **Run Simulation** button to run the Change Planner simulation. For details on the Change Planner, see Change Planner Dialog Box.

Example showing the Criticality_App CI added to the Affects pane:

The **Criticality_App** CI has been added to the Affects pane to show that **TestBusiness** impacts the **Criticality_App** CI.



Reference

Analysis Module User Interface

This chapter describes:

- Action Items Pane
- Add Change Request to Similarity Set Dialog Box
- Add/Edit Action Item Dialog Box
- Approve/Retract/Deny Change Request Dialog Box

- Assess > Impact Tab
- Assess > Collisions Tab
- Assess > Risk Tab
- Assess > Similar Changes Tab
- Assess > Time Period Conflicts Tab
- Change Planner Dialog Box
- Change Requests — Calendar View
- Change Requests — List View
- Change Requests Toolbar Options
- Collaborate > Action Items Tab
- Collaborate > Discussion Tab
- Collaborate > Resolution Tab
- Impact Graph Window
- Launch Manual Change Process Dialog Box
- New Discussion Thread Dialog Box
- Post Implementation Review Dialog Box
- Preview > Details Tab
- Preview > Overview Tab
- Preview > Related Records Tab
- Report Details Dialog Box
- Respond Dialog Box
- Review > Conclusions Tab
- Review > Event Log Tab
- Review > Verifications Tab

Action Items Pane

This pane displays action items that have been created from change requests as well as the basic information and user comments for each action item selected from the list.

To access	Select **Module > Analysis > Action Items**.

See also	Action Items

Action Items List Pane

This pane displays a list of the action items.

Important Information	• By default, the Action Items mode displays all the action items that were created from all the change requests in the system. • You can sort the order of appearance of the requests according to each column by clicking the required column heading.

User interface elements are described below:

UI Elements (A-Z)	Description
Respond	Opens the Respond dialog box, which enables the following: • Any user to post comments. • The assignee to mark an open action item as **Done** or return the item to its creator. • The creator to reopen an action item marked as **Done**. For more information, see Respond Dialog Box. **Note:** Enabled only when the action item selected is assigned to the current user.
	Close Action Item. Enables the creator to change the status of the action item to **Closed**. **Note:** Enabled only when the action item selected is assigned to the current user.
	Edit Action Item. Enables the creator to edit an open action item. Opens the Add/Edit Action Item dialog box. **Note:** Enabled only when the action item selected is assigned to the current user.
	New Action Item. Enables you to create a new action item associated with the same change request as the selected action item. Opens the Add/Edit Action Item dialog box,
	Delete Action Item. Enables the creator to delete an action item. **Note:** • Enabled only when the logged in user is the creator of the action item.

UI Elements (A-Z)	Description
	> • Once you have added an action item, it can be deleted only if it has not been updated. For example, if the assignee of the action item has responded, or a comment has been posted to it. The processing of an action item should end with a **Closed** status, meaning that all the specified tasks for the action item have been completed.
	Forward by E-Mail (FYI). Enables you to send an action item by email for information purposes. Opens the Send E-mail dialog box.
	Add Selected Action Item to Favorites/ Delete Selected Action Item from Favorites. Toggles between adding or removing the selected action item from the Favorites filter. For information about Filters, see Filtering Change Requests and Activities. Click the drop-down arrow and select one of the following options: • **Delete from Favorites.** Deletes the selected action items from the Favorites filter. • **Delete all AI's in the Favorites Filter.** Deletes all the action items in the Favorites filter. > **Note:** You can also subscribe to receive notifications when certain modifications are made to favorite action items. For details, see User Workspace Pane.
	Subscribe to Selected Action Item/Unsubscribe from Selected Action Item. Enables you to receive email notifications or cancel a notification subscription for the selected action item. For information on configuring notification rules and conditions, see Notifications Pane.
	Go to Parent Action Item. Displays the parent action item for the selected derived action item.
<View other pages>	Enables you to view other pages by using the left and right arrows. The number between the left and right arrows indicate which page is currently being displayed. For example, 3 of 5 means that the 3rd page out of 5 is being displayed.
Assigned to	Displays the name of the user to whom the action item was assigned. This user can respond to the request in one of the following ways: • Complete the task involved and mark the action item as **Done** once it has been completed. • Reject the request and return it to the creator. If necessary, the assignee can also create a new, derived action item from the current action item.

UI Elements (A-Z)	Description
Creator	Displays the name of the user who created the action item. The creator is also the user responsible for marking the action item as **Closed**.
Due date	The day by which the creator determined that the action item must be completed. If this date has passed and the item has not been closed, the due date is displayed in red. A tooltip indicating the due date (including the day and hour) of the action item is visible when you hold the mouse pointer over the action item icon. If the due date has passed and the item has not been closed, **[Expired]** is also included in the tooltip.
ID	Displays the Release Control-generated ID number of the action item.
Modified	Displays the date (including the day and hour) on which the action item was last modified. If the item has not been modified since its creation, this column displays the item's creation date and time.
Pending on	Displays the name of the user whose action is being awaited. If the item is open, the name of the assignee, who is supposed to mark the item as **Done**, is displayed in this column (unless the assignee returned the item to the creator). If the item is marked as **Done**, the name of the creator, who is supposed to mark the item as **Closed**, is displayed in this column.
Priority	Displays a colored flag indicating the priority level that the creator assigned to the action item. The color of the flag indicates the priority level as follows: • **Red** - High • **Yellow** - Normal • **Green** - Low A tooltip indicating the priority of the action item is visible when you hold the mouse pointer over the action item icon.
Status	Displays an icon indicating the status of the action item. The following icons indicate the following statuses: • Open • Done • Close A tooltip indicating the status of the action item is visible when you hold the mouse pointer over the action item icon.
Subject	Displays a brief overview of the action item. Parent action items can be

UI Elements (A-Z)	Description
	expanded to display all the derived action items. To expand or collapse action items, click the Expand button to the left of the item. Derived action items are displayed in light blue.

Action Item Posting Pane

This pane displays basic information and user comments for each action item selected from the Action Items List pane.

User interface elements are described below:

UI Elements (A-Z)	Description
Assignee	Displays the name of the user to whom the action item was assigned. If the action item is pending on the assignee, a bullet appears to the right of the assignee's name.
Comments	Displays the comments that were posted regarding the action item. Each comment contains a header that includes the name of the user who posted the comment and the date and time of the comment's posting. The subject of the comment is displayed in blue text and the description entered by the user is displayed in black text. **Note:** Comments can be posted by any Release Control user.
Creator	Displays the name of the user who created the action item. If the action item is pending on the creator, a bullet appears to the right of the creator's name.
Date due	The day by which the creator determined that the action item must be completed.
Status	Displays the status of the action item. The possible options are: • **Open** • **Done** • **Closed**
Subject	Displays the subject line of the action item (above the comments).

Add Change Request to Similarity Set Dialog Box

Release Control calculates similar changes according to specific criteria as defined in the similar settings directory. A user with a Similarity Teacher role can add requests to the Similar Changes list

even if they are not automatically regarded as being similar according to these criteria.

To access	Select **Module** > **Analysis** > **Change Requests** > **Assess** > **Similar** tab, and then click **Add Change Request to Similarity Set**.
See also	• User Configuration • Similar Changes

User interface elements are described below:

UI Elements (A-Z)	Description
Request ID	Enter the ID of the request you want to add to the list.
Service Desk	Select the required service desk.

Add/Edit Action Item Dialog Box

This dialog box enables you to create an action item for a specific change request or edit an existing action item.

To access	If you are in Action Items mode (select **Module** > **Analysis** > **Action Items**), select the action item for whose associated change request you want to create a new action item. If you are in Change Requests mode (select **Module** > **Analysis** > **Change Requests**), select the change request for which you want to create a new action item. • To create an action item, click **New Action Item** in the toolbar. • To edit an existing action item, click **Edit Action Item** in the toolbar.
Important Information	• The creator of an action item can only modify the assigned action item if it is still open. For details about the statuses of action items, see Status. • When modifying an action item, you cannot modify the level (parent/derived) of the action item. • The **Edit Action Item** button is only enabled when the action item selected is assigned to the current user and the status of the item is not **Closed**.
See also	Action Items

User interface elements are described below:

UI Elements (A-Z)	Description
Submit	The action item you create/edit is added to both the Action Items List pane and the Action Items view of the associated change request's Collaboration > Action Items tab. An email notification is sent to the assignee.
Add as	If you select an action item and are the action item's assignee, choose whether you want to create the action item as a new item or as a derived action item. A derived action item is listed under the parent item in the Action Items List pane.
Assignee	Select a user to whom you want to assign the selected action item. Click **Assignee** to the right of the **Assignee** box. The Select Users dialog box opens. Locate and select the user to whom you want to assign the action item. The user name of the user you selected appears in the **Assignee** box.
Creator	The creator of the action item.
Description	(Optional) A free text box containing a brief description of the action item.
Due Date	Select the date and time by which the action item should be completed. Click the calendar button to the right of the **Due Date** box to select the date and time. The date appears in the **Due Date** box. **Note:** You select the time according to your machine's time zone, as indicated in the calendar box.
Priority	Select the priority you want to assign the action item. The options are: • **Low** • **Medium** • **High**
Request ID	The ID of the change request.
Subject	A brief overview of the action item.

Approve/Retract/Deny Change Request Dialog Box

This dialog box enables you to approve, retract, or deny a change request.

To access	Select **Module** > **Analysis** > **Change Requests** > **Collaborate** > **Resolution** tab, and then click **Approve**, **Retract**, or **Deny** in the Resolution pane.

Important Information	• The **Approve/Retract/Deny** buttons are enabled only if the required criteria are met. For details, see Collaborate > Resolution tab. • If the authentication data you provided is incorrect, or if you are not currently allowed to approve the change request, Release Control issues a detailed error message. If the service desk application's version of the request is more current than the version in Release Control, you receive a message asking whether you want to force the approval of the change request. Select the check box and click **Approve** to force approval. • To view details of your approval, click the **Approval Log** button in the Resolution pane of the Collaborate > Resolution tab. • If you have retracted the approval of the change request, the retraction details appear in the Cab Decisions pane of the **Collaborate > Resolution** tab. • To update a change request's status in the Change Requests pane, click the **Refresh** button. The request' s status is updated once Release Control receives the updated request from the service desk application. This may take a few seconds.
See also	Collaborate > Resolution Tab

User interface elements are described below:

UI Elements (A-Z)	Description
Comment	Enter the information you want Release Control to display as part of your approval/retraction/denial. Enter the user name and password of your service desk application in the Login dialog box that opens. Release Control saves this information until you end your session so that you do not have to re-enter this information for each change request that you want to approve, retract, or deny. If you configured the selected change request to contain a URL link to the original request in the service desk application, you can view the request in the service desk application by clicking **Open the original request in the service desk application**. When you click **Approve**, **Retract**, or **Deny**, Release Control checks whether your user name and password are correct and whether you are currently allowed to approve/retract/deny the change request. If so, Release Control approves/retracts/denies the request and the details appear in the Collaborate tab. For more information on approving/denying a change request or retracting an approval, see Collaborate > Resolution Tab.

Assess > Impact Tab

This tab describes how to view the impact analysis calculation results for a change request. The Impact tab displays the business and system CIs that are affected by the change request. This includes general information about the affected business or system CIs and an indication of the severity of the impact of the change request.

In addition, Release Control enables you to change the impact analysis calculation results for the change request by modifying the business CI model which was created in the Modeling Studio in Universal CMDB.

> **Note:** You cannot view the Universal CMDB user interface with Firefox 3.0.9.

To access	Select **Module** > **Analysis** > **Change Requests** > **Assess** > **Impact** tab.
Relevant tasks	• Change the Impact Analysis Calculation Results - Delete a CI • Change the Impact Analysis Calculation Results - Add a CI
See also	• Impact Analysis • Modeling Studio Integration Overview

User interface elements are described below:

UI Elements (A-Z)	Description
	Open Graph Window. Enables you to view the impact analysis calculation results in graphic format. Opens the Impact Graph window.
	CI Attributes. Enables you to view the attributes of the selected CI. Opens the CI Attributes window. > **Note:** To customize the attributes that Release Control displays, see CIs Display Pane.
	Add CI to Model. A link that opens Universal CMDB. Searches for the selected CI and opens Universal CMDB. In Modeling Studio, the selected CI is in the CI Selector and the Editor pane is empty. You can create a new model or add the CI to the existing model. > **Notes:**

UI Elements (A-Z)	Description
	> - If you are using Universal CMDB 9.0, the CI Selector works only if the Release Control and Universal CMDB servers are under the same domain. > - If Lightweight Single Sign-On Authentication Support (LW-SSO) is enabled, you can set the Modeling Studio to open automatically. If LW-SSO is not enabled, Universal CMDB's login page opens. You can access this button in the following places: - **In the Change Planner:** Select **Module** > **Analysis** > **Change Request**. In the Change Requests pane, click **Plan Selected Change** to open the Change Planner window and then click the **Impact** tab. - **In the Analysis module:** Select **Module** > **Analysis** > **Change Request** > **Assess** > **Impact**tab. - In the Impact Graph window: Select **Module** > **Analysis** > **Change Request** > **Assess** > **Impact**tab. In the Impact pane, click **Open Graph Window** to open the Impact Graph window. > **Note:** > - You cannot view the Universal CMDB user interface with Firefox 3.0.9. > - This button only appears if the Universal CMDB version to which you are connected is version 8.01 or later. > - This button is disabled if: > ◦ No CI is selected > ◦ The CI that is selected is not a valid one
	Update Model. A link that opens Universal CMDB. In Modeling Studio, the business CIs of the selected model appear in the Editor pane. You can search for a CI in the CI Selector and add or remove CIs from the model. > **Notes:** > - If you are using Universal CMDB 9.0, the CI Selector works only if the Release Control and Universal CMDB servers are under the same domain. > - If Lightweight Single Sign-On Authentication Support (LW-SSO) is enabled, you can set the Modeling Studio to open

UI Elements (A-Z)	Description

	automatically. If LW-SSO is not enabled, Universal CMDB's login page opens.
	
	You can access this button in the following places:
	• **In the Change Planner:** Select **Module** > **Analysis** > **Change Request**. In the Change Requests pane, click **Plan Selected Change** to open the Change Planner window and then click the **Impact** tab.
	• **In the Analysis module:** Select **Module** > **Analysis** > **Change Request** > **Assess** > **Impact** tab.
	• **In the Impact Graph window:** Select **Module** > **Analysis** > **Change Request** > **Assess** > **Impact** tab. In the Impact pane, click **Open Graph Window** to open the Impact Graph window.
	
	Notes:
	• You cannot view the Universal CMDB user interface with Firefox 3.0.9.
	• This button only appears if the Universal CMDB version to which you are connected is version 8.01 or later.
	• This button is disabled if:
	  ○ No CI is selected
	  ○ The CI that is selected is not a valid one
	  ○ A system CI is selected

	My Business CIs Button. Click this button to narrow the impact CIs search scope to your subscribed CIs as defined in the **My Business CIs** list. Release this button and the search scope is global for all RFC CIs. For details on how to define the maximum number of impact CIs per change request, see Maximum impact search result size.
	CIs Search Box. Enables you to search for CIs by entering a CI name pattern in the CIs search box. This text box also supports wildcard search. For example, if a CI's name is "abc", you can type "`a*`" or "`a?c`" to search for it. The search returns all related CIs with their names match the search pattern. The CIs' direct parents and children are included in the result, too. If you leave it empty, it will default to "`*`".

UI Elements (A-Z)	Description
	Find. Click the **Find** button to run the search for a specific impact CI.
	Expand/Collapse. Enables you to expand/collapse a CI to display/hide all the child CIs.
<Impact Severity Levels of Business CIs>	The icons to the left of each business CI name indicate whether the business CI is directly or indirectly affected by the change request: • . The business CI is directly affected by the change request (DAB). This means that this business CI is included in the uCMDB impact analysis result of RC_DIRECTLY_AFFECTED correlation rule group. • . The business CI is indirectly affected by the change request (IAB). This means that this business CI is included in the uCMDB impact analysis result of RC_IMPACT correlation rule group (and not in the result of RC_DIRECTLY_AFFECTED correlation rule group). If a CI is triggered directly from the ticket (Triggered CI), a black circle surrounds the impact severity level icon . From each affected business CI, you can filter the change requests so that only those that affect the current business CI are displayed. You do this by right-clicking the affected business CI and choosing **Quick filter: show affecting requests** from the menu. The change requests that affect this business CI are displayed in the Change Requests pane.
<Impact Severity Levels of System CIs>	The impact severity level of a CI that is explicitly mentioned in the ticket (Triggered CI) is automatically set to critical. The severity of any CIs which are not triggered CIs are calculated by Universal CMDB. Following are the default impact severity level icons: Critical High Medium Low Very low No impact analysis available • If a CI is directly affected by the change CI (CCI), a black circle surrounds the impact severity level icon .

UI Elements (A-Z)	Description
	• If a CI is triggered directly from the ticket (Triggered CI), a ticket symbol is added to the impact severity level icon . A tooltip indicating the impact severity level of the business or system CI is visible when you hold your mouse over the severity level icon. **CCI** indicates that the CI changes as a result of the change request. **ACI** indicates that the CI is affected by the modification of the change request. **Note:** If you are working with Release Control without Universal CMDB, ACIs cannot be detected.
Affected by pane	Displays the CIs which have an affect on the selected CI.
Affects pane	Displays the CIs which are affected by the selected CI.
Impact CIs pane	Displays the affected and changed CIs (ACIs and CCIs).

Assess > Collisions Tab

This tab displays details about all the change requests that collide with the change request selected in the Change Requests pane.

You can view collisions in the List or Timeline views. The causes of collisions are also displayed.

To access	Select **Module** > **Analysis** > **Change Requests** > **Assess** > **Collisions**tab.
Important Information	The maximum number of collisions for which Release Control calculates collision results is configured in the **Collision count fuse** box in the Collisions Pane. If the number of collisions for the selected change exceeds the specified value in the **Collision count fuse** box, the collisions are not listed and the following message appears instead: Number of collisions exceeded the configured threshold. This may indicate a collision configuration problem. Please contact your administrator.
Relevant tasks	Resolve Open Issues Before the Change Advisory Board (CAB) Meeting
See also	Change Request Collisions

Colliding Changes Pane

This pane enables you to view collisions in the List view or Calendar view.

User interface elements are described below:

UI Elements (A-Z)	Description
	List. Displays the change requests that collide with the change request selected in the Change Requests pane in table format. For details, see List View.
	Timeline. Displays colliding change requests as solid bars on a timeline. For details, see Timeline View.
Go	**Go to Colliding Request.** Enables you to view the change request with which the colliding change request displayed in the Colliding Changes pane collides in the Change Request pane.
	Zoom in/Zoom out. Enables you to divide the timeline into 1-hour or 6-hour time intervals. Click the arrow next to the **Zoom in/Zoom out** button to select the required interval. **Note:** Available in Timeline view only.

Collision Causes Pane

This pane displays the details of the factors causing the collision of the selected change request in the List or Timeline view.

Important Information	If you are working with Release Control without Universal CMDB, ACIs cannot be detected. The only CI-related cause of collision, then, is **CCI-CCI**.

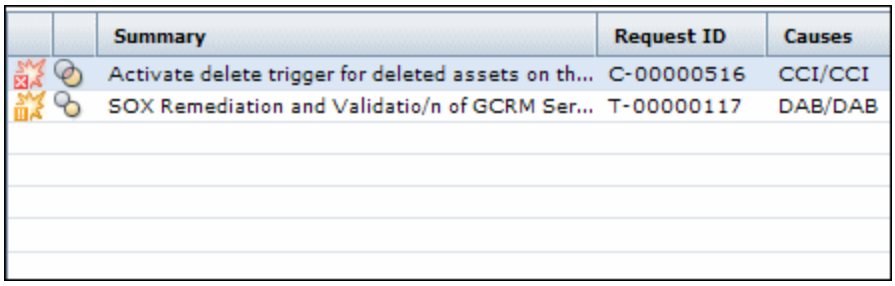
User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Elements (A-Z)	Description
	Expand All/Collapse All. Enables you to expand or collapse the collision causes.
	CI Attributes. Enables you to view the attributes of the selected CI. Opens the CI Attributes window. **Note:** To customize the attributes that Release Control displays, see CIs Display Pane.
<Collision Cause: Business CI>	If a commonly affected business CI causes the collision, it is listed in the Collision Causes pane, under **Business CI**. The icon to the left of the business CI indicates whether it is directly

UI Elements (A-Z)	Description
	or indirectly affected by the collision. • If at least one of the CIs associated with the business CI is a CCI, then the business CI is directly affected by the collision. • If all of the CIs associated with the business CI are ACIs, then the business CI is indirectly affected by the collision. **Note:** You can filter the change requests so that only those that affect a particular business CI are displayed. To do this, right-click the business CI in the Collision Causes pane and select **Quick filter: show affecting requests**. Only the change requests that affect this business CI are displayed in the Change Requests pane.
<Collision Cause: Implementor>	If one of the collision causes is a common implementor, the name of the implementor responsible for implementing the change requests is displayed in the Collision Causes pane, under **Implementors**.
<Collision Cause: System>	If one of the collision causes is commonly affected system CIs, you can view a list of these CIs in the Collision Causes pane, under **System** The colliding CIs are listed alongside icons that indicate the impact severity of the CIs. For more information about impact severity, see Assess > Impact Tab.

List View

This view displays the change requests that collide with the change request selected in the Change Requests pane in table format. The table is sorted in order of the severity of the collisions.



Hold the cursor over an element in the table to view a tooltip with relevant information.

To access	Select **Module** > **Analysis** > **Change Requests** > **Assess** > **Collisions** tab and then click **List** in the Colliding Changes pane.

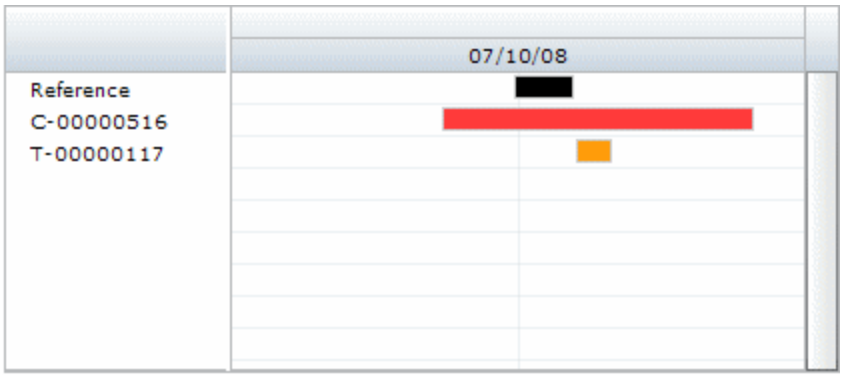
User interface elements are described below:

UI Elements (A-Z)	Description
<Collision severity>	Displays an icon indicating the severity of the collision. If there are multiple causes for a collision, the collision severity is determined by the most severe of the causes. Collision severity is indicated as follows: • Critical • High • Medium • Low • Very Low For details about how collision severity is calculated, see Change Request Collisions.
<Proximity level>	Displays an icon indicating the collision proximity level. Collision proximity is indicated as follows: • Overlap • Overlap warning For more information about collision proximity levels, see Change Request Collisions.
Causes	Displays the causes of the collision. Change request collisions can be caused by several factors (CI-, business CI-, implementor-, or field-related). If multiple factors cause a collision, all of the factors are listed. The following is a list of all the possible collision causes: • **CCI-CCI.** A common CI is changed by both change requests. • **CCI-ACI.** A common CI is changed by one of the change requests and indirectly affected by the other change request. • **ACI-ACI.** A common CI is indirectly affected by both change requests. • **DAB-DAB.** A common business CI is directly affected by both change requests. • **IAB-DAB.** A common business CI is directly affected by one of the change requests and indirectly affected by the other change request. • **IAB-IAB.** A common business CI is indirectly affected by both

UI Elements (A-Z)	Description
	change requests. • **Implementor.** A common implementor is responsible for implementing both change requests. • **Field.** A specified field has the same value in both change requests. For more information about collision causes, see Change Request Collisions.
End	Displays the date on which the implementation of the conflicting change request is scheduled to end.
Request ID	Displays the service desk application request ID of the conflicting change request.
Start	Displays the date on which the implementation of the conflicting change request is scheduled to begin.
Summary	Displays a brief overview of the conflicting change request.

Timeline View

This view displays colliding change requests as solid bars on a timeline. Each block represents a different colliding change request.



The change request selected in the Change Requests pane is always displayed first on the timeline, and is labeled **Reference**. The colliding change requests are labeled by their request IDs.

The color of the bar indicates the severity of the collision. If there is more than one cause for a collision, the collision severity is determined by the most severe cause.

To access	Select **Module** > **Analysis** > **Change Requests** > **Assess** > **Collisions** tab. Then click **List** in the Colliding Changes pane.

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Elements (A-Z)	Description
<Collision severity>	By default, the collision severity is indicated as follows: • **Red** – Critical • **Orange** – High • **Yellow** – Medium • **Khaki** – Low • **Olive Green** – Very low • **Gray** – No collision analysis available

Assess > Risk Tab

This tab enables you to view the risk analysis for a change request. The Risk tab displays an overall summary of the risk analysis for the selected change request, including distribution charts of the risk factors contributing to the Potential Damage and Probability of Failure calculations. These distribution charts enable you to pinpoint the most significant factors contributing towards the risk level of the selected change request.

The risk calculation is displayed in the Risk Information pane. If an override rule is in place, details of the override rule are displayed alongside the distribution charts.

To access	Select **Module** > **Analysis** > **Change Requests** > **Assess** > **Risk** tab.
See also	Risk Analysis

User interface elements are described below:

UI Elements (A-Z)	Description
	Drill Down. Displays the risk calculation details in the Potential Damage and Probability of Failure panes.
	Returns to the upper level view.
Potential Damage	Displays a graphic illustration that 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. **Note:** This graph also appears in the lower level view, after

UI Elements (A-Z)	Description
	clicking **Drill down**.
Potential Damage Factor Details	Displays the details about each risk factor in table format. The table includes the following columns: • **Data.** The source data for the risk factor—for example, data from a field in the integrated service desk application. • **Description.** A description of the risk factor defined during the Release Control configuration process. • **Name.** The name of the risk factor defined during the Release Control configuration process. • **Score.** 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 Release Control configuration process. • **Weight.** The weight assigned to the risk factor during the Release Control configuration process. • **Weighted Value.** The weighted value of the risk factor within the final Potential Damage or Probability of Failure score. The weighted value is calculated as follows: **Weighted Value** = **Weight**/**Total Weight** x **Score** where **Weight** is the weight assigned to the risk factor and **Total Weight** is the sum of all the weights assigned to the risk factors.
Probability of Failure	Displays a graphic illustration that 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. **Note:** This graph also appears in the lower level view, after clicking **Drill down**.
Probability of Failure Factor Details	Displays the details about each risk factor in table format. The table includes the following columns: • **Data.** The source data for the risk factor—for example, data from a field in the integrated service desk application. • **Description.** A description of the risk factor defined during the Release Control configuration process. • **Name.** The name of the risk factor defined during the Release Control configuration process. • **Score.** The score of the risk factor as translated from the source

UI Elements (A-Z)	Description
	data. The mapping used to translate source data into a score is defined during the Release Control configuration process. • **Weight.** The weight assigned to the risk factor during the Release Control configuration process. • **Weighted Value.** The weighted value of the risk factor within the final Potential Damage or Probability of Failure score. The weighted value is calculated as follows: **Weighted Value** = **Weight**/**Total Weight** x **Score** where **Weight** is the weight assigned to the risk factor and **Total Weight** is the sum of all the weights assigned to the risk factors. **To access:** Click **Drill down** in the Probability of Failure pane.
Risk Information	Displays the risk calculation.

Assess > Similar Changes Tab

This tab displays a list of changes that are similar to the change request selected in the Change Requests or Action Items pane.

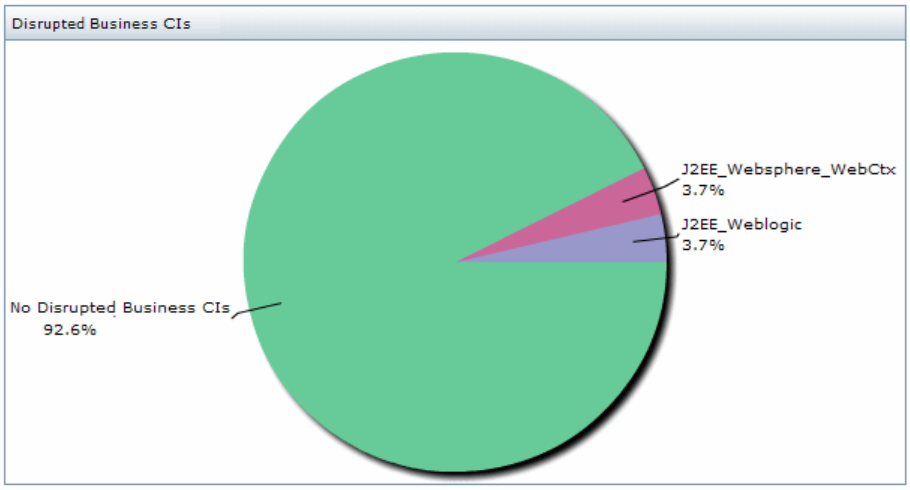
For more information about similar changes, see Similar Changes.

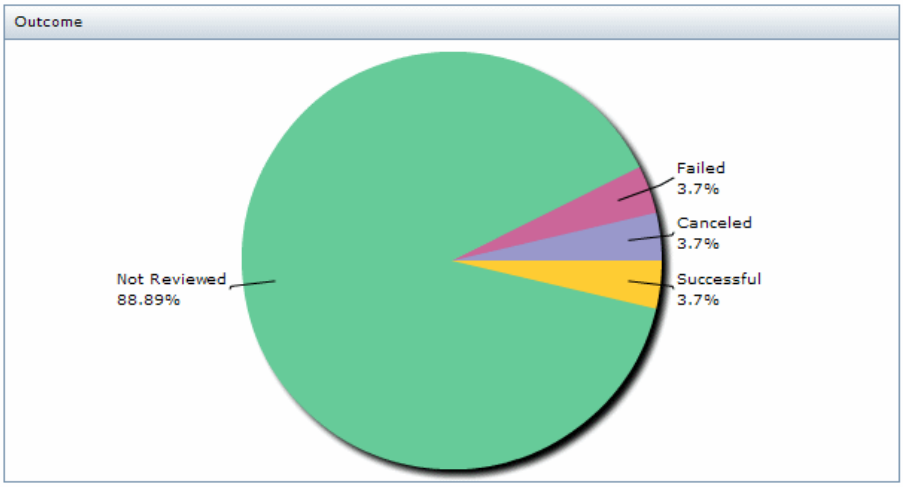
To access	Select **Module** > **Analysis** > **Change Requests or Action Items** > **Assess** > **Similar Changes** tab.

User interface elements are described below:

UI Elements (A-Z)	Description
	Similar Changes. Displays a list of requests which are similar to the selected request in the Change Requests or Action Items pane.
	Statistics. Displays the Outcome and Disrupted Business CIs graphs. The information displayed in the graphs is aggregated over all the requests displayed in the Similar Changes list.
	Add Change Request to Similarity Set. Release Control calculates similar changes according to specific criteria as defined in the similar settings directory. If you have been assigned the Similarity Teacher role, you can add requests to the Similar Changes list even if they are not automatically regarded as being similar according to these criteria. Opens the Add Change to Similarity Set dialog box.

UI Elements (A-Z)	Description
	Notes: • After the request is added to the Similar Changes list, a check mark appears in the **Confirmed** column. • Adding a request to the Similar Changes list influences the way Release Control calculates future similar changes.
	Confirm Change Request Similarity. Enables a user with a Similarity Teacher role to confirm that a request is similar. This guarantees that the request always appears in the Similar Changes list, irrespective of any other changes that are made to the list. **Notes:** • A check mark appears in the **Confirmed** column next to the request that is confirmed as similar. • Confirming a request as similar influences the way Release Control calculates future similar changes.
	Delete Change Request from Similarity Set. Release Control calculates similar changes according to specific criteria as defined in the similar settings directory. If you have been assigned the Similarity Teacher role, you can delete requests from the Similar Changes list even if they are regarded as being similar according to these definitions. **Note:** Deleting a request from the Similar Changes list influences the way Release Control calculates future similar changes.
	Open Similar Details Window. Enables you to view PIR details for any similar change with a **Closed** status, where a PIR was created. The Similar Details window opens and displays the Disrupted Business CIs and Review Notes information entered during the creation of the PIR. For details on creating a PIR, see Review > Conclusions Tab.
Go	**Go to Similar Request.** Enables you to view the list of similar changes for any request that appears in the Similar Changes list. The selected request is displayed in the Change Requests list view, and the Similar Changes list is updated to display the list of similar changes for the newly selected request.
Confirmed	Indicates requests which have been added to the list or have been confirmed as being similar. For more information about similar changes, see Similar Changes. **To access:** Click the **Similar Changes** button.

UI Elements (A-Z)	Description
Disrupted Business CIs pane	Specifies which other business CIs were affected by the similar changes.  **To access:** Click the **Statistics** button.
Ended	Displays the end date for the request. **To access:** Click the **Similar Changes** button.
Impact Severity	Indicates the impact severity level of the request. **To access:** Click the **Similar Changes** button.
Outcome	Displays the outcome for the request. Requests with any status other than **Closed** are automatically assigned the outcome **Not reviewed**. **To access:** Click the **Similar Changes** button.
Outcome pane	Displays aggregate outcome statistics for all the requests in the Similar Changes list.

UI Elements (A-Z)	Description
	 **To access:** Click the **Statistics** button.
Request ID	Displays the reference ID number for the request in the service desk application. **To access:** Click the **Similar Changes** button.
Review Date	Displays the date a Post Implementation Review (PIR) was created for the request. For more information on PIRs, see Review > Conclusions Tab. **To access:** Click the **Similar Changes** button.
Risk	Displays the risk level (low, medium, or high). **To access:** Click the **Similar Changes** button.
Started	Displays the start date for the request. **To access:** Click the **Similar Changes** button.
Summary	Displays a brief overview of the request. **To access:** Click the **Similar Changes** button.

Assess > Time Period Conflicts Tab

This tab displays the time period conflicts in which the selected change request is scheduled to take place either outside of a **Change Window** (periods in which change requests are allowed to take place) or within a **Blackout** period (periods in which change requests are not allowed to take place).

For more information on how time period conflicts are calculated, see Time Periods Tab.

You can choose to display the time period occurrences in the background of the view, according to the category colors and time period patterns that were configured by the Release Control administrator.

To access	• Select **Module** > **Analysis** > **Change Requests** > **Assess** > **Time Period Conflicts** tab. or • Select **Module** > **Analysis** > **Change Requests** > **Preview** > **Overview**tab. In the Analysis Info pane, the displayed category for the **Time Period Conflicts** field serves as a link to the Time period Conflicts tab. or • In the Change Planner dialog box, click the **Time Period Conflicts** tab.
Important Information	If the selected change request has no planned start or end time, the buttons on the toolbar become unavailable and the grid inside the timeline disappears.
Relevant tasks	Define Time Periods
See also	Time Periods

Conflicts Pane

This pane displays the configured Change Window and/or Blackout periods that are the causes of the time period conflict.

User interface elements are described below:

UI Elements (A-Z)	Description
	**Plan Selected Change.** Opens the Change Planner dialog box where you can simulate the effects of modifying the details of a change request. You can use the Change Planner dialog box to modify the planned start and/or end of the change request to avoid creating a time conflict, and then simulate the effects of the modifications. **Note:** For Change categories such as Emergency, Normal and Standard, scheduling a Change does not happen in the first Registration and Categorization phase. The **Plan Selected Change** button is unavailable until the Change gets Planned start/Planned end time filled in.
	**Blackout.** Denotes a period in which change requests are not allowed to take place.
	**Change Window.** Denotes a period in which change requests are allowed to take place.

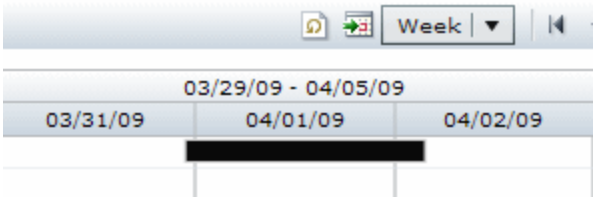
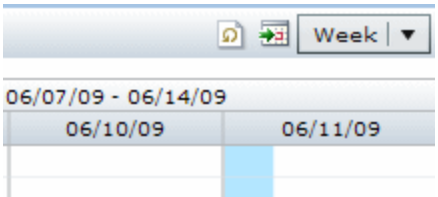
UI Elements (A-Z)	Description
<Color of time period>	The color assigned to the time period category as defined by the Release Control administrator. This is the color that Release Control uses to display the category in the Analysis module.
Time Period	The time period category defined by the Release Control administrator, with which the change request is conflicting.

Timeline Pane

This pane displays the occurrences of the time period conflict of the selected change request in a timeline.

The following elements are included:

UI Elements (A-Z)	Description
	Select Time Period. Displays a list of time period categories in which the request meets the criteria of the category's selected filter. You can select the configured time periods you want to display in the background. **Default:** All the time periods are displayed. For information on how to configure time periods, see Time Period Configuration Overview.
	Reset Time Line. Returns you to the start time of the selected change request.
	Now. Displays the current date.
Day Day Week Month	Select a time frame over which to display the change requests. • **Day**. Displays the change requests for the selected date only. • **Week**. Displays the change requests for the week surrounding the selected date. • **Month**. Displays the change requests for the month surrounding the selected date. By default, the time frame that appears depends on the duration and end time of the change request.
	Select Date. Select the date you want to display. The calendar displays the week around the selected date. **Note:** The latest date which Release Control enables you to

UI Elements (A-Z)	Description
	navigate to in the calendar is whichever of the following is longer: • The current date + 60 days Note that the value 60 is the default which can be modified. For details on how to configure time periods, see Time Periods Tab. or • The planned end date of the selected change + 30 days
<Selected change request in the timeline>	The selected change request in the timeline is represented by a thick, black line. 
<Selected date>	Displays the selected date. The calendar displays the day, week, or month around the selected date, depending on which time frame was selected.  You can either use the **Select Date** button, or alternatively, scroll through by clicking the left/right arrows.
<Time period in the timeline>	The time period in the timeline is displayed in the color defined by the Release Control administrator. 
<Timeline>	Displays the planned duration of the selected change request in a timeline as well as the time period categories to which the time period belongs.

Change Planner Dialog Box

This dialog box enables you to simulate the effects of modifying the details of a change request.

You use the Change Planner to simulate the effects of modifying the following change request details:

- The planned start and end of the change request.
- The CIs that are changed as a result of the change request (CCIs).

To access	• Select **Module** > **Analysis** > **Change Requests** and then click **Plan Selected Change** . • Click **Assess** > **Time Period Conflicts** and then click **Plan Selected Change** . Click the drop-down arrow next to the **Change Planner** button and select one of the following options: • **Plan Selected Change.** The Change Planner opens, displaying the current details of the selected change request. Use this option to simulate changes to an existing change request. • **Plan New Change.** The Change Planner opens without any current change request data. Use this option to simulate a new change.
Important Information	If you are using Service Manager as your service desk, you can save the updated planned start and end times of the change request to the service desk.
Relevant tasks	Use the Change Planner to Reschedule a Change

User interface elements are described below:

UI Elements (A-Z)	Description
	Run Simulation. Runs the change planner simulation. **Notes:** • The simulated results are displayed in the Change Planner details pane. • If you are planning an existing change and you are satisfied with the results of the simulation, you can save the updated planned start and end times of the change request to the originating service desk. The save action is only available if you are using Service

UI Elements (A-Z)	Description
	Manager as your service desk.
	Save. Saves the updated planned times of the change request to your service desk. **Notes:** • If you are simulating a new change, this option is not available. • Available only if you are using Service Manager as your service desk. • If Release Control is not integrated with Lightweight Single Sign-On (LW-SSO), you are asked to fill in your Service Manager credentials.
	Open the Original Request. Opens the Change Request in the originating service desk. **Notes:** • If you are simulating a new change, this option is not available. • To enable this option, see Linking to Release Control Interfaces from the Service Desk.

Scheduling Pane

This pane enables you to set the planned start and end for the change request simulation. If you are working with Service Manager, you can save the updated times to your service desk.

User interface elements are described below:

UI Elements (A-Z)	Description
	Reset Time. Enables you to restore the currently planned times.
	Get Suggested Time. Enables Release Control to suggest the next possible time for implementing the change, which is either within a **Change Window** and outside a **Blackout** period associated with the change request. Release Control does not suggest a time in the following cases: • If there is no time periods associated with the change • If the change is within a Blackout period and there is no future Change Window

UI Elements (A-Z)	Description
	Note: When the planned end of the change request is later than the **Requested End** field as specified in the request ticket in the service desk application, the following warning appears: `Requested end exceeds the planned end of the change request.`
<< >>	Scroll to the previous and next suggested times. **Note:** These button appear only if Release Control has suggested another time. They are only enabled when there is more than one possible suggested time.
Accept	Accept the time suggested by Release Control and run the change planner simulation according to the suggested time. **Note:** Appears only if Release Control has suggested another time.
Cancel	Restore the previous time. **Note:** Appears only if Release Control has suggested another time.
Lock duration	Enables you to lock the duration of the change. For example, if this option is selected and you modify the planned end time to 4 hours later, the planned start time is automatically adjusted to 4 hours later so that the duration of the change remains the same. Appears when this option is selected, that is, when the duration of the change is locked. Appears when this option is not selected, that is, when the duration of the change is not locked.
Planned duration	The difference in time between the start time and the end time of the change request.
Planned end	Use the calendar to set the date and time for the planned end of the change request **Note:** If the change request does not include a planned end time, this box is empty.
Planned start	Use the calendar to set the date and time for the planned start of the

UI Elements (A-Z)	Description
	change request **Note:** If the change request does not include a planned start time, this box is empty.

Change CIs Pane

This pane enables you to select the CIs (CCIs) that have changed as part of the change request simulation.

User interface elements are described below:

UI Elements (A-Z)	Description
	Reset CIs. Enables you to restore the current changed CIs.
	Show Business CIs/System CIs. Toggles between displaying either Business CIs or System CIs.
	CI Attributes. Enables you to view the attributes of the selected CI. Opens the CI Attributes window. **Notes:** • To customize the attributes that Release Control displays, see CIs Display Pane. • If more than one CI is selected or if no CI is selected, this button is disabled.
	Advanced CI Search. A link that opens the CI Selector within Universal CMDB. Enables you to import CIs that do not yet exist in Release Control's database, and import them into Release Control. The imported CIs appear in the Selected CIs pane. For details about the CI Selector, see Universal CMDB documentation. **Notes:** • You cannot view the CI Selector with Firefox 3.0.9. • If you are using Universal CMDB 9.0, the CI Selector works only if the Release Control and Universal CMDB servers are under the same domain. • If Lightweight Single Sign-On Authentication Support (LW-SSO) is enabled, you can set the CI Selector to open automatically. If LW-SSO is not enabled, Universal CMDB's

UI Elements (A-Z)	Description
	login page opens. • The CIs that are imported into Release Control from Universal CMDB are not added to the database. Once you close the Change Planner dialog box, the imported CIs no longer appear in the Selected CIs pane. • This button only appears if the Universal CMDB version to which you are connected is version 8.01 or later.
	Find. Search for a specific Business/System CI by entering the name or part of a name in the search box. The search returns all Business/System CIs that contain the entered string somewhere in the name. Click the **Find** button to run the search.
<View other pages>	To view other pages, use the left and right arrows. The number between the left and right arrows indicate which page is currently being displayed. For example, 3 of 5 means that the 3rd page out of 5 is being displayed. Page 3 of 5
Available Business CIs/System CIs pane	Contains a list of the available Business/System CIs that can be used in the simulation. Select one or more of the required CIs (using the CTRL key) and then click the top arrow to move them to the **Selected CIs** list. Only the selected CIs are included in the simulation.
Selected CIs pane	Contains a list of the Business/System CIs to be included in the simulation. Select one or more of the required CIs (using the CTRL key) and then click the bottom arrow to move them to the **Available Business CIs/System CIs** list. The CIs that were moved to the **Available Business CIs/System CIs** list are not included in the simulation. **Note:** The CIs that appear in this pane are displayed by their display label. If two or more CIs appear with identical display labels, you can use the CI Attribute window to distinguish between them by viewing their their different attributes. To open the CI Attribute window, click **CI Attributes**.

Preview Tab

This tab displays the current planned times of the change compared with the simulated times, as well as a summary of the current analysis results compared with the simulated analysis results.

The following elements are included:

UI Elements (A-Z)	Description
Analysis Info Pane	Displays a summary of the current analysis results compared with the simulated analysis results. For more information, see Preview > Overview Tab.
Time Window Info Pane	Displays the current planned times of the change compared with the simulated time. **Planned start.** The date and time for the planned start of the change request. **Planned end.** The date and time for the planned end of the change request. **Duration.** The difference in time between the start time and the end time of the change request. **Requested end.** The latest date and time for the end of the change request as specified in the request ticket in the service desk application. **Note:** When the planned end of the change request is later than the end of the change request as specified in the request ticket in the service desk application, the following warning appears: `The requested end exceeds the planned end of the change request as specified in the ticket.`

Impact Tab

This tab displays the impact analysis of the simulation.

Important Information	The information in this tab is presented in the same way as in the Analysis module's Assess > Impact tab. For more information about viewing impact analysis results, see Assess > Impact Tab.

User interface elements are described below:

UI Elements (A-Z)	Description
	Enables you to view the current impact analysis or the simulated impact analysis and select the relevant option from the list. **Note:** This option is relevant only if you are planning an existing

UI Elements (A-Z)	Description
	change.

Collisions Tab

This tab displays the collision analysis of the simulation.

User interface elements are described below:

Important Information	The information in this tab is presented in the same way as in the Analysis module's Assess > Collisions tab. For more information about viewing collision analysis results, see Assess > Collisions Tab.

UI Elements (A-Z)	Description
	Enables you to filter the information displayed in the tab and select one of the following options from the list: • **Simulated Collisions.** Displays all the collisions that occur when the simulated settings are applied. • **Additional Collisions.** Displays the additional collisions that occur as a result of the simulated settings. These collisions do not occur for the current settings. • **Unresolved Collisions.** Displays the collisions that are common to both the current settings and the simulated settings. These collisions are not resolved as a result of the simulated settings. • **Resolved Collisions.** Displays the collisions that are resolved as a result of the simulated settings. These collisions occur for the current settings and do not occur for the simulated settings. **Note:** This option is relevant only if you are planning an existing change.

Time Period Conflicts Tab

This tab displays the time periods conflict analysis of the simulation.

Important Information	The information in this tab is presented in the same way as in the Analysis module's Assess > Time Period Conflicts tab. For more information about viewing time period conflict analysis results, see Assess > Time Period Conflicts Tab.

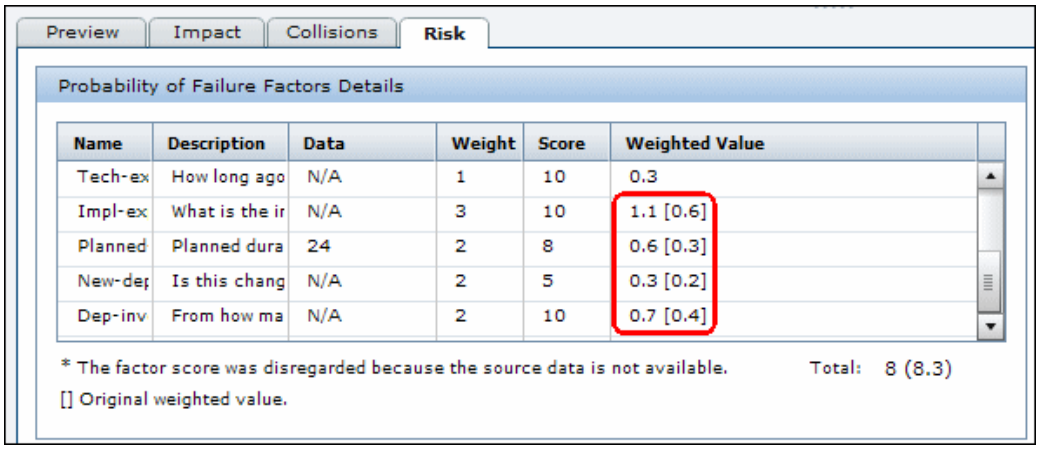
User interface elements are described below:

UI Elements (A-Z)	Description
	Enables you to filter the information displayed in the tab and select one of the following options from the list: • **Current Time Conflicts.** Displays all the time period conflicts for the currently displayed date. • **Simulated Time Conflicts.** Displays all the time period conflicts that occur when the simulated settings are applied. **Note:** This option is relevant only if you are planning an existing change.

Risk Tab

This tab displays the risk analysis of the simulation.

In the risk factor tables, in the **Weighted Value** column, for each risk factor that changed, the original weighted value is displayed in square brackets.



Important Information	• The information in this tab is presented in the same way as in the Analysis module's Assess > Risk tab. For more information about viewing risk analysis results, see Assess > Risk Tab. • This option is relevant only if you are planning an existing change.

Change Requests – Calendar View

The Change Requests — Calendar View pane displays change requests that have been processed by Release Control for each calendar day in calendar format. The change requests that appear are those that are included in the currently active filter.

This pane displays the change requests in calendar and/or list format depending on which viewing mode you selected:

- **Day and Week mode.** Displays the change requests processed by Release Control in both table and calendar format.
- **Month mode.** Displays the number of change requests for each calendar day as a link.

To access	Select **Modules** > **Analysis** > **Change Requests**. In the Change Requests pane, click **Calendar**.
Important Information	• Change requests with no start or end times, or with start times later than their end times, do not appear in the Calendar view. • By default, the calendar week begins on Monday and ends on Sunday. • The bar color of the change requests in **Day** and **Week** modes indicates the color to which the value of a field is mapped to in **Module** > **Administrator** > **Modules** > **Analysis** > **Calendar**. For example, you can map Medium for impact severity to purple. To reconfigure these settings, see Calendar Pane.

User interface elements are described below:

UI Elements (A-Z)	Description
< Today >	Enables you to select the: • Previous day/week/month • The current date • The next day/week/month
Day Week	**Day mode.** Displays the change requests for the selected date only. Day mode is divided into four equal periods of six hours each. **Week mode.** Displays the change requests for the week surrounding the selected date. In **Day** or **Week** mode, the Change Request pane displays the change requests that have been processed by Release Control in

UI Elements (A-Z)	Description
	the form of a table and in calendar format. You can enlarge or decrease the size of the table and the calendar by clicking and dragging the vertical line dividing them to the left or the right. > **Note:** The table that appears on the left contains the same columns as the Change Requests—List View. For details, see Change Requests — List View. You cannot sort the order of the appearance of the requests. Each column represents a calendar day and each bar represents a single change request. The data is displayed as blocks of time on a timeline. Each entry is displayed on a separate row. The view resembles a typical Gantt chart, providing a time-based overview. When you hold the mouse pointer over different items, a tooltip appears displaying detailed information about those items. When you click a row entry, details and analysis information are displayed in the Preview, Assess, Collaborate, and Review panes. You can choose to display the configured time periods in the Calendar view. You do so by clicking the **Select Time Periods** button and selecting the time period categories you want to view. When you hold the mouse pointer over an icon, the name of the category to which the time period belongs as well as the period's start and end times are listed in the tooltip.
Month	**Month mode.** Displays the change requests for the month surrounding the selected date. In **Month** mode, the Change Request pane displays the change requests in calendar format only and the <Change Request Summary Chart pane> appears below the Change Request pane to display the aggregated data in graphic format. For details, see <Change Request Summary Chart Pane>. The change requests appear as a link. When you click the link, Release Control automatically switches to **Day** mode and displays the change requests in table format.
<Change Request Summary Chart pane>	Displays graphs that represent the data of a specific field for the change requests that are included in the currently active filter. For details, see Change Request Summary Chart Pane.
<Date selector>	Enables you to select the change requests you want to display. > **Note:** If you are in **Day** or **Week** mode, you can use the Shift key to select additional adjacent dates.

UI Elements (A-Z)	Description
<Toolbar>	For details, see Change Requests Toolbar Options.
Filters pane	Enables you to filter the change requests displayed in the Change Requests pane. For details, see Filters Pane. **Note:** By default, Release Control displays all the change requests in the system. When a filter is being used, it filters the change requests in all of the different views

Change Request Summary Chart Pane

This pane displays graphs that represent the data of a specific field for the change requests that are included in the currently active filter. The data can appear in column graph or pie chart format.

Note: This pane appears in **Month** mode only.

To access	Select **Modules** > **Analysis** > **Change Requests**. In the Change Requests pane, click **Calendar**.
Important Information	• The graphs support fields whose data group uses values that represent only one number. For example, graphs can display the priority levels of a change request, where a priority of **Low** is given the value of 1, **Normal** is given the value of 2, and **High** is given the value of 3. The graphs do not support fields where the value is a group of numbers. For example, time fields that contain the value mm/dd/yy. • You can define the fields whose data you want to appear in the monthly Calendar view, as well as determine the default graphic format in which the data is displayed. For details, see Charts Pane. By default, three fields are configured. If you choose not to define any fields, then no graphs appear in the Calendar view. • If there are more than eight values, then **(Top 8)** is displayed at the top of the pane. • The colors of the fields that appear in the graphs are defined in the Calendar mapping pane. The Calendar mapping pane enables you to configure a color mapping scheme that associates a color with an existing field value. If a field value is not mapped in the Calendar mapping pane, the field value gets the default color that is defined in the **Default color** box. For details, see Calendar Pane.

User interface elements are described below:

UI Elements (A-Z)	Description
	Column graph. Displays the field data in column graph format. The column graph displays up to the eight highest values per field, from high to low, starting from the left. If there are bars that have the same amount, then they are displayed in alphabetical order. A tooltip indicating the name of the value is visible when you hold the mouse pointer over each bar.
	Pie chart. Displays the field data in pie chart format. The pie chart displays up to the eight highest values per field. A tooltip indicating the number of changes, the value represented by the slice, and its percentage of the pie, is visible when you hold the mouse pointer over each section. If there are more than eight values, then another segment is created called **Others**, which represents all the other values combined into one.
	Legend. Provides the complete name of each field value. **Note:** The legend can be dragged to any place on the screen.

Change Requests – List View

The List view displays the change requests that have been processed by Release Control in the form of a sortable table. You can sort the order of appearance of the requests according to each column by clicking the appropriate column heading.

In the List view, changes appear, by default, in descending order according to their impact severity. In **Day** and **Week** modes of the calendar view change requests appear in ascending order according to their scheduled start times.

When you select a change request in the list, details and analysis information for the selected change request are displayed in the Preview, Assess, Collaborate, and Review panes.

You can view the related tasks for each selected change request in the Preview > Related Records Tab.

To access	Select **Module** > **Analysis** > **Change Requests** and then click **List**.
Important Information	• You can filter the change requests displayed in the Change Requests mode. For details, see Filtering Change Requests and Activities. By default, Release Control displays all the change requests in

	the system. When you use a filter, it displays only the change requests that meet the conditions of the selected filter. • You can customize the List view to display different information. For details on customizing the List view columns, see <Bottom Pane> - List Tab.

Unless otherwise customized by the administrator, the following elements are included:

UI Elements (A-Z)	Description
Abnormal	An icon Indicates that the change request occurred either outside of a Change Window (periods in which change requests are allowed to take place) or within a Blackout period (periods in which change requests are not allowed to take place).
Collision Severity	Displays an icon indicating the collision severity level of the change request. If the change request collides with more than one other change request, the severity level for the worst collision is displayed. By default the following color-coded icons (which also include symbols) indicate the following severity levels: • **Critical** • **High** • **Medium** • **Low** • **Very Low** If there are no collisions with the change request, no collision severity icon is displayed. A tooltip indicating the severity level of the collision is visible when you hold the mouse pointer over the collision severity icon. For more information about collisions and how collision severity is calculated, see Change Request Collisions.
Contact Person	Displays the name of the user responsible for the change request.
Impact Severity	Displays an icon indicating the impact severity level of the change request. The severity level for the change request is determined by the highest severity level of the business CI affected by the request. By default the following color-coded icons (which also include symbols) indicate the following impact severity levels: • **Critical**

UI Elements (A-Z)	Description
	• **High** • **Medium** • **Low** • **Very low** • **No impact analysis available** A tooltip indicating the impact severity level of the change request is visible when you hold the mouse pointer over the severity level icon. For more information about impact analysis and how impact severity is calculated, see Impact Analysis.
Priority	Displays the Release Control priority level of the change request. When you configure Release Control, you configure the priority levels that can be assigned to a change request.
Request ID	Displays the reference ID number of the change request in the service desk application.
Risk	Displays the risk level (low, medium, or high). These levels can be manually configured to correspond to different numeric risk levels. Release Control calculates this figure based on risk factors that are subjectively weighted by the Release Control administrator during the configuration process. For more information about how the risk level is calculated, see Risk Analysis.
Start	Displays the date on which the change request is scheduled to begin.
Status	Displays the Release Control status of the change request. When you configure Release Control, you configure the statuses that can be assigned to a change request.
Summary	Displays a brief description of the change request.
User Discussion Threads & Posts	The presence of a user discussion threads & posts icon indicates that user discussion threads and comments to these threads exist in response to the selected change request. A tooltip indicating how many discussion threads and comments exist is visible when you hold the mouse pointer over this icon. You can view the discussion threads themselves in the Collaboration tab's Discussion view. For details, see Collaborate > Discussion Tab.

Change Requests Toolbar Options

This section describes the toolbar options for the Change Requests pane.

To access	Select **Module** > **Analysis** > **Change Requests**.
See also	• Change Requests — List View • Change Requests — Calendar View

The following table contains a description of each toolbar option in the Change Requests — List view.

UI Elements (A-Z)	Description
	List. Displays the Change Requests in a list format. Opens the Change Requests — List view.
	Calendar. Displays the Change Requests in a calendar format. Opens the Change Requests — Calendar view.
	Plan Selected Change. Enables you to simulate the effects of modifying the details of a change request and to view how these modifications influence the analysis data. Click the drop-down arrow and select one of the following options: • **Plan Selected Change.** • **Plan New Change.** Opens the Change Planner.
	New Discussion Thread. Enables you to add a new thread to the discussion in the Votes pane in the Collaborate > Discussion tab. Opens the New Discussion Thread Dialog Box.
	New Action Item. Used to create an action item associated with the request. Opens the Add/Edit Action Item Dialog Box.
	Launch manual change process. Enables you to manually rerun the recalculation process for a selected change request or all the change requests in a selected filter. Opens the Launch Manual Change Process Dialog Box.
	Generate Report. Enables you to generate a PDF, an HTML report, or an Excel report. Opens the Report Details Dialog Box.
	Send change data. Enables you to send discussion threads by email. Click the drop-down arrow and select one of the following options:

UI Elements (A-Z)	Description
	• **Send Change data.** Send an email containing only the selected change request. • **Send Change data and log.** Send an email containing the selected change request as well as the event log information associated with it. • **Send CAB invitation.** Send an invitation to the CAB meeting. • **Send CAB minutes.** Send the CAB minutes of the selected change. • **Send PIR invitation.** Send an invitation to the PIR meeting. • **Send PIR minutes.** Send the PIR minutes of the selected change.
	Add Selected Request to Favorites/ Delete Selected Request from Favorites. Toggles between adding or removing the selected change request from the Favorites filter. For details, see Filtering Change Requests and Activities. Click the drop-down arrow and select one of the following options: • **Delete from Favorites.** Deletes the selected change request from the Favorites filter. • **Delete all AI's in the Favorites Filter.** Deletes all the change requests in the Favorites filter. **Note:** You can also subscribe to receive notifications when certain modifications are made to favorite change requests. For details, see User Workspace Pane.
	Subscribe to Selected Request/Unsubscribe from Selected Request. Enables you to receive email notifications or cancel a notification subscription for the selected change request. For information on configuring notification rules and conditions, see Notifications Pane. **Note:** Not all modifications to the change requests will trigger notification. Release Control will send email notifications to the users who subscribe to a change only when one of following events occurs: • Post Added Event: A new discussion post is added to the Change Request. • Action Item Added Event: A new action item is added to the Change Request. • Approved Event: The Change Request is approved.

UI Elements (A-Z)	Description
	• Retract Event: The Change Request is retracted.
	Select Time Period. Enables you to select the configured time periods to display in the background of the Calendar view. For information on how to configure time periods, see Time Period Configuration Overview. **Note:** Is enabled only in the Calendar view.
	Refresh. Enables you to refresh the change requests displayed in the Change Requests pane or the action items displayed in the Action Items List pane.
	Search for Request/Action Item ID. Locate a required change request or action item. • In the Change Request pane, enter a search request ID in the **Search for Change Request** box to locate the required changed request in the list of change requests. • In the Action Item pane, enter an action item ID in the **Search for Action Item** box to locate the required action item in the list of action items.
Total	The number of change requests that meet the set of criteria you defined. **Note:** In **Month** mode, the total number represents the actual number of changes for that month.

Collaborate > Action Items Tab

This tab enables you to view the change request's action items.

- If you are in Change Requests mode, this tab enables you to view the action items associated with a change request and work with these action items as you would in the Action Items pane of the Action Items mode.
- If you are in Action Items mode, this tab enables you to view all the action items associated with the same change request as the selected action item.

Action Items Pane

This pane displays the action items associated with a change request. For information on this pane, see Action Items Pane.

User interface elements are described below:

UI Elements (A-Z)	Description
Go	Displays the selected action item in the Action Items pane.

Action Item Postings Pane

Displays information for each action item selected from the list. For information on this pane, see Action Items Pane.

Collaborate > Discussion Tab

This tab displays the discussion threads and comments as well as a summary of the votes pertaining to the selected or associated change request. This tab enables users to conduct online discussions about a change request prior to the CAB actually meeting to discuss it. As a result, the CAB discussion can begin at a more advanced stage or may not be necessary at all if it is clear from the user responses whether or not the change request should be approved.

To access	Select **Module** > **Analysis** > **Change Requests** > **Collaborate** > **Discussion** tab.

Comments Pane

This pane displays all the discussion threads pertaining to the change request. Each thread includes a heading with the name of the user who initiated the discussion, an icon representing the vote posted by the discussion initiator, the date and time of the initial comment, the subject and text of the initial comment, and the comments posted by other users to the thread.

User interface elements are described below:

UI Elements (A-Z)	Description
	Expand All Comments. Enables you to expand all the comments included in the discussion threads.
	Collapse All Comments. Enables you to collapse all the comments included in the discussion threads.
	Older First / Newer First. Enables you to sort the comments to either display the oldest comment first or the newest comment first.
	New Discussion Thread. Enables you to add a thread to any change request. Opens the New Discussion Thread Dialog Box.

UI Elements (A-Z)	Description
	Send E-Mail. Enables you to send one or more discussion threads by email. Opens the Send Email dialog box opens. Enter the email address of each recipient of the email and any additional comments you have on the change request.

Votes Pane

This pane displays a summary of the most recent votes posted by discussion initiators for the change request.

User interface elements are described below:

UI Elements (A-Z)	Description
<Voting summary tree>	Displays the most recent votes posted by discussion initiators for the change request. Each available voting option is displayed (**Disagree**, **Agree**, **To CAB**, and **No Vote**) with the number of users who voted for that option displayed in parentheses. > **Note:** Only the user's most recent vote is taken into account. Under each voting option, a list of users (discussion initiators) who voted for that option is displayed. You can expand or collapse the list of users under each voting option by clicking the arrow next to the voting option. When you select a user, all the discussion threads initiated by that user are displayed in the Comments pane. To view all the discussion threads initiated by all the users in the Comments pane, click **All**. To sort the discussion threads chronologically, click the **Older First/Newer First** button. > **Note:** Users can initiate more than one discussion thread for each change request. All discussion threads are displayed along with the user's most recent vote.

Collaborate > Resolution Tab

This tab enables you to approve a change request or retract the approval, view approval history and status, and create CAB minutes and as pre- and post-implementation guidelines.

To access	Select **Module** > **Analysis** > **Change Requests** > **Collaborate** > **Resolution** tab.

Resolution Pane

> **This pane is only relevant if you are working with the following service desks:**
>
> - Service Manager
> - Project and Portfolio Management / IT Governance Center

This pane enables you to approve/deny a change request or retract an approval, and view approval history and status.

The approve, retract, and deny options depend on the status of the request, and is only available if you are a user with **approveChange** permissions. The approval/retraction/denial of a change request within Release Control results in an updated status of the request within the service desk application. If you are using Service Manager, the approval comments are also exported along with the updated status.

This feature enables you to manage the request approval process from Release Control, without having to directly access each request from within the service desk application.

Important Information	• When you approve a change request, Release Control checks whether your user name and password are correct and whether you are currently allowed to approve the change request. If so, Release Control approves the request and the approval details appear in the Collaborate tab. If the authentication data you provided is incorrect, or if you are not currently allowed to approve the change request, Release Control issues a detailed error message. If the service desk application's version of the request is more current than the version in Release Control, you receive a message asking whether you want to force the approval of the change request. Select the check box and click **Approve** to force approval. • The administrator can define the status for which the **approval button** is enabled. For details, see Configure Release Control for Request Approval.

User interface elements are described below:

UI Elements (A-Z)	Description
	**Approval Log.** Displays a history of approvals and retractions made in Release Control for the selected change. The users who approved the change request or retracted approval are listed, along with comments that they posted.
	**Approval Status.** You can view the approval status of the selected change.

UI Elements (A-Z)	Description
	The Resolution pane is divided into three approval categories. Each category lists the relevant user groups (for example, **Admin**). The following three approval categories are displayed: • **Completed Approvals.** Lists the user groups who have already approved the change. • **Pending Approvals.** Lists the user groups whose approval is still required. • **Future Approvals.** List the user groups who can only approve a change after a different user group has already approved it. The user groups that need to first approve the change, are listed in the **Pending Approvals** category.
  	**Approve.** Enables you to approve a change request. Opens the Approve Change Request dialog box. **Retract.** Enables you to retract the approval you gave for the selected request. Opens the Retract Change Request dialog box. **Deny**. Enables you to deny a change request. Opens the Deny Change Request dialog box. For more information about approving, retracting or denying a change request, see Approve/Retract/Deny Change Request Dialog Box. When you select the relevant change request, or action item in the Change Requests or Action Items pane, and then select the **Collaborate > Resolution** tab, the **Checking** status message is displayed as the tooltip for the **Approve**, **Retract** and **Deny** buttons while Release Control checks the following: • Whether you are a user with **approveChange** permissions, who is authorized to approve change requests. • Whether the selected change request can be approved at the current time. If all the above criteria are met, the **Approve** button is enabled. If request approval is not authorized by the service desk application, an **Operation not supported** status message is displayed as a tooltip for **Approve**, **Retract** and **Deny** buttons. If the change request was recently approved and its status has not yet been updated in Release Control, an **Approved** status message is displayed as the tooltip for the **Approve** button. If an error occurred during the Release Control verification process, an error message is displayed as the tooltip for the **Approve**, **Retract** , and **Deny** buttons.

CAB Decisions Pane

This pane enables you to post different types of notes regarding the approval/retraction/denial process.

Important Information	To perform this procedure, you must be a user with the role of **Change Manager**.

User interface elements are described below:

UI Elements (A-Z)	Description
	Add Decision. Enables you to post different types of notes regarding the approval/retraction/denial process. Opens a dialog box in which you can select the type of note you want to post: • **CAB Minutes.** Details of relevant CAB discussions. • **Pre-Implementation Guidelines.** Guidelines to follow before implementing a change. These guidelines appear in the Director module in the alerts pane before a change request is scheduled. • **Post-Implementation Guidelines.** Follow-up procedures after implementing a change. These guidelines appear in the director module in the alerts pane after a change request is scheduled. Enter the subject and content of the note in the dialog box that appears. The note appears in the CAB Decisions pane.

Impact Graph Window

This window displays a visual representation of the impact relationships of the selected change request.

You can manipulate the display by dragging and dropping individual CIs. The lines, arrows, and relationships are not affected.

Impact graphs for individual CIs or groups of CIs can be viewed by selecting the CI or CI group while in the impact graph window.

To access	Select **Module** > **Analysis** > **Change Requests** > **Assess** tab, click **Open Graph Window**.

User interface elements are described below:

UI Elements (A-Z)	Description
	Root Node. Returns the Impact Graph window to the original display if an impact graph for individual CIs or groups of CIs is the

UI Elements (A-Z)	Description
	current view.
	Concentric Radial Layout. Reorganizes the CIs in concentric radial layout.
	Hierarchy Layout. Reorganizes the CIs in hierarchy layout.
	Parent-Centered Radial Layout. Reorganizes the CIs in Parent-Centered Radial Layout.
	Spring Forced Layout. Reorganizes the CIs in Spring Forced Layout
	Zoom. Enables you to change the magnification by zooming in or out.
All Impact CIs Affect	Displays a visual representation of the impact relationships in graphic format. The CIs are connected by lines with arrows indicating the direction of impact. For example, if a CI named **host11** has an arrow pointing to **serverB**, it means that **host11** affects **serverB**. You can customize the impact graph layout to reorganize the CIs while still maintaining the same impact relationships.
Impact CIs	Displays the affected and changed CIs (ACIs and CCIs).

Launch Manual Change Process Dialog Box

This dialog box enables you to manually rerun the calculation process for a selected change request or all the change requests in a selected filter.

> **Caution:** Running the manual change process on a large number of changes may affect the performance of the system.

The following use cases describe situations in which you might need to rerun the calculation process manually:

- There is a change in Universal CMDB. For example, a change in a CI.
- There is a change in the configuration. For example, due to a changed CI, two change requests involve at least one common CI, causing a change request collision.
- There is a change in the risk factor configuration.

To access	Select **Module** > **Analysis** > **Change Requests**. In the Change Requests pane, click **Launch manual change process** .
Important Information	You cannot run the manual change process for latent changes or if you are using a filter that contains latent changes.

Launch New Process Pane

User interface elements are described below:

UI Elements (A-Z)	Description
Current Filter	Recalculates all the change requests in a selected filter. Click the downward arrow and select the required filter.
Description	Enables you to enter free text describing the recalculation process.
Run	Runs the recalculation process.
Selected change request	Recalculates the selected change request.

Calculating Change Requests Pane

User interface elements are described below:

UI Elements (A-Z)	Description
Abort	Select the check box to the left of the required recalculation processes and click **Abort** to end the manual recalculation. **Note:** You can always abort your own recalculation processes. To abort other users' processes, you require the **abortAnyManualChangeProcess** permission.
Auto remove completed from list	Select to automatically remove the recalculation processes from the pane once the process is complete.
Calculation status	After you click the **Run** button to launch the manual recalculation, a progress bar appears displaying the number of change requests that still have to be recalculated.
Description	Name of the recalculation process as described in the **Description** box in the Launch New Process pane.
Show processes from all users	Select this check box to display the manual recalculation processes launched by all users. If this check box is not selected, only the processes that you launched are displayed.
Started time	The time at which the recalculation process was submitted.

UI Elements (A-Z)	Description
User	The user that launched the manual recalculation process.

New Discussion Thread Dialog Box

This dialog box enables you to add a discussion thread to any change request. As part of the discussion thread, you can express an opinion about the change by selecting the required voting option.

You can add more than one discussion thread for each change request. All discussion threads along with the user's most recent vote are displayed in the Collaborate > Discussion tab.

To access	• Select **Module** > **Analysis** > **Change Requests**. From the toolbar in the Change Requests pane, click **New Discussion Thread**. • Select **Module** > **Analysis**> **Change Requests** > **Collaborate Discussion** tab. From the toolbar, click **New Discussion Thread**.
See also	Collaborate > Discussion Tab

User interface elements are described below:

UI Elements (A-Z)	Description
<Message box>	(Optional) Type the required message.
Subject	Type the required subject.
Voting	Select one of the following voting options. • **Disagree** • **To CAB** • **Agree** • **No Vote** If you voted on this change request before, your most recent vote is displayed as the **Current vote** on the right-hand side of the dialog box.

Post Implementation Review Dialog Box

This dialog box enables you to create/edit a Post Implementation Review (PIR) for a change request.

The PIR is added to the change request and all submitted PIR information appears in the Conclusions Information pane of the **Review > Conclusions** tab.

To access	Select **Module** > **Analysis** > **Change Requests** > **Review** > **Conclusions** tab, and then click **Review** in the Conclusion Information pane.
Important Information	• By default, Release Control enables you to create a PIR for a change request only with an **Evaluation and Closure** status. • If you are working with Service Manager, Release Control updates the PIR information directly to that application.
See also	Review > Conclusions Tab

Details Tab

This tab enables you to create/edit a PIR for the selected change request.

User interface elements are described below:

UI Elements (A-Z)	Description
Change outcome	Select the change request's outcome from the drop-down list.
Customer satisfaction	The customer is the person who opened the request ticket in the service desk application. Select the overall level of customer satisfaction for the request from the drop-down list.
Planning satisfaction	Select the overall level of planning satisfaction for the request from the drop down list.
Review comments	Add any comments that may be relevant.
Review date	Use the calendar to set the date and time for the review creation. The date and time of the first PIR creation is saved in the system. If you are editing a PIR, we recommend that you do not change this.
Service desk authentication	If you are working with Service Manager, enter your user name and password to update the PIR information directly to that application. This field does not appear if you are using any other service desk application.

Disrupted Business CIs Tab

This tab displays the business CIs that are included in the PIR.

The business CIs you include in the PIR appear in the Disrupted Business CIs pane of the **Review > Conclusions** tab.

The following elements are included:

UI Elements (A-Z)	Description
	Show only impacted business CIs/Show all business CIs. Toggles between displaying: • A list of all business CIs that are impacted by the current request (Show only impacted business CIs). • A list of all the relevant business CIs that Release Control recognizes in the Universal CMDB (Show all business CIs).
	Show Obsolete. View the obsolete business CIs.
	Find. Search for a specific business CI in the Available Business CIs list by entering the name or part of a name in the search box. The search returns all business CIs that contain the entered string somewhere in the name. Click the **Find** button to run the search.
<View other pages>	To view other pages, use the left and right arrows. The number between the left and right arrows indicate which page is currently being displayed. For example, 3 of 5 means that the 3rd page out of 5 is being displayed. Page 3 of 5
Available Business CIs	Contains a list of the available business CIs that are either impacted by the current request or business CIs that Release Control recognizes in the Universal CMDB. To include one or more of the business CIs in the PIR, select the required CIs (using the CTRL key), and then click the top arrow to move them to the **Disrupted Business CIs** list.
Disrupted Business CIs	Contains a list of the business CIs to be included PIR. To remove one or more of the business CIs from the PIR, select required CIs (using the CTRL key) and then click the bottom arrow to move them to the **Available Business CIs**list.

Preview > Details Tab

This tab displays the change request details that originate from the service desk application and some key analysis data processed by Release Control.

To access	Select **Module** > **Analysis** > **Change Requests** > **Preview** > **Details** tab.

Important Information	For details on customizing the Preview > Details tab, select **Module** > **Administrator** > **Configuration** > **Integrations** > **Fields** > **<Bottom Pane> - Details** tab. For details, see <Bottom Pane> - Details Tab.

User interface elements are described below:

UI Elements (A-Z)	Description
Actual end	The time at which execution of the change request actually ended.
Actual start	The time at which execution of the change request actually began.
Category	The category describing the type of change request.
Contact person	The name of the user responsible for the change request.
Contact location	The geographic location of the person responsible for the change request.
Created	The time at which the change request was originally created in the service desk application.
Emergency	Indicates that the change request is handled according to the Emergency Change procedure.
Estimated risk	The estimated risk level that was assigned to the change request by a user.
Impact severity	The Release Control-calculated impact severity level of the change request. For more details about impact severity, see Impact Analysis.
Implementors	The people responsible for implementing the change request.
Initiated by	The person initiating the request (first level change requests only).
Last impact analysis	The time at which an impact analysis was last calculated.
Last updated	The time at which the change request was last updated in the service desk application.
Opened by	The person initiating the request (second level change requests only).
Planned end	The time at which the execution of the change request is scheduled to end.
Planned start	The time at which the execution of the change request is scheduled to begin.
Priority	The Release Control priority level of the change request. When you configure Release Control, you configure the priority levels that can

UI Elements (A-Z)	Description
	be assigned to a change request.
Request ID	The reference ID number of the change request in the service desk application.
Requested end date	The latest date by which to implement the request.
Risk analysis	Displays the risk level (low, medium, or high) calculated by Release Control. For more information about how the risk level is calculated, see Risk Analysis.
Scheduled downtime start	The change activity's planned downtime start time.
Service desk	The service desk application in which the change request originated.
Subcategory	Elaborates on the **category** field, and describes the type of change request in further detail.
Urgency	The urgency assigned to the request by the request initiator.

Preview > Overview Tab

This tab displays a summary of the change request information received from the service desk application.

To access	Select **Module** > **Analysis** > **Change Requests** > **Preview** > **Overview**tab.

User interface elements are described below:

UI Elements (A-Z)	Description
Analysis Info	Displays a summary of the change analysis performed by Release Control for the change request and includes the following data: • **Impact severity.** Displays the impact severity level of the change request as represented by the impact severity icon. A tooltip indicating the impact severity level of the change request is visible when you hold your mouse over the icon. The icon serves as a link to the Impact Analysis tab. For more information about impact analysis and how impact severity is calculated, see Impact Analysis. • **Collisions.** Displays the collision severity level of the change request as represented by the collision severity icon. If the change request collides with more than one other change request, the severity level for the worst collision is displayed. A

UI Elements (A-Z)	Description
	tooltip indicating the severity level of the collision is visible when you hold your mouse over the icon. The icon serves as a link to the Collisions tab. For more information about collisions and how collision severity is calculated, see Change Request Collisions. • **Risk.** Displays the risk level (low, medium, or high). The displayed level serves as a link to the Risk tab. For more information about the Risk tab and how the risk level is calculated, see Risk Analysis. • **Changed CIs.** Displays the number of CIs that were changed as a direct result of the change request. The displayed number serves as a link to the Impact Analysis tab. • **Affected business CIs.** Displays the number of business CIs that were affected as a result of the change request. The displayed number serves as a link to the Impact Analysis tab. • **Time period conflicts.** If the change request breached the recurrence rules of a time period category, the name of the category is displayed. The displayed category serves as a link to the Time Period Conflicts tab.
General Info	• **Request ID.** The reference ID number of the change request in the service desk application. • **Service desk.** The service desk application from which the change request originated. • **Scheduled for.** The scheduled start time of the change request. • **Duration.** The scheduled duration of the change request. • **Status.** The status of the change request as defined in the service desk application. • **Outcome.** The outcome of the change request. The outcome is submitted in the Review tab. The Outcome value links to the Review > Conclusion tab.
User Info	Displays the following information: • **Discussion threads.** The number of discussion threads posted by users in response to the change request. • **Disagree.** The number of users who posted the vote **Disagree** in response to the change request. • **To CAB.** The number of users who posted the vote **To CAB** in response to the change request. • **Agree.** The number of users who posted the vote **Agree** in response to the change request.

UI Elements (A-Z)	Description
	Note: The data links to the Collaboration Discussion tab. For details, see Collaborate > Discussion Tab.

Preview > Related Records Tab

From version 5.0, change requests and their tasks (related records) no longer appear together in the same pane. Release Control enables you to view change requests and their related tasks in different panes.

- When you are in Change Request mode:
  - If the change requests appear in the Change Request pane, the tasks that are assigned to the selected change appear in the Preview > Related Records tab.
  - If the change requests appear in the Preview > Related Records tab, the the tasks that are assigned to the selected change appear in the Change Request pane.
- When you are in Action Item mode, the tasks always appear in the Preview > Related Records tab.

To access	Select **Module** > **Analysis** > **Change Requests** > **Preview** > **Related Records** tab.
Important information	By default, change requests are displayed in the Change Requests pane and their related tasks are displayed in the Preview > Related Records tab. This is configured by selecting **Change** in the **Hierarchy** box in the Activity/Change Request Filter dialog box. (Select **Module** > **Analysis** > **Change Requests**. In the Filters pane, click the downward arrow to the right of the **New** button and select **New** or **Edit**.) Alternatively, you can configure the related tasks to be displayed in the Change Requests pane by default by selecting **Task** in the **Hierarchy** box.
See also	◦ Change Requests — List View ◦ Action Items Pane

User interface elements are described below:

UI Elements (A-Z)	Description
	Open Related Records. Toggles between displaying the tasks and change requests in the Change Requests pane and the Preview > Related Records tab.

UI Elements (A-Z)	Description
	Notes: • This button is enabled in the Change Requests pane only. • When you click this button, Release Control automatically creates a temporary filter called **Related Records**. • In Change Request mode, you can display the items from your previous filter by clicking the **Back** button. For details, see Filters Pane.
<columns>	For a description of the columns that appear in this tab, see Change Requests - List View.
Total	The number of records assigned to the selected item in the Change Requests or Action Items pane.

Report Details Dialog Box

This dialog box enables you to generate a PDF, an HTML, or an Excel report that contains data for a single change request, or all the change requests included in the current filter.

To access	Select **Module** > **Analysis**. Then select the change request, or filter, for which you want to create a report, and click **Generate Report**.
Important Information	If you are working in an Asian language environment and want to generate PDF reports, you must modify the PDF encoding value (currently defined as CP1250) within the following report template files, located in the **<Release Control installation directory>\conf\reports.ext** directory: • **calendar.changes-report.days-subreport.pdf.jrxml** • **calendar.changes-report.pdf.jrxml** • **calendar.changes-report.tickets-subreport.pdf.jrxml** • **grid.change-single-pager-report.pdf.jrxml** • **grid.changes-report.pdf.jrxml** • **grid.changes-report.tasks-subreport.pdf.jrxml**
See also	Reports Panes

User interface elements are described below:

UI Elements (A-Z)	Description
Data	Depending on the data you want to view in the report, choose the required request range. The options are: • **Current filter.** All the change requests in the selected filter. • **Selected change request.** The currently selected change request. **Note:** If the number of change requests in the report exceeds the maximum number of change requests that can be included in a generated report, as defined in Reports Panes, the following warning appears: `Your selection exceeds n (the maximum number of requests for a report). Some of the requests will be omitted from the report.`
Format	Select the required report output type. The options are: • **PDF** • **Excel** **Note:** This option only appears when you select **List** as your Layout option. • **HTML**
Layout	Choose the required request layout option: • **One page.** Displays the data for each change request on a separate page. **Note:** This option only appears in List view mode. • **List.** Displays the data for each change request concisely, in a list format. Several lists are displayed on each page.
Level Policy	Enables you to define whether you want to include child change requests (tasks) as well as parent change requests (changes) in the report. Select: • **Collapsed**, to include data for parent change requests (changes) only. • **Expanded**, to include child change requests (tasks) as well as parent change requests (changes) in the report. **Default value:** Collapsed

Respond Dialog Box

This dialog box enables:

- Any Release Control user can add a comment to any action item that is not closed.
- The assignee of an action item to return the action item to its creator, if, for any reason he/she does not want to accept it.
- The assignee of an action item to change the status of an action item from **Open** to **Done**.
- The creator of an action item to change the status of an action item from **Open** or **Done** to **Closed**.

To access	Select **Module** > **Analysis** > **Action Items**. In the Action Items pane, select the required action item and click Respond.
Important Information	The Respond button is enabled only when the action item selected is assigned to the current user.

User interface elements are described below:

UI Elements (A-Z)	Description
Description	• If you have selected **Post and pend the action item on <creator>**, enter the reason why you do not want to accept the action item. • If you have selected **Respond with a post**, enter the full text of your comment.
Inform <creator> that the action item is done	Enables the assignee to change the status of an action item from **Open** to **Done**. For details about the statuses of action items, see Status. **Note:** This option appears when the selected action item is assigned to the current user and does not yet have a **Done** status.
Post and pend the action item on <creator>	Enables you, as the assignee, to return the action item to its creator if for any reason you do not want to accept it. **Send it back to: <creator>** appears in the **Subject** box. **Note:** Your action is now listed as a comment in both the Action Items List pane and the Collaboration tab's Action Items view pane. The action item is now listed as pending on the creator.

UI Elements (A-Z)	Description
Reopen the action item and inform <assignee> that it needs more work	Enables the creator to change the status of an action item from **Done** to **Reopen** or **Closed**.
Respond with a post	Enables any Release Control user to add a comment to any action item that is not closed. When the action item is selected in either the Action Items List pane or the Collaboration tab's Action Items view, the comment appears in the Action Item Posting pane.

Review > Conclusions Tab

This tab enables the Change Reviewer to:

- Add review notes to any change request with an **Evaluation and Closure** status.
- Close the request so that no further modifications can be made to it.

The review notes present the conclusions regarding the request, providing information about its overall success and satisfaction levels of relevant parties.

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

To access	Select **Module** > **Analysis** > **Change Requests** > **Review** > **Conclusions** tab.
Important Information	• The Change Reviewer can use the **Send by E-mail** button on the Change Requests toolbar to send an email invitation to participate in a PIR meeting, as well as a summary of the PIR conclusions for any completed request. • You can define a change request filter according to review-related criteria. For details, see Filtering Change Requests and Activities.
See also	Post Implementation Review Dialog Box

Conclusion Information Pane

This pane enables you to create/edit a PIR for any change request with an **Evaluation and Closure** status.

If you are working with Service Manager, you can also close the request so that no more modifications can be made to it.

Important Information	The **Close** button in this pane is available only if you are working with Service Manager. If you are using any other service desk application, the **Close** button is disabled.

User interface elements are described below:

UI Elements (A-Z)	Description
	If you are fully integrated with Service Manager, clicking this button enables you to create/edit a PIR for any change request whose status is not **Closed**. Opens the Post Implementation Review dialog box. **Note:** If you are using any other service desk application, the button is disabled.
	If you are fully integrated with Service Manager, clicking this button enables you to close the request directly to Service Manager so that no more modifications can be made to it. **Note:** If you are using any other service desk application, the button is disabled. Opens the Login dialog box. Enter your Service Manager user name and password. If the operation is successful, the ticket is updated in Service Manager, which then updates the request in Release Control to a **Closed** status.
<Conclusion information>	Contains the review information entered in the Post Implementation Review dialog box for the selected request.

Disrupted Business CIs Pane

This pane displays the disrupted business CIs selected in the Post Implementation Review dialog box to be included in the PIR.

Review > Event Log Tab

This tab displays all events related to the selected activity.

These events can be either user- or system-induced.

- User-induced events include:
  - Updates to the status of an activity
  - Changes to an activity's implementation schedule

  - Alerts handled for an activity
  - Notes submitted about an activity
  - Similar changes added/confirmed/deleted
  - Approval, denial, or retraction of approval of change requests
  - Minutes or implementation guideline posted
  - Management of Action Items
  - Post Implementation Review updates
  - Votes posted for a change request
- System-induced events include:
  - Alerts generated for an activity
  - Processes on a change request, such as risk analysis, impact analysis, and collision analysis

To access	• **In Analysis module:** Select **Module** > **Analysis** > **Change Requests** > **Review** > **Event Log** tab. • **In Director module:** Select **Module** > **Director** > **Control**. In either the Activity Timeline or Alerts pane, click **Activity Information** to open the Activity Information dialog box. Then click the **Event Log** tab.

User interface elements are described below:

UI Elements (A-Z)	Description
Description	A description of the event.
Time	The time that the event was written to the Event Log.
User	• System-induced events are listed under the user name, **System**. • User-induced events display the name of the relevant user.

Review > Verifications Tab

This tab enables you to view data for **detected** and **latent** changes.

The selected request's detected changes are displayed along with information received from the Universal CMDB.

For more information on detected and latent changes, see Detected and Latent Changes.

The Detected Changes pane displays the following information for each detected change:

- **CI Name.** The name of the CI that was changed.
- **CI Type.** The type of CI that was changed.
- **Change Type.** The type of change performed on the CI.
- **Detection Window.** The change detection time range when the detected change was discovered.

The Changed Attributes pane displays the following information for each detected change:

- **Attribute.** The specific aspect of the CI that was changed. For example, the operating system (OS_VERSION).
- **Old Value.** The attribute's definition before the change. For example, XP SP1.
- **New Value.** The attribute's definition after the change. For example, XP SP2.

Latent changes are displayed as separate changes in the Change Requests List View, along with all the other change requests. A latent change is indicated by the **Latent** icon and the words **Latent change** in the List view's Summary column.

To access	Select **Module** > **Analysis** > **Change Requests** > **Review** > **Verifications** tab.
Important Information	• This feature may not be available in your Release Control application. For more information, contact your Release Control administrator. • This section assumes that the latent change feature is fully activated.

Filtering Change Requests and Activities

This chapter includes:

Concepts

- Change Request and Activity Filter Overview
- Regular Expressions

Tasks

- Create a Union Filter

Reference

- Filtering User Interface

Concepts

Change Request and Activity Filter Overview

You can filter change requests in the Analysis module and activities in the Director module. You can select either a public filter or a filter that you previously defined, or you can define a new filter. You can also use the Quick Filter fields to display commonly required information in the Change Requests pane.

Regardless of where you create the filter, the same filters are visible in both the Analysis and Director modules.

For details on the Analysis module, see Analysis Module. For details on the Director module, see Director Module.

This section also includes:

- Using Filters in the Analysis Module
- Using Filters in the Director Module

Using Filters in the Analysis Module

You can use the filter mechanism in the Filters pane to define a set of criteria by which Release Control determines which change requests to display in Change Requests mode or which action items to display in Action Items mode.

If you are working in Change Request mode, you can:

- Search for a specific change request by entering the request's ID number in the search box in the top right corner of the page and clicking the **Find** button. For a list of regular expressions that can be used, see Regular Expressions.
- Select a change request filter. Release Control displays the change requests that meet the criteria of the change request filter you selected.

If you are working in the Action Item mode, you can:

- Search for a specific action item by entering the action item's ID number in the search box in the top right corner of the page and clicking the **Find** button. For a list of regular expressions that can be used, see Regular Expressions.
- Select an action item filter. Release Control displays the action items that meet the criteria of the change request filter you selected.

> **Note:** The action item filter is not applied to the Action Items view in the Collaborate tab. If you are working with the Change Requests pane, this view displays all the action items associated with the selected change request. If you working with the Action Items pane, this view displays all the action items associated with the change request with which the selected action item is associated.

Using Filters in the Director Module

You use the filter mechanism at the top of the Director module to define a set of criteria by which Release Control determines which activities to display in the Director module.

The filter mechanism in the Director module works in the same way as the filter mechanism in the Analysis module and you can use filters created in the Analysis module to filter activities in the Director module. However, some of the filter criteria that are only relevant to the Analysis module are not included in the Director module and vice versa.

For example, time-related criteria, which are only relevant to the Analysis module are not included in Director module. If a filter was created in the Analysis module with time-related criteria, the filter can still be used in the Director module. However, you are not able to edit time-related criteria in the Director module.

Regular Expressions

In certain filter and search fields, you can use regular expressions to refine your search or filter. In these fields, you can use the following regular expressions:

- **OR or a comma (,).** This creates a logical OR between the predicates. For example, if you enter **david OR steve**, both **david** and **steve** are included in the filter. Similarly, if you enter **steve, da***, both **steve** and any string that begins with **da** are included in the filter.
- **NOT.** By entering `NOT` at the beginning of the expression, a logical NOT is created for the whole expression. The NOT refers to the entire logical condition, regardless of whether it contains one predicate or more. Parentheses should not be specified. For example, if you enter **NOT a***, all strings that do not begin with the letter **a** are included in the filter. Similarly, if you enter **NOT da*, steve**, all strings that do not begin with the letters **da** and are not **steve** is included in the filter.

An asterisk (*) indicates any number of zero or more characters. A question mark (?) indicates any single character.

Tasks

Create a Union Filter

In your next Change Advisory Board meeting, you are going to discuss change requests that are scheduled to be implemented during the first week in June 2009 that are high risk, collide critically with other requests, or have been voted on prior to the CAB.

This task describes how to create a union filter that displays the change requests whose criteria meet these conditions.

Step 1: Define a new filter

Select **Module** > **Analysis** > **Change Request**. In the Filters pane, click the downward arrow to the right of the **New** button and select **New**. Define a new filter called **Next CAB Meeting**. In the **Time** tab, select the first week in June under **Planned within**. For more information on how to define a filter, see Activity/Change Request Filter Dialog Box.

Step 2: Combine the next CAB meeting filter with existing filters

In the **Union Filters** tab, select the **Critical collisions**, **High risk**, and **Voted to CAB** filters that were previously defined in Release Control. For more information on the **Union Filters** tab, see Activity/Change Request Filter Dialog Box.

Step 3: Results

When you select the **Next CAB Meeting** filter, Release Control displays all the change requests that are scheduled for the first week in June 2009 and meet any one of the following criteria:

- Risk = high
- Collision severity = critical
- Contain votes to CAB

Reference

Filtering User Interface

This section describes:

- Activity/Change Request Filter Dialog Box
- Available Filters Dialog Box
- <Criteria> Values Dialog Box
- Filters Pane
- Filters Selection List
- Save Filter Dialog Box

Activity/Change Request Filter Dialog Box

This dialog box enables you to create a new change request or activity filter. You can create a new filter in either the Analysis module or the Director module.

You filter activities according to different criteria. These criteria are divided into predefined filter categories. You can also combine the results of the current filter with other existing filters in the **Union Filters** tab.

To access	• In the Director module: Select **Module** > **Director** > **Control**. In the Activities Timeline pane, click the downward arrow to the right of the **New** button and select **New** or **Edit**. • In the Analysis module: Select **Module** > **Analysis** > **Change Requests**. In the Filters pane, click the downward arrow to the right of the **New** button and select **New** or **Edit**.
Important Information	• Release Control applies all defined criteria to a filter (using the AND operator). For example, if you defined a filter with **Priority** set to **High** and **Impact Severity** set to **Critical**, you only see results that meet both these criteria (**Priority: High** and **Impact Severity: Critical**). • The Release Control administrator can remove some of the pre-defined filter criteria. Some of the criteria listed in the description of the **General**, **Analysis Data**, **Business CIs**, and **Union Filters** tabs, therefore, may not be available. • The Release Control administrator can create additional customized filters, in which case additional filter categories are available in the Activity/Change Request Filter dialog box. For details on creating customized filters, see Fields Pane. • Some filter criteria may be included in one module and not in another. If a filter was created in one module with criteria that are only relevant to that module, the filter can still be used in the other module but with some limitations For example, time-related criteria, which are only relevant to the Analysis module are not included in Director module. If a filter was created in the Analysis module with time-related criteria, the filter can still be used in the Director module. However, you cannot edit time-related criteria in the Director module.
Relevant tasks	Create a Union Filter
See also	Change Request and Activity Filter Overview

User interface elements are described below:

UI Elements (A-Z)	Description
	Clear. Clear all the selected filter properties.
	Save As. Save your filter settings. Opens the Save Filter dialog box.
View	**View Filtered Results.** View the filter results in the Activity Timeline pane without saving the filter.

General Tab

This tab contains filter criteria which are based on fields that originate in the service desk application.

The following user interface elements are included when you create a filter for change requests and activities:

UI Elements (A-Z)	Description
Category	Filters change requests according to category.
Change type	Filters activities according to their request type. The following options are available: • **Planned.** Displays regular change requests scheduled in Release Control. • **Latent.** (Available if the latent change feature is configured). Displays change requests detected by Universal CMDB. For more information, see Detected and Latent Changes. • **Surrogate.** Displays change requests automatically created by Release Control to represent a change request existing in the service desk application that has not yet been retrieved by Release Control. • **Automated.** Displays changes that originate from Network Automation or Server Automation.
Contact person	Filters change requests according to the contact people responsible for the change requests. For a list of the regular expressions that can be used, see Regular Expressions.
Detection status	Filters change requests according to the way in which they were detected. The following options are available: • **Not detected.** Displays regular change requests scheduled in Release Control. • **Detected.** Displays latent changes, or change requests that contain detected changes. For more information, see Detected and Latent Changes. **Note:** Relevant to Analysis module only. Available only if the **Latent** change feature is configured.
Emergency	Filters change requests as follows: • **True.** Change requests that were handled in an emergency procedure. • **False.** Change requests that were not handled in an emergency procedure.
Hierarchy level	Filters activities according to their hierarchical structure. The following options are available: • **Change.** Displays only top-level change requests.

UI Elements (A-Z)	Description
	• **Task.** Displays only second-level change requests. **Notes:** • If you selected the **Hierarchy Level** option in versions previous to 5.0, the filter displays only top-level change requests. • The names of the top-level and second-level requests are configurable in the **enumeration-labels.properties** file in the Labels and Terms pane. For details, see Labels and Terms Pane.
Implementors	Filters change requests according to their implementors. To select an implementor, you can either type the name of the implementor in the box or you can click the **Select From List** button and select an implementor from the dialog box that opens. For a list of the regular expressions that can be used, see Regular Expressions.
Service desk	Filters change requests according to the service desk applications from which they originated. You can select one or more of the listed service desk applications.
Status	Filters change requests according to their statuses. You can select one or more of the listed statuses. The status is determined in the service desk application.
Subcategory	Filters change requests according to subcategory.

Analysis Data Tab

This tab describes the filter criteria, which are based on the calculations that Release Control performs during the processing of change requests.

User interface elements are described below:

UI Elements (A-Z)	Description
Calculated risk	Filters change requests according to their risk analysis levels. The risk analysis level is a number from 0-100 that indicates the risk level of this change request relative to the other change requests. A higher number indicates a higher risk level. Enter or select a range using the boxes provided. For more information about the calculation of risk levels, see Risk Analysis.

UI Elements (A-Z)	Description
CIs	Filters change requests according to the CIs affected by each change request based on the impact analysis calculation. To select CIs, you can either type the names of the CIs in the box or you can click the **Select Values** button to open the Select Values dialog box. For a list of the regular expressions that can be used, see Regular Expressions. To select CIs using the Select Values dialog box, select the relevant CIs in the **Available Values** list, double-click them or click the top arrow to move them to the **Selected Values** list and click **OK**. To deselect a CI, select the CI in the **Selected Values** list and click the bottom arrow. **Note:** If you use the NOT regular expression, the filter excludes all change requests that contain only the specified CI and no other CIs. However, if a change request also includes other CIs besides the one you specified, that change request is still displayed in the results.
Collision severity	Filters change requests according to their collision severity levels. You can select one or more of the listed collision severity levels. Collision severity is calculated by Release Control. For more information about collision severity, see Change Request Collisions.
Collision type	Filters change requests according to the types or causes of the collisions. You can select one or more of the listed collision causes. For more information about collision causes, see Change Request Collisions. **Notes:** • If you defined a custom collision cause, you can select the name of the field you specified as a collision cause. • Relevant to the Analysis module only.

UI Elements (A-Z)	Description
Discussion created	Filters change requests according to the time at which request discussion threads and comments were added. **Note:** Relevant for the Analysis module only.
Impact severity	Filters change requests according to their impact severity levels. You can select one or more of the listed impact severity levels. Impact severity is calculated by Release Control. For more information about impact severity, see Impact Analysis. **Note:** You cannot filter by impact severity level if you selected **Requests with unknown impact** in the **Business CIs** tab.
Time period conflicts	Filters change requests according to the time period categories whose recurrence rules the requests breach. You can select one or more of the listed time period categories. For more information on time period categories, see Time Period Configuration. **Note:** Relevant to the Analysis module only. When you view the filtered change requests in the Timeline and Calendar views, the time period categories you selected in the Change Requests Filter are automatically displayed.
Voted as	Filters change requests according to the user votes they received. You can select one or more of the listed voting options. Users can express their opinion about a change request by posting a vote (**Disagree**, **To CAB**, **Agree**, **No vote**) regarding the request. For more information on change request voting, see Collaborate > Discussion Tab. **Note:** Relevant for the Analysis module only.

Action Items Tab

This tab filters change requests according to the action items associated with them.

- If you are in the Change Request pane and create a filter using action item fields, the Change Request pane displays all the change requests whose associated action items meet the criteria from action items defined in the filter. For example, all change requests that have an associated action item whose status is defined as **Open**.
- If you are in the Action Item pane, the Action Items pane displays all action items that meet the criteria from both action item and change request fields defined in the filter.

User interface elements are described below:

UI Elements (A-Z)	Description
Action Item Assignee	Filters action items according to the user to whom they were assigned. You can either enter the name of the assignee in the text box provided or click the **Select From List** button to the right of the text box to locate and select the assignee in the Select Users dialog box.
Action Item Creator	Filters action items according to the user who created them. You can either enter the name of the creator in the text box provided or click the **Select From List** button to the right of the text box in order to locate and select the creator in the Select Users dialog box.
Action Item Due Date	Filters action items according to the day by which the creator determined that the action item must be completed.
Action Item Last Modified	Filters action items according to the date (including the day and hour) on which the action item was last modified.
Action Item Pending on	Filters action items according to the user whose action is being awaited. You can either enter the name of a user in the text box provided or click the **Select From List** button to the right of the text box in order to locate and select a user in the Select User dialog box.
Action Item Priority	Filters action items according to their priority levels. You can select one or more of the listed priority levels. The priority levels are determined in the service desk application.
Action Item Status	Filters action items according to their statuses. You can select one or more of the listed statuses. The status is determined in the service desk application.

Business CIs Tab

This tab filters change requests according to impact.

User interface elements are described below:

UI Elements (A-Z)	Description
	Show/Hide Obsolete. Toggles between hiding and displaying the obsolete CIs. **Note:**Available only when you select the **Requests affecting selected business CIs** option.
	Find. Search for a specific business CI by entering the name or part of a name in the search box. The search returns all business CIs that contain the entered string somewhere in the name. Click the **Find** button to run the search.
	Move the selected business CIs from the **Available Business CIs** list to the **Selected Business CIs** list. The business CI is included in the filter.
	Move the selected business CIs from the **Selected Business CIs** list to the **Available Business CIs** list. The business CI is not included in the filter.
<View other pages>	To view other pages, use the left and right arrows. The number between the left and right arrows indicate which page is currently being displayed. For example, 3 of 5 means that the 3rd page out of 5 is being displayed. Page 3 of 5
All requests	Displays all change requests.
Available Business CIs	The list of available business CIs. **Notes:** • Available only when you select the **Requests affecting selected business CIs** option. • You can select multiple business CIs using the **Ctrl** key.
Requests affecting any business CI	Displays change requests whose impact analysis results affect any business CI.
Requests affecting my business CIs	Displays change requests whose impact analysis results affect the business CIs associated with you.
Requests affecting selected business CIs	Select the change requests whose impact analysis results affect the business CIs associated with you.
Requests with unknown impact	Displays only change requests for which there are no impact analysis results.
Selected Business CIs	Displays the business CIs you want to include in the filter.

UI Elements (A-Z)	Description
	Notes: • Available only when you select the **Requests affecting selected business CIs** option. • You can select multiple business CIs using the **Ctrl** key.

Time Tab

This tab filters change requests according to time-related criteria by selecting one or more of the time-related options.

From the box adjacent to each filter criterion that you selected, select the desired option from the drop-down list.

If you selected **After**, **Before**, or **Between**, click the calendar button and select a date and time.

> **Note:** You select time intervals according to your machine's time zone, as indicated in the calendar box.

Important Information	This tab is only available in the Analysis module.

The following user interface elements are included when you create a filter for change requests and activities:

UI Elements (A-Z)	Description
Actual end	Filters change requests according to their actual execution end time.
Actual start	Filters change requests according to their actual execution start time.
Created	Filters change requests according to the time at which they were created.
Implemented within	Filters change requests according to the time range in which they were implemented. Any part of the actual implementation that falls within this time range is included in the filter.
Last update	Filters change requests according to the time at which they were last updated.
Planned end	Filters change requests according to their planned execution end time.
Planned start	Filters change requests according to their planned execution start time.
Planned within	Filters change requests according to the time range in which they were scheduled to take place. Any part of the planned execution that falls within this time range is included in the filter.

UI Elements (A-Z)	Description
Requested end date	Filters change requests according to the date by which the implementation of the change request must be completed.
Scheduled downtime end	Filters change requests according to when their downtime is scheduled to end.
Scheduled downtime start	Filters change requests according to when their downtime is scheduled to start.

The following user interface elements are included when you create a filter for action items:

UI Elements (A-Z)	Description
Due date	Filters actions items according to the date by which they must be completed.
Modified	Filters actions items according to the time at which they were modified.

Review Tab

This tab filters requests according to review-related criteria.

Important Information	This tab is only available in the Analysis module.

User interface elements are described below:

UI Elements (A-Z)	Description
Customer satisfaction	Filters change requests according to the customer satisfaction rating they were assigned by change reviewers. You can select one or more of the listed ratings.
Disrupted Business CIs	Filters change requests according to the business CIs that were negatively affected by their implementation. You can select one or more business CIs (using the **Ctrl** key) from the **Available Business CIs** list and click the top arrow to move the selected business CIs to the **Selected Business CIs** list.
Outcome	Filters change requests according to the outcomes they have been assigned by change reviewers. You can select one or more of the listed outcomes.
Planning satisfaction	Filters change requests according to the planning satisfaction rating they were assigned by change reviewers. You can select one or more of the listed ratings.
Reviewed	Filters change requests according to the time at which they were reviewed.

UI Elements (A-Z)	Description
	You define the review time interval by choosing the desired option from the selection box drop-down list. If you select **After**, **Before**, or **Between**, click the calendar button to open the calendar box, select a month using the left and right arrows next to the month name, select a date from the calendar, enter or select an exact hour in the time box, and click **OK**. **Note:** You select the time interval according to your machine's time zone, as indicated in the calendar box.

Union Filters Tab

This tab enables you to select an existing filter whose criteria you want to combine with the filter you are currently defining.

Note: You can select multiple filters using the Ctrl key.

Important Information	A union filter uses the **A AND** (**BOR C OR D OR**...) operator, where **A** is the current filter and **B**, **C**, and **D**... are existing Release Control filters. For an example, see How to Create a Union Filter. **Notes:** • The Favorites filter and filters containing union filters do not appear in the Available Filters list and therefore cannot be combined as union filters with the current filter you are defining. • If you chose to combine private filters with the filter you are currently defining, you can save the current filter only as a private filter. • You cannot combine filters that were defined by an administrator as time period filters with filters that were not defined as time period filters.

User interface elements are described below:

UI Elements (A-Z)	Description
	Move the selected filters from the **Available Filters** list to the **Selected Filters** list. The selected filters are combined with the filter you are currently defining.
	Move the selected filters from the **Selected Filters** list to the **Available Filters** list. The selected filters are not combined with the filter you are currently defining.

UI Elements (A-Z)	Description
Available Filters	The existing filters.
Selected Filters	Select the filter whose results you want to combine with the current filter.

Available Filters Dialog Box

This dialog box enables you to add, edit or delete categories in the Analysis and the Director modules.

To access	• **In the Director module:** Select **Module** > **Director** > **Control**. In the Activities Timeline pane, click the downward arrow to the right of the **Activities** box and select **Organize**. • **In the Analysis module:** Select **Module** > **Analysis** > **Change Requests**. In the Filters pane, click the downward arrow to the right of the **New** button and select **Organize**.
Important Information	• Relevant to the Analysis and Director modules. • If the default filter does not appear in the Available Filters dialog box, for example, if it was deleted, Release Control opens with the following filter: **Unsaved Filter(All)**. The Action Items filter always opens with **Unsaved Filter(All)** filter.
Relevant tasks	Create a Union Filter
See also	Change Request and Activity Filter Overview

User interface elements are described below:

UI Elements (A-Z)	Description
	Remove Filter. Enables you to delete a filter. **Notes:** • You can delete all filters in the Available Filters dialog box except the **Favorite RFCs** and **Favorite AIs** filters. • You cannot delete a filter if it is a time period filter that has been used in defining a time period category, or a filter that is being used as a union filter within another filter. • You can use multiple selection to delete several filters at once using the CTRL key.

UI Elements (A-Z)	Description
	Add Category. Enables you to add a category. **Note**: You cannot place a new category under another category.
	Edit Category. Enables you to edit a category.
	Remove Category. Enables you to delete a category. **Notes:** • You can delete all categories in the Available Filters dialog box except the **My Filters** category. • You can only delete a category if it is empty. • You can use multiple selection to delete several categories at once using the CTRL key.
	Refresh. Updates the Available Filters list. **Note:** If you add, edit, or delete a category or filter in the Available Filters dialog box in the Analysis module, and you want to see the updated Available Filters list in the Available Filters dialog box in the Director module, click the **Refresh** button in the Available Filters dialog box.

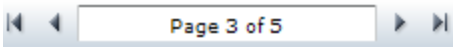
<Criteria> Values Dialog Box

This dialog box enables you to select additional criteria values with which to create a new filter.

To access	Select **Module** > **Analysis** > **Change Requests**. In the Filters pane, click the downward arrow to the right of the required quick filter field and click **More**.
Important Information	Only relevant to the Analysis Module.
See also	Change Request and Activity Filter Overview

User interface elements are described below:

UI Elements (A-Z)	Description
	Enter the name or part of a name of a criteria value for which to search and then click the **Find** button.

UI Elements (A-Z)	Description
	Move the selected values from the **Available Values** list to the **Selected Values** list. The values that are moved to **Selected Values** list are used to create the filter.
	Move the selected values from the **Selected Values** list to the **Available Values** list. The values that are moved to **Available Values** list are not used to create the filter.
<View other pages>	To view other pages, use the left and right arrows. The number between the left and right arrows indicate which page is currently being displayed. For example, 3 of 5 means that the 3rd page out of 5 is being displayed. 

Filters Pane

This pane enables you to:

- Select a filter that determines which change requests appear in the Change Requests pane.
- Define new filters and edit existing ones. Any filter that you create or edit in the Filters pane appear in the Filter Selection list in the Action Items pane and Director module as well.
- Add, edit, or delete categories in the Analysis and the Director modules.
- Use the Quick Filter fields to display commonly required information in the Change Requests pane.

To access	Select **Module** > **Analysis** > **Change Requests** > **Filters** pane.
Important Information	The Filters pane appears only in the Change Request pane in the Analysis module.
Relevant tasks	Create a Union Filter
See also	Change Request and Activity Filter Overview

User interface elements are described below:

UI Elements (A-Z)	Description
	Select Filter. Select the filter that determines: The activities to be displayed in the Director module The change requests to be displayed in the Change Request pane The action items to be displayed in the Action Items pane

UI Elements (A-Z)	Description
	Opens the Filters Selection List.
	Back\Forward. Enables you to go back and forth to the previous filter, view, and selected change request.
	Reset to the last selected filter. Returns the filter to its previously saved filter settings.
	Save as. Copy any filter except the **Favorites** filter by saving it under a different name or with different access (private/public) properties. Opens the Save Filter Dialog Box. For example, if you are a user without administrative privileges and want to modify one of the public filters, you can rename the public filter so that it is saved as one of your personal filters and then modify the filter's properties. **Notes:** • You cannot modify the properties of the automatically generated **Favorites** filter. • Only an administrator can modify the properties of the public filters. • If the modified filter is a time period filter and is included in time period categories, Release Control recalculates the compliance of the change requests that fit the configured categories with the rules pertaining to these categories.
	Edit filter. Contains the following options: • **New.** Defines a new filter. Opens the Activity/Change Request Filter Dialog Box. • **Edit.** Edits an existing filter. Opens the Activity/Change Request Filter Dialog Box. • **Organize.** Enables you to add, edit or delete categories in the Analysis and the Director modules. Opens the Available Filters Dialog Box.
<Default quick filter fields>	Enables you to predefine fields to display commonly required information. • Administrators can define default Quick Filter fields in the Administrator module. Select **Administrator** > **Configuration** tab > **Fields**. In the Available fields pane, click the **Manage Quick Filter Display** button to open the Quick Filter Display dialog box. For details, see the Quick Filter Display pane in the Quick Filter Display Pane. • Users with non-administrator privileges can define default Quick

UI Elements (A-Z)	Description
	Filter fields. For details, see Quick Filter Display Pane. The Quick Filter fields defined in the User Preferences dialog box apply to the specific user only and override the fields defined by the administrator in the Administrator module. To modify filter results, click the downward arrow to the right of each field and do the following: • Select the required filter values. For details, see Available Filters Dialog Box. • Click **More** to select additional criteria values. Opens the <Criteria> Values Dialog Box. • Click **Clear** to clear the values selected for the filter criteria. **Note:** Release Control applies all defined criteria to a filter (using the AND operator). For example, if you defined a filter with Priority set to High and Impact Severity set to Critical, you will only see results that meet both these criteria (Priority: High and Impact Severity: Critical). You can view the filter results without saving the filter, or alternatively, save the new filter using the **Save** button to open the Save Filter Dialog Box.

Filters Selection List

The Filter Selection list enables you to select the filter that defines the criteria which determines the activities to be displayed in the Activity Timeline pane in the Director module and in the Change Request/Action Item pane in the Analysis module.

To access	• **In the Director module:** Select **Module** > **Director** > **Control**. In the Activities Timeline pane, click the downward arrow to the right of the **Activities** box. • **In the Change Requests pane:** Select **Module** > **Analysis** > **Change Requests**. In the Filters pane, click the downward arrow to the right of the **Select Filter** button. • **In the Action Items pane:** Select **Module** > **Analysis** > **Actions Items**. Click the downward arrow to the right of the **Filters** box.

Relevant tasks	Create a Union Filter
See also	Change Request and Activity Filter Overview

User interface elements are described below:

UI Elements (A-Z)	Description
	Denotes a filter.
	Denotes a union filter. For details, see Union Filters Tab.
My Filters category	Displays the filters that are saved to the **My Filters** category. These filters are not viewed by any other user. For details, see the Save Filter Dialog Box.
Public Filters category	Displays the filters that are saved to the **Public Filters** category by selecting the **Public Filters** option in the Save Filter dialog box. **Notes:** • Filters that appear under the **Public Filters** category can be viewed by all users. • If you have not been assigned the administrator role, the filter appears under the **My Filters** category.
Time Period Filters	Displays the filters that are saved to the **TIme Period Filters** category by selecting the **Time Period Filter** option in the Save Filter dialog box.

Save Filter Dialog Box

This dialog box enables you to save your filter settings and display the filter results in the Change Request pane in the Analysis module and in the Activity Timeline pane in the Director module.

> **Note:** If the saved filter is a time period filter and is included in time period categories, Release Control recalculates the compliance of the change requests that fit the configured categories with the rules pertaining to these categories.

To access	• In the Activity/Change Request Filter dialog box, click **Save** . • In the Filters pane, click **Save as**.
Important Information	• When you save a **Public Filter** or **Time Period Filter**, you must save it to a specified category (select a category from the **Category** drop-down list). • Once you have saved the filter, it appears in one of the following

	categories in the **Filters Selection** list: ○ **My Filters** ○ **Public Filters**(if the **Public filter** check box was selected) ○ **Time Period Filters** (if the **Time Period Filter** check box was selected)
Relevant tasks	Create a Union Filter
See also	Change Request and Activity Filter Overview

User interface elements are described below:

UI Elements (A-Z)	Description
Category	When you save a **Public Filter** or **Time Period Filter**, you must save it to a specified category (select a category from the **Category** drop-down list).
Description	Enter a description for the filter.
Name	Enter the name of the filter. > **Note:** You cannot use a a question mark (?) or the ampersand character (&) in the filter name.
Public Filter	If you are assigned the Administrator or Change Manager role, you can select the **Public Filter** check box to enable the filter you are creating to be viewed by all users. > **Note:** If you are a regular user, the filter appears under **My Filters** in the filter selection list. If you are an administrator and selected the **Public filter** check box, the filter appears under **Public Filters** in the filter selection list.
Time Period Filter	If you are an administrator and want to be able to define a time period category based on the filter you are creating, select the **Time Period Filter** check box. The filter then appears in the Select Filter dialog box and you can select this filter when defining a time period category in the Administrator module's **Time Periods**tab. For details on defining time periods, see Time Periods Tab. > **Note:** The Time period filter check box cannot be selected in the following cases: > • If the **Time Period Conflicts** option is selected in the **Analysis Data** tab > • If the **Requests affecting my business CI** option is selected in the **Business CIs** tab

UI Elements (A-Z)	Description
	• If options other than **Before**, **After**, or **Between** are selected in the **Time** tab

Part IV: Monitoring and Implementing Activities

Director Module

> **Note:** This chapter is intended for NOC Users. That is, most of the actions described require NOC privileges.

This chapter includes:

Concepts

- Director Module Overview
- Viewing Activities on the Timeline
- Activity Alerts
- User Communication

Tasks

- Monitor the Implementation Progress of an Activity

Reference

- Director Module User Interface

Concepts

Director Module Overview

The Director module enables you to monitor the status of change requests scheduled for implementation.

All users can view the Director module. If you are a **NOC user** (users who are assigned the NOC role), you can perform actions in this module. If you do not have NOC privileges, for example, a Release Manager or Change Manager, you can use this module to communicate with other users about change requests that interest you.

During the implementation stage, change requests are referred to as **activities**. In the Director module, you can observe events surrounding the activities, such as updates to the status of activities, problems

that occur during implementation, and so on. If problems arise, you can take immediate action, ensuring that implementation runs as efficiently and with as little impact on the production environment as possible.

For an example of how to monitor the implementation progress of an activity and how to handle the problems that may arise during the implementation, see Monitor the Implementation Progress of an Activity.

Viewing Activities on the Timeline

The Activity Timeline pane lists activities scheduled within a selected time range and their schedules are displayed graphically on a timeline. For details, see Activity Timeline Pane.

The graphical representation of an activity schedule indicates the status of the activity. If an activity's schedule is modified, this is indicated on the timeline. For details, see Representation of Activities on the Timeline below.

The timeline area is divided into a shaded area representing time in the past, and a non-shaded area representing time in the future. The vertical line dividing the past and future represents the current time. By default, the table displays activities scheduled up to 12 hours behind the current time and 12 hours ahead of the current time. You can change the time interval displayed on the timeline. For details, see Modifying the Time Display of the Timeline.

You can filter the activities to view only those with certain criteria. For details, see Filtering Change Requests and Activities.

This section also includes:

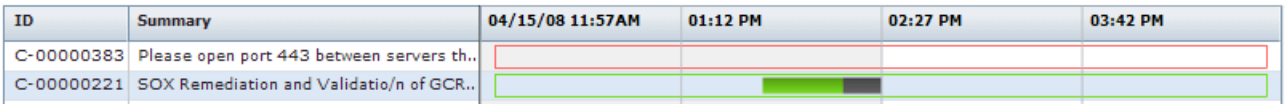
- Representation of Activities on the Timeline
- Modifying the Time Display of the Timeline

Representation of Activities on the Timeline

The timeline displays activities in such a way that the you can immediately identify an activity's planned schedule and the current status of the activity.

The **planned schedule** of an activity is represented by an empty horizontal bar, while the **actual implementation** period is represented by a solid bar.

For example, in the following image, the planned schedule for Activity C00000221 is represented by an empty bar. The solid bar represents the actual implementation time. You can see that the implementation of the activity started at about 01:30 PM.



Downtime for an activity is indicated on the timeline by a solid, dark gray bar. In the above example, downtime was started at about 02:15 PM.

The color of an activity on the timeline is determined by whether or not there are alerts for the activity, or if it has finished implementation.

- If there are no alerts for the activity, the activity is displayed in green.
- If there are alerts for the activity, the activity is displayed in red, yellow, or blue, according to the alert for the activity with the highest severity. For more information about activity alerts, see Activity Alerts.
- If the implementation of an activity is complete, the activity is displayed in gray.

Modifying the Time Display of the Timeline

The timeline is divided into four equal parts where, by default, half of the time displayed is in the past, represented by a shaded area, and half of the time is in the future, represented by the non-shaded area. The current time is represented by the vertical line separating the past and the future.

You can modify the time range displayed on the timeline, and the time amount of past/future time displayed. For details, see Activity Timeline Pane.

Activity Alerts

The Alerts pane of the Director module displays alerts about activities displayed on the timeline. These alerts notify you about problems detected regarding the listed activities, prompting you to take action where necessary. For details, see Alerts Pane.

Alerts can indicate errors or warnings, or can simply be informative. They are generated under any of the following circumstances:

- An activity started earlier than scheduled
- An activity is likely to start late or started late
- An activity is likely to end late or ended late
- An activity breached a Time Period without approval from the Change Advisory Board (CAB)
- An activity has pre- or post-implementation guidelines

- An activity is likely to collide or collides with another activity without approval from the CAB
- An implementer is calling for assistance
- An emergency activity was added
- An activity's details were modified

User Communication

You can communicate with other users to convey or obtain information regarding the common activities with which you are associated, or regarding other topics through the Communications pane. For details, see Communications Pane.

Tasks

Monitor the Implementation Progress of an Activity

This task describes how to monitor the implementation progress of an activity and how to handle the problems that may arise during the implementation.

Step 1: Check the Activity for alerts

As the NOC Change Manager for your company, you are responsible for monitoring the implementation progress for the deployment of a new webmail server.

In the Activity Timeline pane, you select the activity on which you are working. In the Alerts pane, there is an alert notifying you that the activity has started late. As a result, the activity is scheduled to collide with another activity without the approval of the CAB. For details about the Alerts pane, see Alerts Pane.

Step 2: Understand why an Activity is delayed

You want to understand why the activity is not starting on time. So you communicate with the implementor in charge of the activity by opening a chat room in the Communications pane to obtain information regarding the reasons for the delay. For details about the Communications pane, see User Communication.

Step 3: Reschedule an Activity to avoid collisions

To avoid a collision with another activity, you decide to reschedule an activity to end earlier than the original CAB planned schedule. You click **Reschedule Activity** in the Activity Timeline pane to open the Reschedule Activity dialog box. For details, see Reschedule Activity Dialog Box.

Reference

Director Module User Interface

This section describes:

- Activity Information Dialog Box
- Activity Timeline Pane
- Alerts Pane
- CI Attributes Dialog Box
- Communications Pane
- Director Module Window
- Handle Alerts Dialog Box
- Notes for Activity <ID> Dialog Box
- Reschedule Activity Dialog Box
- Update Activity Status Dialog Box

Activity Information Dialog Box

This dialog box enables you to view information about each activity. The information provided comprises all the details about the activity. It also displays pre- or post-implementation guidelines, and any events related to the activity, for example, if the activity was rescheduled, if the status was updated, and so on.

To access	• **In the Director Module:** Select **Module** > **Director** > **Control**. Select the required activity in either the Activity Timeline pane or the Alerts pane, and click **Activity Information**. • **In the Implementor Module:** Select **Module** > **Director** >

	Implementor. Select the required activity in the To-Do List pane, and click **Activity Information** .
Relevant tasks	Monitor the Implementation Progress of an Activity
See also	• Review Tab • Alerts Pane

User interface elements are described below:

UI Elements (A-Z)	Description
View in Analysis	View the activity in the Analysis module.

Details Tab

This tab displays details about the selected activity.

User interface elements are described below:

UI Elements (A-Z)	Description
Actual End	The date and time at which implementation of the activity actually ended.
Actual Start	The date and time at which implementation of the activity actually started.
Change Type	The type of change (for example, planned or automated).
Contact Location	The geographic location of the person responsible for the activity.
Contact Person	The name of the user responsible for the activity.
Created	The date and time at which the activity was originally created in the service desk application.
Description	A description of the activity.
Estimated Risk	The estimated risk level that was assigned to the activity by a user.
Impact Severity	The impact severity level of the activity, as calculated by Release Control.
Implementors	The people responsible for implementing the activity.
Last Impact	The time at which an impact analysis was last calculated.
Last Update	The last time the activity was updated in the service desk application.
NOC Planned End	The date and time that the activity implementation is scheduled to end, as rescheduled by the NOC users.

UI Elements (A-Z)	Description
NOC Planned Start	The date and time that the activity implementation is scheduled to start, as rescheduled by the NOC users.
Planned End	The date and time that the activity implementation is scheduled to end.
Planned Start	The date and time that the activity implementation is scheduled to start.
Priority	The priority level of the activity.
Request ID	The reference ID number of the activity in the service desk application.
Risk	A number from 0 – 100 that indicates the risk level of this activity relative to the other activities, as calculated by Release Control.
Service Desk	The service desk application in which the activity originated.

Implementation Guidelines Tab

This tab displays CAB-assigned guidelines to follow before and/or after implementing the activity.

User interface elements are described below:

UI Elements (A-Z)	Description
Post-Implementation	Displays CAB-assigned guidelines to follow after implementing the activity.
Pre-Implementation	Displays CAB-assigned guidelines to follow before implementing the activity.

Event Log Tab

This tab displays events related to activities. These can be user- or system-induced events. For information on what the Event Log displays, see Review > Event Log Tab.

CI KPIs Tab

This tab displays KPIs (Key Performance Indicators) for the CIs impacted by the selected activity.

To access	• Select an activity in the Activity Timeline pane and click **KPIs for Activity CIs**. • Select an activity in the Activity Timeline pane, click **Activity Information**, and select the **CI KPIs** tab.
Important Information	• This feature is only available if Release Control is integrated with Business Availability Center 8.0 or later. • To view the CI KPIs, Business Availability Center needs to be running.

See also	• For information about configuring this feature, refer to Monitoring Pane. • To submit information or comments about an activity, see Notes for Activity <ID> Dialog Box. • To view additional layers of information on the timeline, see Activity Timeline Pane.

User interface elements are described below:

UI Elements (A-Z)	Description
Impact CIs pane	Displays the business and system CIs that are affected by the change request. • . Release Control automatically refreshes the list of impact CIs every minute. Click **Refresh Activity Timeline** any time to refresh the display. • . Displays the attributes of the selected CI. Opens the CI Attributes dialog box. • **<List of impact CIs>**. The list of business and system CIs that are affected by the change request. When you select one of the CIs in the Impact CIs pane, the KPI details are displayed in the **Key Performance Indicators** pane. For a detailed description of the icons in this pane, see Assess > Impact Tab.
Key Performance Indicators pane	Displays the details of the KPIs associated with the CI you select in the Impact CIs pane. • **Name**. The KPI type. • **Source**. The application that provides the KPI information. • **Status**. The status of the KPI. • **Value**. If no status is available, the value of the KPI is displayed. The unit of the value is displayed in parenthesis.

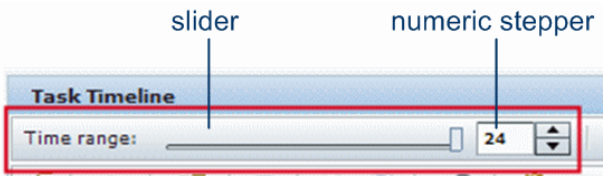
Activity Timeline Pane

This pane lists activities scheduled within a selected time range, and their schedules are displayed graphically on a timeline. The graphical representation of the activity schedules indicates the status of the activity, that is, whether it has not yet started, has started, or is complete, and so on. If you modify an activity's schedule, this is indicated on the timeline.

To access	Select **Module** > **Director** > **Control** > **Activity Timeline** pane.
See also	Viewing Activities on the Timeline

User interface elements are described below:

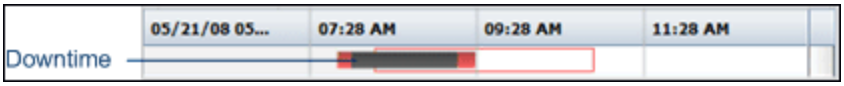
UI Elements (A-Z)	Description
	View Layer. Enables you to view additional information by adding layers of information to the timeline. Select the layer of information you want to display. For information on the available layers of information you can view, see Information Layers in the Activity Timeline Pane.
	Drag mode/Cursor mode. Enables you to modify the amount of past and future time you want displayed in the timeline area. You can toggle between **Drag Mode** and **Cursor Mode**. • Click **Drag Mode** to turn the cursor into a hand when you hold it over the timeline area. Drag the timeline area to the left to display more time in the future, or to the right to display more time in the past. The activities displayed are updated according to the new time range displayed. • Click **Cursor Mode** to revert back to the regular cursor.
	Activity Information. Opens the Activity Information dialog box. Contains details about the selected activity. **Note:** The **Activity Information** button is also available in the Alerts pane.
	Update Activity Status. Opens the Update Activity Status dialog box. Enables you to update the status on the implementor's behalf if the implementor is unable to update the activity status directly.
	Reschedule Activity. Opens the Reschedule Activity dialog box. Enables you to reschedule an activity to start or end earlier or later than the original CAB planned schedule.
	Submit Note to Event Log. Opens the Notes for Activity <ID> dialog box. Enables you to submit information or comments about an activity to the Event Log.
	Open Activity Chat Room. Open a chat room in the Communications pane. For details, see User Communication.
	Refresh Activity Timeline. Release Control automatically refreshes the Activity Timeline pane every minute. At any time, you can click **Refresh Activity Timeline** to refresh the display.

UI Elements (A-Z)	Description
Activities	Define a set of criteria by which to determine the activities to be displayed in the Activity Timeline pane. For details, see User Communication.
ID	The reference ID number of the activity in the service desk application.
Results	The number of activities that are displayed in the Activity Timeline pane.
Summary	A description of the activity.
Time Range	Modify the time range displayed on the timeline.  Drag the **Time Range** slider left or right, or use the numeric stepper to select the number of hours to display. You can select a time range of between 1 and 24 hours. By default, a 24-hour time range is displayed.

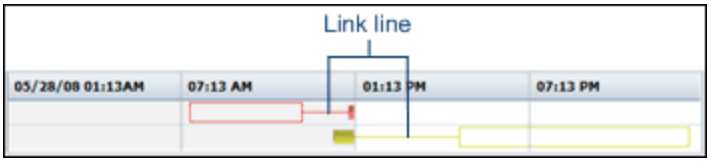
Information Layers in the Activity Timeline Pane

You can view the available layers of information in the timeline—one at a time, or simultaneously.

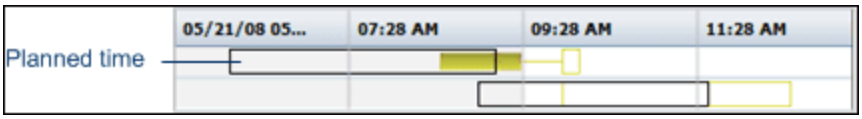
- **Downtime.** Intervals of downtime on CIs during activity implementation. Downtime is represented by a solid, dark gray bar.



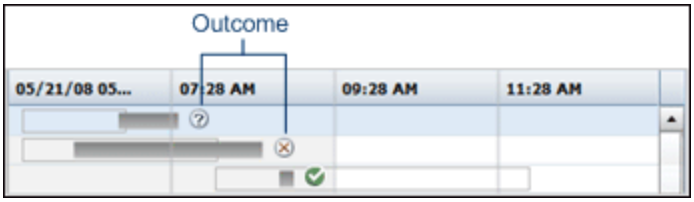
- **Link Line.** When an activity's planned and actual implementation schedules do not overlap, a thin line links the two schedules.



- **Planned Time.** The original implementation schedule for the activity defined by the CAB, represented by an empty bar with a black border.



- **Implementation Outcome.** For activities that have ended, you can view the implementation outcomes on the timeline.



  - **Successful.** Denotes that the implementation is successful.
  - **Successful with problems**. Denotes that the implementation is successful but you encountered some problems.
  - **Failed.** Denotes that the implementation failed.
  - **Cancelled.** Denotes that the implementation is cancelled.

Alerts Pane

This pane displays notifications about problems relating to the activities. Alerts also indicate warnings, or can simply be informative.

To access	Select **Module** > **Director** > **Control** > **Alerts** pane.
Important Information	You must log out and then log on for these configurations to take effect.
See also	Activity Alerts

User interface elements are described below:

UI Elements (A-Z)	Description
	Show Open Alerts Only. Displays only the open alerts. This view hides dismissed alerts and alerts in reminder mode. **Note:** This is the default view.
	Synchronize with Selected Activity. Displays only the alerts associated with a selected activity. **Note:** To view only the open alerts for the activity, click **Show Open Alerts**

UI Elements (A-Z)	Description
	Only .
	Group by Activity. Enables you to group alerts in the Alerts pane by activity. The alerts are grouped by activity, indicated by a bullet adjacent to the alert's icon Time | Description Mon 03:33 PM | T-00000131 (2) Click the bullet to expand the activity's alerts. Click here to see an example. Time | Description Mon 05:04 PM | Alona_3 (2) Mon 05:04 PM | Alona_3 which was planned to start at: Mon 04:30 AM is late to start Mon 05:04 PM | Emergency Alona_3 was inserted Mon 04:59 PM | 2000 (4) Mon 04:59 PM | Collision detected between 2000 and 3000 on Implementor, DAB/DAB Mon 04:58 PM | 2000 which was planned to start at: Mon 07:30 AM has started early Mon 05:11 PM | 2000 has pre-implementation CAB guidelines Mon 03:51 PM | Emergency 2000 was inserted **Note:** To view only the open alerts for the activity, click **Show Open Alerts Only** .
	Activity Information. Contains details about the selected activity. Opens the Activity Information dialog box. **Note:** The **Activity Information** button is also available in the Activity Timeline pane.
Handle	**Handle Alert.** Enables you to determine how to handle an alert when an alert is generated. Opens the Handle Alert dialog box.
	Open Activity Chat Room. Open a chat room in the Communications pane. For details, see User Communication.
	Indicates the alert's severity. The color of the alert icon is determined by the activity's most severe alert. The icon displayed alongside each alert indicates the severity of the alert and the alert's status. An alert icon can be: • Red , indicating an error

UI Elements (A-Z)	Description
	• Yellow , indicating a warning • Blue , indicating a notification Alerts can have one of the following statuses: • **Open** The alert is active. • **Dismissed** The alert was acknowledged and removed from the Alerts pane. • **In reminder mode** The alert is in reminder mode.
Description	The ID of the activity. The number in parentheses next to the activity ID indicates the number of alerts for the activity.
Time	The time at which the alert was generated.

CI Attributes Dialog Box

This dialog box displays the attributes of the selected CI.

To access	• **To access in Analysis Module:** Select **Module** > **Analysis** > **Assess** > **Impact** tab. Then click **CI Attributes** in the Impact CIs pane. • **To access in Director Module:** Select **Module** > **Director** > **Control**. Click **Activity Information** either in the Activity Timeline pane or the Alerts pane to open the Activity Information dialog box. Click the **CI KPIs** tab and then click **CI Attributes** in the Impact CIs pane.
Important Information	To customize the attributes that are displayed, see CIs Display Pane.

User interface elements are described below:

UI Elements (A-Z)	Description
Name	The name of the attribute.
Value	The attribute's value.

Communications Pane

This pane provides a medium where you can communicate with all other users that are involved in a particular activity or are interested in a particular topic. For details, see User Communication.

To access	Select **Module** > **Director** > **Control** > **Communications pane** .
Relevant tasks	Monitor the Implementation Progress of an Activity

Director Module Window

This window enables you to monitor the status of change requests scheduled for implementation.

This window contains the following panes:

- Activity Timeline Pane
- Alerts Pane
- Communications Pane

To access	Select **Module** > **Director** > **Control**.
Relevant tasks	Monitor the Implementation Progress of an Activity
See also	Director Module Overview

Handle Alerts Dialog Box

This dialog box enables you to determine how to handle an alert.

When an alert is generated, you can select how to handle it. You can:

- Request an alert reminder
- Dismiss the alert
- Reopen a dismissed alert or an alert in reminder mode

To access	Select **Module** > **Director** > **Control**. In the Alerts pane, select the required alert and then click **Handle Alert** Handle.

Relevant tasks	Monitor the Implementation Progress of an Activity
See also	Activity Alerts

User interface elements are described below:

UI Elements (A-Z)	Description
Dismiss alert and reopen only if an alert's severity increases	Enables you to dismiss the alert. If the severity of this alert increases, the alert reopens with a higher severity. For example, if an alert is about to collide with another alert, a warning alert (yellow) is generated. If, after you dismiss this alert, the activities do collide, the alert reopens as an error alert (red).
Notes	(Optional) A free text box for any notes you want to associate with the alert.
Remind me again in:	Request an alert reminder. In the drop-down list, select when to activate the reminder.
Reopen alert	Reopen a selected alert that has been dismissed. A regular alert icon appears next to the alert, indicating that it is open. **Note:** To reopen an alert, ensure that **Show Open Alerts Only** is not selected.

Notes for Activity <ID> Dialog Box

This dialog box contains a free text box for any information or comments you want to submit about an activity to the Event Log.

To access	Select **Module** > **Director** > **Control**. In the Activity Timeline pane, select the activity you have comments about and click **Submit Note to Event Log**.
See also	Event Log Tab

User interface elements are described below:

UI Elements (A-Z)	Description
Notes	Notes or information you want to submit about an activity to the Event Log.

Reschedule Activity Dialog Box

This dialog box enables you to reschedule an activity to start or end earlier or later than the original CAB planned schedule.

To access	Select **Module** > **Director** > **Control**. In the Activity Timeline pane, select the required activity and click **Reschedule Activity**.
Important Information	You can reschedule an activity to start up to 12 hours earlier than the original CAB planned start time, and end up to 12 hours later than the original CAB planned end time.
Relevant tasks	Monitor the Implementation Progress of an Activity
See also	Event Log Tab

User interface elements are described below:

UI Elements (A-Z)	Description
	Opens a calendar. Select a new time and date. **Note:** The updated schedule is displayed on the timeline, and the event is logged in the Event Log.
End time	Displays the new end time for the selected activity.
Start time	Displays the new start time for the selected activity.

Update Activity Status Dialog Box

This dialog box enables you to update the status on the implementor's behalf if the implementor is unable to update the activity status directly.

To access	Select **Module** > **Director** > **Control**. In the Activity Timeline pane, select the required activity and click **Update Activity Status**.
Relevant tasks	Monitor the Implementation Progress of an Activity

User interface elements are described below:

UI Elements (A-Z)	Description
Actual end	• Click to select the date and time (current or in the past) that the activity ended. • Click to clear the current status. **Notes:** • You must update **Actual start** before you can update **Actual end**. • If you are fully integrated with Service Manager as your service desk, the **Actual end** field is automatically updated in the originating service desk when you update it in the Director module.
Actual start	• Click to select the date and time (current or in the past) that the activity started. • Click to clear the current status. **Note:** If you are fully integrated with Service Manager as your service desk, the **Actual start** field is automatically updated in the originating service desk when you update it in the Director module.
Downtime end	• Click to select the date and time (current or in the past) that the downtime ended. • Click to clear the current status. **Note:** You must update **Downtime start** before you can update **Downtime end**.
Downtime start	• Click to select the date and time (current or in the past) that the downtime started. • Click to clear the current status. **Notes:** • You must update **Actual start** before you can update **Downtime start**. • If you update **Downtime start**, you must first update **Downtime end** before you can update **Actual end**.

UI Elements (A-Z)	Description
>Notes	(Optional) A free text box for any notes you want to add about the status update.
On behalf of	Select the implementor on whose behalf you want to update the activity status. You can choose the name of the implementor from the drop-down menu or by clicking **Select Implementor** and selecting a name from the list that appears.
Outcome	If you are updating **Actual end**, the Outcome box is enabled. Select one of the following activity outcomes: • **Successful.** Indicates that the activity was successful. • **Successful with Problems.** Indicates that overall the activity was successful, but had some problems. • **Failed.** Indicates that the activity failed. • **Cancelled.** Indicates that the activity was cancelled.

Implementor Module

This chapter includes:

Concepts

- Implementor Module Overview
- Managing Activity Implementation

Tasks

- Modify the Implementation Progress of an Activity

Reference

- Implementor Module User Interface

Concepts

Implementor Module Overview

As an implementor, you can manage the activities assigned to you from the Implementor module. You can view activity information and update the status of activities on which you are working. In turn, the NOC users are notified of the current status of the activity. For details, see To-Do List Pane.

From the Implementor module, you can communicate with other implementors assigned the same activity, as well as with NOC and other users involved in the activity. For details, see User Communication.

Managing Activity Implementation

The Implementor module lists the activities assigned to you over the current 24-hour period, that is, over the last 12 hours and over the next 12 hours, sorted by their scheduled start times.

The current status of each activity is displayed in the To-Do List. As you progress through the implementation, you update the status of the activity. For information on how to update the status of the activity, see To-Do List Pane.

When implementation is complete, you can update the implementation outcome. For information on how to update the implementation outcome, see Report Activity As Finished Dialog Box.

Tasks

Modify the Implementation Progress of an Activity

This task describes how to modify the implementation progress of an activity and how to handle the problems that may arise during the implementation.

This task includes the following steps:

Step 1: View the Activity Information

Step 2: View Event Log Information

Step 3: Update the Status of the Activity

Step 4: Request NOC Assistance

Step 5: Communicate with Other Implementors

Step 6: Report the Start of Server Downtime

Step 7: Report the End of Server Downtime

Step 8: Report the Activity Outcome

Step 1: View the Activity Information

As an implementor for your company, you are responsible for modifying the implementation progress for fixing the email notification problem in the Release Control server.

In the To-Do List, you select the activity on which you are working. You click the **Activity Information** button to open the Activity Information dialog box. You then click the **Implementation Guidelines** tab to view the CAB-assigned guidelines to follow before and after implementing the activity.

Since fixing the email notification problem involves scheduling a period of downtime for the Release Control server, the pre-implementation guidelines require that you notify the relevant people when, and for how long, the server will be down.

The post-implementation guidelines require that you give notification when the relevant people have been informed of the pending downtime.

For details on the Implementation Guidelines tab, see Implementation Guidelines Tab.

Step 2: View Event Log Information

To confirm that downtime of the Release Control server does not impact any other critical applications, you need to review information related to the activity on which you are working.

You review the information in:

- **The Event Log.** You click the Event Log tab in the Activity Information dialog box. For details about Event Log information, see Event Log Tab.
- **The Analysis module.** In the Activity Information dialog box, you click the **View in Analysis** button in the Details tab. For details, For details, see Details Tab.

Step 3: Update the Status of the Activity

Before implementation begins, the activity status is **Not started**. After deciding that you can begin implementation, you update the status of the the activity to **Report Activity as Started**.

In the To-Do list, you select the activity on which you are working and click the **Report the Activity as Started** button. The status of the activity is updated to **Started**.

For more information about activity status, see To-Do List Pane.

Step 4: Request NOC Assistance

While the email notification problem is being worked on, you notice another hardware failure in the server you are working on and begin to investigate. You submit a message to the NOC users requesting their assistance with this problem.

In the To-Do list, you select the activity for which you need assistance. You click the **Request NOC Assistance** button In the To-Do List toolbar to open the NOC Assistance Request dialog box. You enter your request for assistance and click **OK**. The request is sent to the Director module where it is displayed as an alert with high severity.

For more information, see NOC Assistance Request Dialog Box.

Step 5: Communicate with Other Implementors

You are now ready to implement the planned server downtime, but you remember that your colleague

Lauren had been working on the server. So you open an activity chat room to tell her that you need to take the server down.

In the To-Do list, you select the activity about which you want to chat and then click the **Open Activity Chat Room** button in the To-Do List toolbar. A chat room window opens in the Communications pane. You type your message in the box adjacent to the **Send** button, and click **Send**.

For more information about using the activity chat room, see User Communication.

Step 6: Report the Start of Server Downtime

Before you take the server down, you need to update the status of the activity. You select the activity on which you are working and click the **Report Start of Downtime** button in the To-Do List toolbar.

Step 7: Report the End of Server Downtime

When you are ready to restart the server, you select the activity on which you are working and click the **Report End of Downtime** button in the To-Do List toolbar.

Step 8: Report the Activity Outcome

After implementation of the activity has ended, you need to update the activity's status and indicate its outcome. You select the activity on which you are working and click the **Report Activity as finished** button in the To-Do List toolbar. The Report Activity as Finished dialog box opens, in which you select the required activity outcome.

For information about activity outcome options, see Report Activity As Finished Dialog Box.

Reference

Implementor Module User Interface

This section describes:

- Communications Pane
- Implementor Window
- NOC Assistance Request Dialog Box
- Report Activity As Finished Dialog Box
- To-Do List Pane

Communications Pane

This pane provides a medium where you can communicate with all other users that are involved in a particular activity or are interested in a particular topic. For details, see User Communication.

To access	Select **Module** > **Director** > **Implementor** > **Communications pane**.
Relevant tasks	Modify the Implementation Progress of an Activity

Implementor Window

This window lists the activities assigned to you over the current 24-hour period, that is, over the last 12 hours and over the next 12 hours, sorted by their scheduled start times.

You can view activity information and update the status of activities on which you are working. For information on how to update the status of the activity, see To-Do List Pane.

When implementation is complete, you can update the implementation outcome. For details, see Report Activity As Finished Dialog Box.

This window contains the following panes:

- To-Do List Pane
- Communications Pane

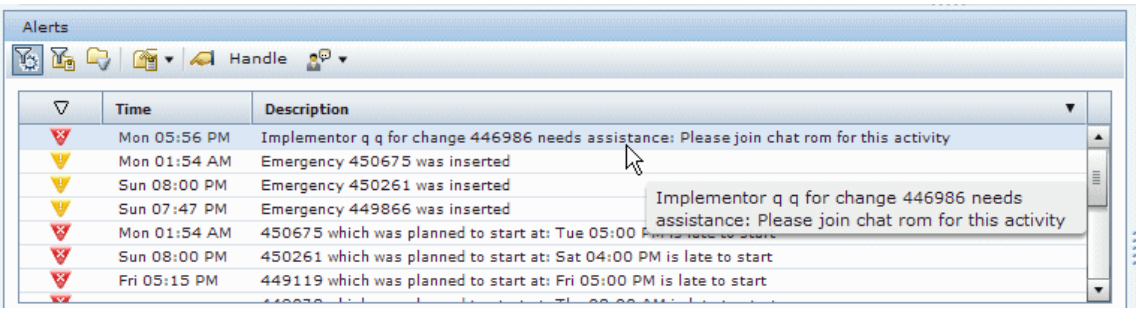
To access	Select **Module** > **Director** > **Implementor**.
Relevant tasks	Modify the Implementation Progress of an Activity
See also	Managing Activity Implementation

User interface elements are described below:

UI Elements (A-Z)	Description
Description	A full length description of the selected change.
Summary	A brief description of the selected change.

NOC Assistance Request Dialog Box

If you are an implementor, this dialog box enables you to submit a message to the NOC users requesting assistance for a certain activity. The message is conveyed in the Director module in the form of a high severity alert noting that you are in need of assistance.



For more information about the Director module, see Director Module.

To access	Select the activity for which you need assistance and then click **Request NOC Assistance** on the To-Do List toolbar.
Relevant tasks	Modify the Implementation Progress of an Activity
See also	Managing Activity Implementation

Report Activity As Finished Dialog Box

This dialog box enables you to select the required implementation outcome in the To-Do List after updating the activity status. For information on how to update the status of the activity, see To-Do List Pane.

The status in the **Status** column changes to **Done**, and the **Outcome** column is updated with the relevant icon. For details on the icons that can appear in the Updated column, see To-Do List Pane.

To access	Click **Report Activity as Finished** from the toolbar in the To-Do List.
Relevant tasks	Modify the Implementation Progress of an Activity
See also	Managing Activity Implementation

User interface elements are described below:

UI Elements (A-Z)	Description
Notes	(Optional) Enter your comments about the outcome of the activity.
Outcome	Select one of the following activity outcomes: • **Successful.** Indicates that the activity was successful. • **Successful with Problems**. Indicates that overall the activity was successful, but had some problems. • **Failed.** Indicates that the activity failed. • **Cancelled**. Indicates that the activity was cancelled.

To-Do List Pane

The To-Do List displays the activities assigned to you over the current 24-hour period, that is, over the last 12 hours and over the next 12 hours. It displays the scheduled start times of the activities, as well as their summaries and descriptions. As implementation proceeds, the activity status and implementation outcome are updated here.

To access	Select **Module** > **Director** > **Implementor** > **To-Do List** pane.
Relevant tasks	Modify the Implementation Progress of an Activity
See also	Managing Activity Implementation

User interface elements are described below:

UI Elements (A-Z)	Description
	Activity Information. Opens the Activity Information dialog box. Contains details about the selected activity. For details, see Activity Information Dialog Box.
	Open Activity Chat Room. Open a chat room in the Communications pane. For details, see User Communication.
	Request NOC Assistance. The NOC Assistance Request dialog box opens. As an implementor, you can submit a message to the NOC users requesting assistance for a certain activity. The message is conveyed in the Director module in the form of a high severity alert noting that the implementor is in need of assistance. For details, see Activity Alerts.
	Report Activity as Started. Updates the status of the activity to **Started**

UI Elements (A-Z)	Description
	Note: If you are fully integrated with Service Manager as your service desk, the **Report Activity as Started** field is automatically updated in the originating service desk when you update it in the Implementor module.
	Report Activity as Finished. Updates the status of the activity to **Finished**. Opens the Report Activity As Finished dialog box, prompting you for the implementation outcome. **Note:** If you are fully integrated with Service Manager as your service desk, the **Report Activity as Finished** field is automatically updated in the originating service desk when you update it in the Implementor module.
	Report Start of Downtime. Reports the start of activity downtime.
	Report End of Downtime. Reports the end of activity downtime.
	Outcome. After you select the required outcome in the Report Activity As Finished dialog box, the outcome column is updated with one of the following icons: • **Successful.** The implementation was successful. • **Successful with problems.** The implementation was successful but you encountered some problems. • **Failed.** The implementation failed. • **Cancelled.** The activity was cancelled.
Activity ID	The reference ID number of the activity in the service desk application.
NOC Planned Start Time	The planned start time of the activity as rescheduled by the NOC users.
Status	Before implementation begins, the activity status is **Not Started**. When you start implementation and update the status, the Director module is automatically updated as well. This enables the NOC users to follow the progress of the implementation, and assist where necessary. To update the activity status in the Implementor module, you select the activity you want to update using the appropriate buttons in the To-Do List toolbar. The status for the activity is updated as follows: • **Not Started.** Before implementation begins, the activity

UI Elements (A-Z)	Description
	status is **Not started**. • **Started.** To update the activity's status to Started, click either **Report Activity as Started** or **Report End of Downtime** • **Down.** To update the activity's status to **Down**, click **Report Start of Downtime**. • **Done.** Implementation of the change is complete.

User Communication

This chapter includes:

Concepts

- User Communication Overview

Reference

- Communications Pane User Interface

Concepts

User Communication Overview

You can communicate with other users to convey or obtain information regarding the common activities with which you are associated, or regarding other topics by opening an activity chat room in the Communications pane. For details, see Communications Pane.

The Communications pane appears in both the Director and the Implementor modules.

- Director module users, such as NOC users, Release Managers, and Change Managers, communicate from the Director module. For details, see Director Module.
- Implementors communicate from the Implementor module. For details, see Implementor Module.

Activity Chat Rooms

If you are a NOC user, when you start a chat session, all users who are associated with that activity, and who are online, are alerted to the chat session.

If you are an implementor or other non-NOC user, all non-NOC users who are associated with the activity, and who are online, are alerted to the chat session. To involve NOC users in an activity chat session, you need to force their participation.

> **Note:** Users are **online** when they have opened the Director or Implementor module.

Reference

Communications Pane User Interface

This section describes:

- Add New Room Dialog Box
- Communications Pane
- Manage Chat Rooms Dialog Box

Add New Room Dialog Box

This dialog box enables you to create a new chat room. Enter a name for the custom chat room. The chat room is added to the list of rooms, listing you as its owner.

To access	Click **Add Chat Room** in the Manage Chat Rooms dialog box.
See also	User Communication Overview

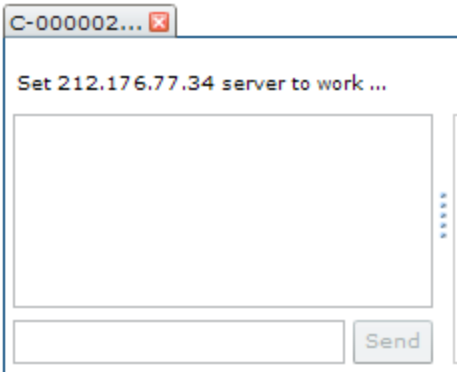
Communications Pane

This pane enables you to communicate with other users to convey or obtain information regarding the common activities with which you are associated, or regarding other topics. Opens an activity chat room window.

To access	• **In the Director module:** In the Activity Timeline pane, select the activity about which you want chat. Then, on the Activity Timeline or Alerts pane toolbar, click **Open Activity Chat Room**. • In the Implementor module: In the To-Do List pane, select the activity about which you want chat. Then, on the To-Do List toolbar, click **Open Activity Chat Room**.
Important Information	The Communications pane appears in both the Director and the

	Implementor modules.
Relevant tasks	Monitor the Implementation Progress of an Activity
See also	User Communication Overview

User interface elements are described below:

UI Elements (A-Z)	Description
	Enables you to leave a chat room. **Note:** This button appears when you hold the cursor over the chat room tab, adjacent to the activity ID. 
	Opens the Manage Chat Rooms dialog box. Enables you to create custom chat rooms where you can hold discussions about general issues.
	Forces NOC users to participate in the chat room. The next message you send opens a chat room window in the NOC users' Communications panes. **Note:** This button only appears in the Director module if the user is a NOC user.
	Users displayed in regular font are online but not in the chat room.
	Users displayed in bold font are in the chat room.
<Activity ID>	The name of the chat room window. The chat room window tab is named according to the ID of the activity in discussion.
Send	Type a message in the box to the left of the **Send** button, and click **Send** to send it to the other users. The message you send appears in the message pane. • If you are a NOC user, all the users listed are automatically

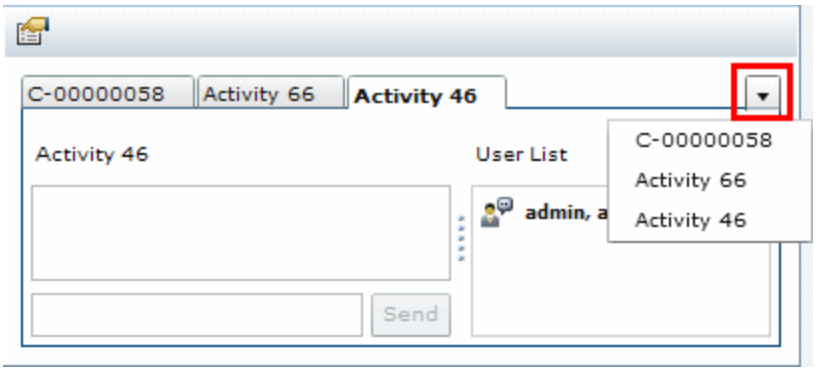
UI Elements (A-Z)	Description
	forced to participate in the chat session. ◦ A chat room windows open in each user's Communications pane. ◦ All users in the **User List** then appear in bold text, indicating that they are in the room. • If you are an implementor or other non-NOC users, NOC users are not automatically forced to participate the chat session. They continue to appear online, until they join the room on their own accord. Alternatively, you can force them to participate in the chat room by clicking **Force NOC Intervention** in the Communications pane. The next message you send opens a chat room window in the NOC users' Communications panes as well. Throughout the chat session, automated messages indicate when users come online and go offline, and when they join and leave the chat room.
User List	Displays all the online users associated with the activity in any way.

Manage Chat Rooms Dialog Box

This dialog box enables you to create custom chat rooms where you can hold discussions about general issues. For example, you can create chat rooms where database administrators can hold discussions, or where implementors can discuss general issues about activities they are implementing.

To access	Click **Manage Chat Rooms** in the Communications pane.
Important Information	When you create a chat room, you are its owner. Anyone can join the chat room. Only you, the owner, can delete it.
Relevant tasks	Monitor the Implementation Progress of an Activity
See also	• Implementor Module • Director Module • User Communication Overview

User interface elements are described below:

UI Elements (A-Z)	Description
	Create a custom chat room. Opens the Add New Room dialog box.
	Deletes the selected chat room. **Note:** You can only delete chat rooms that you created.
	Join the selected chat room. You can participate in many chat rooms at a time, enabling you to discuss different issues with relevant fellow users. A chat room window opens in your Communications pane. Other users in the chat room appear in the **User List**.
	Displays the list of chat rooms in which you are participating. The drop-down arrow appears when you have joined two or more chat rooms. 
Owner	The name of the user who created the chat room.
Room name	Enter a name for the new chat room.

Part V: Dashboard

Working with the Dashboard

> **Note:** This chapter describes the Dashboard features available to the regular user. If you are an administrator, contact customer support for assistance in working with the additional Dashboard features available to you.

This chapter includes:

Concepts

- Viewing the Default Portlets
- Trends Portlets
- Analysis Portlets
- Post Implementation Portlets

Tasks

- Modify the Trend Portlets Display Preferences
- Modify the Display Preferences for the Application Severity Distribution Portlet
- Modify the Display Preferences for the Application Status Distribution Portlet
- Modify the Display Preferences for the Change Request Impact Analysis Ratio Portlet
- Modify the Display Preferences for the Outcome Over Time Portlet
- Modify the Display Preferences for the Outcome Grouped by Risk Portlet
- Personalize the Dashboard
- Manage Portlets

Reference

- Working with Dashboard Pages

Concepts

Viewing the Default Portlets

To open the Dashboard, select **Module** > **Dashboard**. The Dashboard opens displaying the Home tab.

The portlets displayed in the Home tab provide change request information based on Trends, Analysis, and Post Implementation. By default, the Trends portlets are displayed.

To display a different set of portlets, click **Switch to page**, then select **Release Control Default Module** and the desired portlets.

To maximize a portlet, click the **Maximize** button in the upper right hand corner of the portlet. A magnified view of the portlet is displayed on a page by itself. To return to the original view, click **Back**.

> **Notes:**
>
> 1. If you are the first user logging on to the application after the server was started, the Dashboard may take a few minutes to load. The next time you enter the Dashboard, it loads immediately.
> 2. The Release Control Default Page cannot be edited or personalized. To personalize or edit the preferences on this page, you must copy this page to your list of personal Dashboard pages. Copying pages is not available by default and must be enabled by the administrator.
> 3. If you copied the Release Control Default Page and the administrator required a preference to be defined before displaying one of the portlets on the page, you must define a preference for this portlet in order to view it.
> 4. Even if you copied the Release Control Default Page and can, in general, edit the preferences on this page, you are not able to edit a portlet preference that the administrator preconfigured.

Trends Portlets

The default Trends portlets display information relating to change requests shown over time.

The following portlets are displayed:

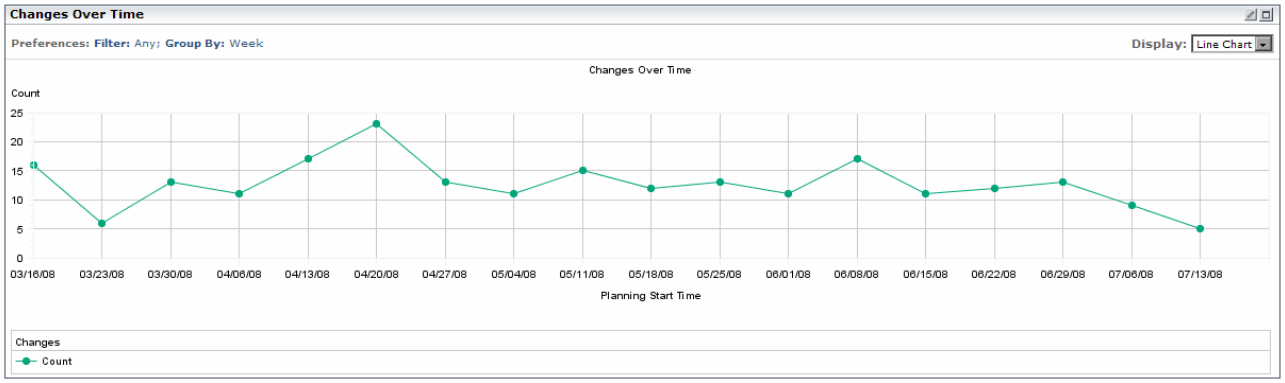
- Changes Over Time Portlet
- Abnormal Changes Over Time Portlet
- Latent Changes Over Time Portlet

By default, the Trends portlets are displayed in line chart format. To display the same information as a list, select **List** from the **Display** drop down list in the upper right hand corner of each portlet.

For information on modifying the display preferences of the Trends portlets, see Modify the Trend Portlets Display Preferences.

Changes Over Time Portlet

The Changes Over Time portlet displays the upward or downward movement in the number of overall change requests, measured at one week intervals.



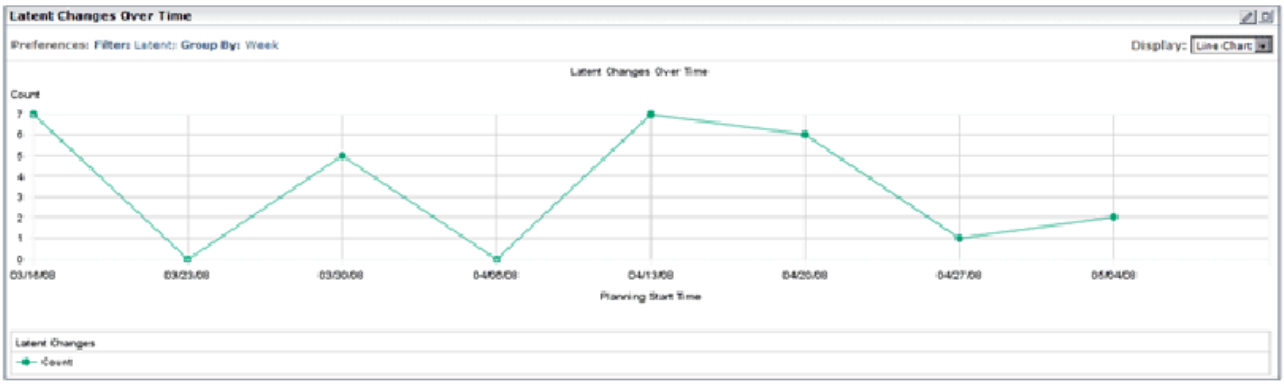
Abnormal Changes Over Time Portlet

The Abnormal Changes Over Time portlet displays the upward or downward movement in the number of abnormal change requests, measured at one week intervals.

Latent Changes Over Time Portlet

The Latent Over Time portlet displays the upward or downward movement in the number of latent

change requests, measured at one week intervals.



Analysis Portlets

The default Analysis portlets display analysis information relating to change requests.

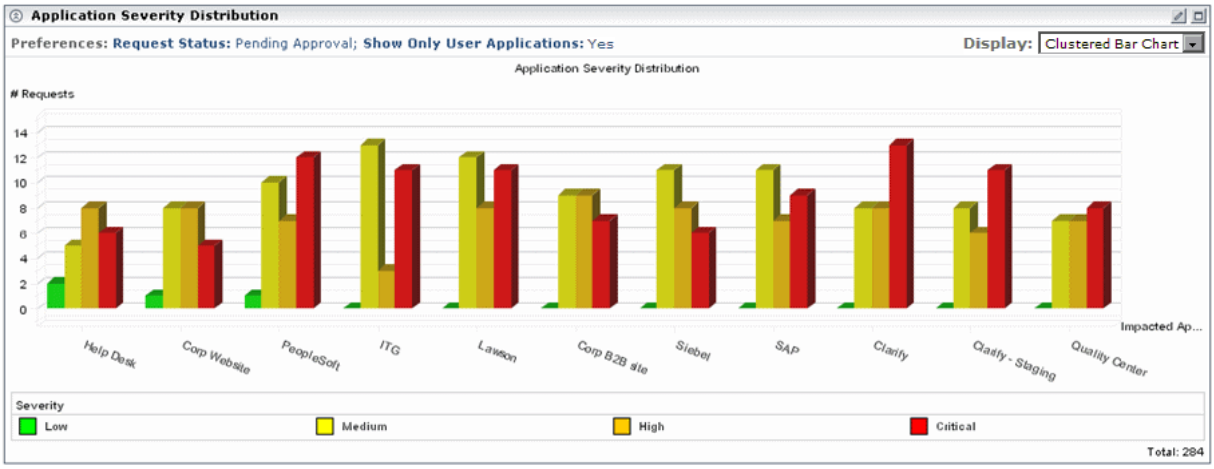
The following portlets are displayed:

- Application Severity Distribution Portlet
- Application Status Distribution Portlet
- Change Request Impact Analysis Ratio Portlet

By default, the Analysis portlets are displayed as clustered bar charts. To display the same information as either a pie chart or a list, select the desired option from the **Display** drop down list in the upper right hand corner of each portlet.

Application Severity Distribution Portlet

The Application Severity Distribution portlet displays the number of change requests at each severity level, per application, for the request status selected by the user.

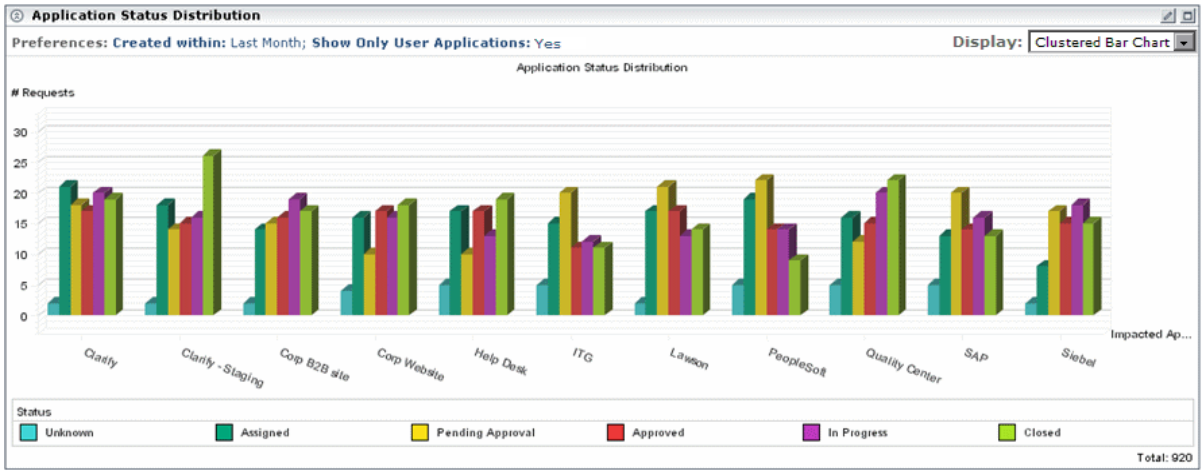


For example, the above graph shows that the Help Desk application has:

- 2 Pending Approval change requests with a severity level of **Low**
- 5 Pending Approval change requests with a severity level of **Medium**
- 8 Pending Approval change requests with a severity level of **High**
- 6 Pending Approval change requests with a severity level of **Critical**

Application Status Distribution Portlet

The Application Status Distribution portlet displays the number of change requests for each request status level, per application, that were created within the time frame selected by the user.

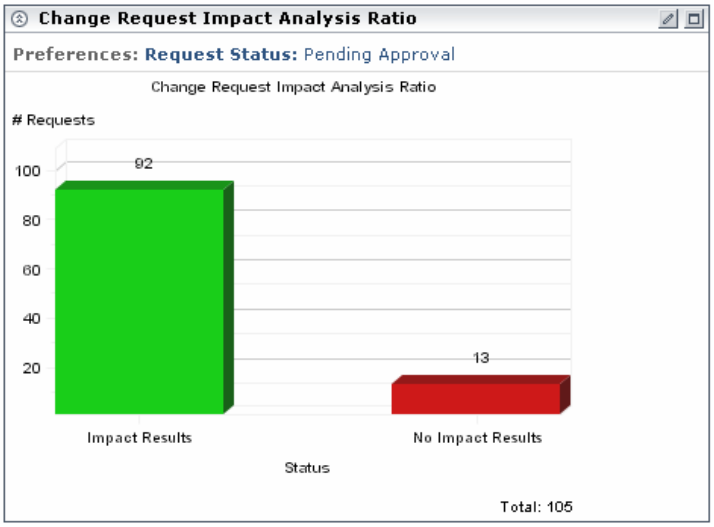


For example, the above graph shows that the following change requests affecting the Help Desk application were created during the last month:

- 5 change requests with a current status level of **Unknown**
- 17 change requests with a current status level of **Assigned**
- 10 change requests with a current status level of **Pending Approval**
- 17 change requests with a current status level of **Approved**
- 13 change requests with a current status level of **In Progress**
- 19 change requests with a current status level of **Closed**

Change Request Impact Analysis Ratio Portlet

The Change Request Impact Analysis Ratio portlet displays both the number of change requests for which impact analysis results were available as well as the number of change requests for which impact analysis results could not be found, for the request status selected by the user.



For example, the above graph shows the following:

- Impact analysis results were available for 92 Pending Approval change requests.
- No Impact analysis results were found for 13 Pending Approval change requests.

Post Implementation Portlets

The default Post Implementation portlets display information relating to completed change requests.

The following portlets are displayed:

- Outcome Over Time Portlet
- Outcome Grouped By Risk Portlet

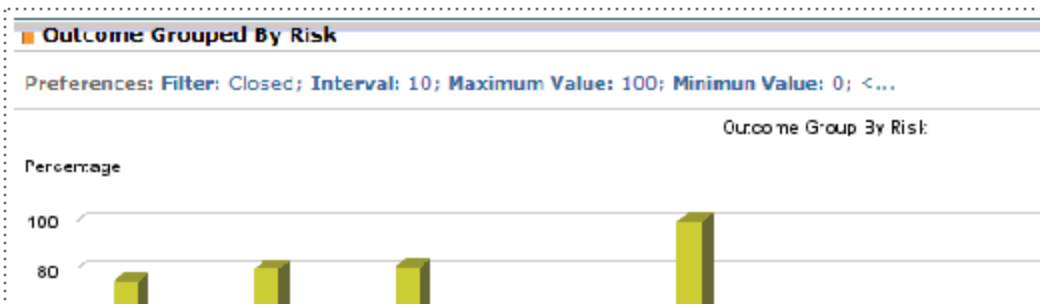
Outcome Over Time Portlet

The Outcome Over Time portlet displays the upward or downward movement in the percentage of each change outcome, measured at one week intervals.

By default, the portlet is displayed in line chart format. To display the same information as a list, select **List** from the **Display** box in the upper right hand corner of the portlet.

Outcome Grouped By Risk Portlet

The Outcome Grouped By Risk portlet displays the percentage of change requests with specific outcomes, grouped within intervals of calculated risk values.



For example, the above portlet shows that for completed change requests that had a risk value between 0 and 9:

- 22% have the outcome **Successful With Problems**
- 78% have the outcome **Not Reviewed**
- None have the outcome **Cancelled**
- None have the outcome **Failed**

By default, the portlet is displayed as a clustered bar chart. To display the same information as a stacked bar chart or a list, select the desired option from the **Display** drop-down list in the upper right hand corner of the portlet.

Tasks

Modify the Trend Portlets Display Preferences

You can modify the Trend portlets display preferences only after the portlets have been copied to your list of personal Dashboard pages.

To modify display preferences:

1. Click the **Edit** button . The Edit Preferences page opens, displaying the following options:
   - **Change Title.** Clicking this button opens the Change Portlet Title window in which you can enter an alternative title for the Changes Over Time portlet.
   - **Filter.** You can select which category of change requests to include in the portlet. The options that appear here are the same as the filter options in the Analysis module.
   - **Group by.** You can choose to show movement in the number of changes over daily, weekly, monthly or yearly intervals.
   - **Display preferences summary on portlet.** Although, by default, preferences are displayed as part of the portlet, you can choose to view the portlet without a display of the preferences. To do so, clear the **Display preferences summary on portlet** check box.
2. Click **Done** to save your preference settings and return to the default Dashboard page.

Modify the Display Preferences for the Application Severity Distribution Portlet

You can modify the Application Severity Distribution portlet display preferences only after the portlet has been copied to your list of personal Dashboard pages.

To modify the display preferences:

1. Click the **Edit** button . The Edit Preferences page opens, displaying the following options:
   - **Change Title.** Clicking this button opens the Change Portlet Title window in which you can enter an alternative title for the Application Severity Distribution portlet.
   - **Show Only User Applications.** You can modify the default option whereby data is displayed only for those applications associated with the current user. (You associate applications with the current user in the User Settings dialog box. For details, see User Preferences.) To display data for all IT applications affected by the change requests that Release Control processes, select **No** under **Show Only User Applications**.
   - **Request Status.** You can modify the default option whereby data is displayed only for requests with the status **Pending Approval**. To display data for requests with a different status, select the required status from the **Request Status** selection box.
   - **Display preferences summary on portlet.** Although, by default, preferences are displayed as part of the portlet, you can choose to view the portlet without a display of the preferences. To do so, clear the **Display preferences summary on portlet** check box.
2. Click **Done** to save your preference settings and return to the default Dashboard page.

Modify the Display Preferences for the Application Status Distribution Portlet

You can modify the Application Status Distribution portlet display preferences only after the portlet has been copied to your list of personal Dashboard pages.

To modify the display preferences:

1. Click the **Edit** button . The Edit Preferences page opens, displaying the following options:
   - **Change Title.** Clicking this button opens the Change Portlet Title window in which you can enter an alternative title for the Application Status Distribution portlet.
   - **Created Within.** You can choose to display data for change requests that were created within a time frame other than the default one, **Last Month**. To display data for change requests created within a different time frame, select **Last Week** or **Last Two Weeks** from the **Created Within** selection box.
   - **Show Only User Applications.** You can modify the default option whereby data is displayed only for those applications associated with the current user. (You associate applications with the current user in the User Settings dialog box. For details, see User Preferences.) To display

data for all IT applications affected by the change requests that Release Control processes, select **No** under **Show Only User Applications**.

- **Display preferences summary on portlet.** Although, by default, preferences are displayed as part of the portlet, you can choose to view the portlet without a display of the preferences. To do so, clear the **Display preferences summary on portlet** check box.

2. Click **Done** to save your preference settings and return to the default Dashboard page.

Modify the Display Preferences for the Change Request Impact Analysis Ratio Portlet

You can modify the Change Request Impact Analysis Ratio portlet display preferences only after the portlet has been copied to your list of personal Dashboard pages.

To modify the display preferences:

1. Click the **Edit** button . The Edit Preferences page opens, displaying the following options:
   - **Change Title.** Clicking this button opens the Change Portlet Title window in which you can enter an alternative title for the Change Request Impact Analysis Ratio portlet.
   - **Request Status.** You can modify the default option whereby data is displayed only for requests with the status **Pending Approval**. To display data for requests with a different status, select the required status from the **Request Status** selection box.
   - **Display preferences summary on portlet.** Although, by default, preferences are displayed as part of the portlet, you can choose to view the portlet without a display of the preferences. To do so, clear the **Display preferences summary on portlet** check box.
2. Click **Done** to save your preference settings and return to the default Dashboard page.

Modify the Display Preferences for the Outcome Over Time Portlet

You can modify the Outcome Over Time portlet display preferences only after the portlet has been copied to your list of personal Dashboard pages.

To modify the display preferences:

1. Click the **Edit** button. The Edit Preferences page opens, displaying the following options:
   - **Change Title.** Clicking this button opens the Change Portlet Title window in which you can enter an alternative title for the Changes Over Time portlet.
   - **Filter.** You can select which category of change requests to include in the portlet. The options that appear here are the same as the filter options in the Analysis module.
   - **Group by.** You can choose to show movement in the percentage of the different change outcomes over daily, weekly, monthly or yearly intervals.
   - **Display preferences summary on portlet.** Although, by default, preferences are displayed as part of the portlet, you can choose to view the portlet without a display of the preferences. To do so, clear the **Display preferences summary on portlet** check box.
2. Click **Done** to save your preference settings and return to the default Dashboard page.

Modify the Display Preferences for the Outcome Grouped by Risk Portlet

You can modify the Outcome Grouped by Risk portlet display preferences only after the portlet has been copied to your list of personal Dashboard pages.

To modify the display preferences:

1. Click the **Edit** button. The Edit Preferences page opens, displaying the following options:
   - **Change Title.** Clicking this button opens the Change Portlet Title window in which you can enter an alternative title for the Changes Over Time portlet.
   - **Filter.** You can select which category of change requests to include in the portlet.
   - **Numeric Type.** You can choose to view change outcomes according to any numeric field as defined in your system settings.
   - **Minimum Value.** The lowest value of the numeric type to include in the portlet.
   - **Maximum Value.** The highest value of the numeric type to include in the portlet.
   - **Interval.** You can define at which numeric intervals to group the change requests.
   - **Display preferences summary on portlet.** Although, by default, preferences are displayed as part of the portlet, you can choose to view the portlet without a display of the preferences. To do so, clear the **Display preferences summary on portlet** check box.
2. Click **Done** to save your preference settings and return to the default Dashboard page.

Personalize the Dashboard

You can personalize the Dashboard by adding groups and pages within these groups, choosing the portlets to be displayed on each page, and specifying the positions of the portlets on the page.

You personalize groups, pages, and portlets in the Personalize screen, which you can access by clicking the **Personalize** button in the top right-hand corner of the current page, or the **Personalize** tab in the top menu.

This section describes:

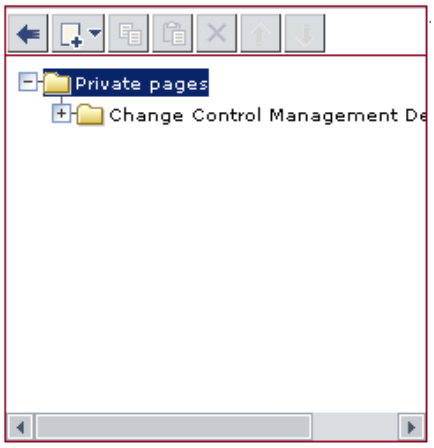
- Add Groups
- Add Pages
- Copy Pages
- Modify Pages
- Add Portlets

Add Groups

You can add groups under which you can place pages. This enables you to categorize your personal pages.

To add a group:

1. In the Personalize screen, select **Private pages** in the Dashboard page tree.



2. Click the **Add** button  and select **New Group**. A new group is added to the Dashboard page tree.

3. In the Edit Group pane on the right, enter a name for the new group and a brief description of the group. The new group is renamed in the Dashboard page tree.

Add Pages

You can add new blank pages either to the groups that you created or directly to the Dashboard page tree. You then populate these pages with portlets.

If you have been assigned the necessary privileges, you can also add preconfigured pages (also referred to as modules). Preconfigured pages are sets of pages containing portlets that the administrator has already created.

To add a new page to the Dashboard page tree:

1. In the Personalize screen's Dashboard page tree, select **Private pages** or the specific group to which you want to add a page.
2. Click the **Add** button and select **New Page**. A new page is added to the Dashboard page tree.
3. In the Edit Page pane on the right, enter a name for the new page. The new page is renamed in the Dashboard page tree.
4. Specify how often you want the data on the page to be refreshed by selecting the **Automatically refresh this page every X minutes** check box and entering the refresh rate. By default, the Dashboard does not refresh pages.

After creating the page, you can populate it with portlets. For more information, see Add Portlets.

To add a pre-configured page to the Dashboard page tree:

1. In the Personalize screen's Dashboard page tree, select **Private pages**.
2. Click the **Add** button and select **Add Preconfigured Pages**. The Add Preconfigured Pages dialog box is displayed in the right pane.
3. Select the check box to the left of the modules whose pages you want to add to the Dashboard page tree. Each module you select is added as a group in the tree. The module's pages appear under the group created for the module.

Copy Pages

You can copy pages from one group to another in the Dashboard page tree. In addition, if you have been assigned the necessary privileges, you can copy a shared module (containing several pages) or page to the list of your personal Dashboard pages.

To copy a module or page:

1. Select the module or page you want to copy (either in the Dashboard page tree or under **Shared pages**) and click the **Copy** button .
2. In the Dashboard page tree, select **Private pages** or the group under which you want to place the copied module or page, and click the **Paste** button . The module or page is copied to the selected location.

Modify Pages

You can change the order of the Dashboard pages in the **Switch to page** list. You can also rename and remove pages, and modify the refresh rate of a page.

To modify a page:

Access the Personalize screen.

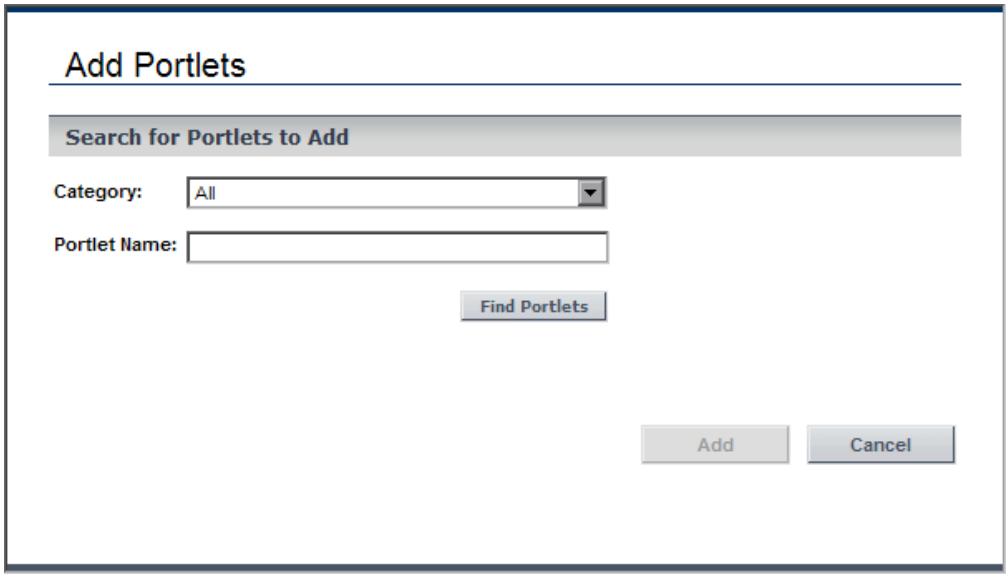
- To change the position of a page in the **Switch to page** list, change the position of the page in the Dashboard page tree by clicking the **Up** and **Down** buttons .
- To rename a page, select the page in the Dashboard page tree and enter a new name in the Edit Page pane's **Page Name** box.
- To remove a page from the Dashboard, select the page in the Dashboard page tree and click the **Delete**button . Click **Yes** to confirm deletion.
- To modify the refresh rate of a page, select the page in the Dashboard page tree, then select the **Automatically refresh this page every X minutes** check box and specify a new refresh rate in the Edit Page pane.
- To add portlets to a page, see Add Portlets.
- To modify how portlets are displayed on a page, see Manage Portlets.

Add Portlets

You can add portlets to a selected page. Note that to optimize the time that it takes to load a page and make the page easy to view, it is recommended that you limit the number of portlets on a page to six.

To add a portlet to a page:

1. In the Personalize screen's Dashboard page tree, select the page to which you want to add portlets and click **Add Portlets** in the Edit Page pane. The Add Portlets window opens.



2. In the **Portlet Name** box, enter the name of the portlet you want to add to the page.
3. From the **Category** box, select the category to which the portlet belongs if the administrator has defined portlet categories.
4. Click **Add**.

Alternatively, click **Find Portlets** to display a list of available portlets, select the portlets that you want to add to the page, and click **Add**.

The portlets you specified are added to the page in both the Edit Page pane and the Dashboard page tree.

To rearrange the order in which the portlets are displayed, or to move or remove portlets from a page, see Manage Portlets.

Manage Portlets

This section describes the following Dashboard functionality:

- Arrange Portlets on a Page
- Copy Portlets to Other Pages
- Rename Portlets
- Remove Portlets from Pages

Arrange Portlets on a Page

You can determine the layout of the portlets on each of the Dashboard pages.

To arrange the portlets on a page:

1. In the Edit Page pane, select the portlet you want to move. Selecting the portlet causes it to be highlighted on the page.
2. Drag the portlet to its new position.

For each portlet you want to move, repeat steps 1 and 2.

The portlets appear in their new positions in the Edit Page pane and Dashboard page tree.

Copy Portlets to Other Pages

You can copy an existing portlet from one personal page to another. You can also copy a shared portlet to a personal page if you have been assigned the necessary privileges by the administrator.

> **Note:** To optimize the time that it takes to load a page and make the page easy to view, it is recommended that you limit the number of portlets on a page to six.

To copy a portlet to another page:

1. Select the portlet that you want to copy and click the **Copy** button .
2. Select a page in the Dashboard page tree and click the **Paste** button . The portlet is copied to the selected page.

> **Note:** The new portlet's name is the original portlet's name preceded by **Copy of**. To rename the copied portlet, see Rename Portlets.

Rename Portlets

Renaming a portlet is useful when the same portlet is duplicated with different preferences in each copy.

To rename a portlet:

1. In the Edit Page pane, select the portlet that you want to rename and click the **Edit Portlet Preferences** button . The Edit Preferences: <name of portlet> pane is displayed.
2. Click **Change Title**. The Change Portlet Title window opens.
3. Enter the new name (with a maximum of 30 characters) in the **Title** box and click **Change**. The new portlet title is displayed in the Edit Page pane and Dashboard page tree.

Remove Portlets from Pages

You can remove a portlet from a Dashboard page. Note that this does not affect other occurrences of the portlet on other Dashboard pages.

To remove a portlet from a page:

1. In the Dashboard page tree, select the portlet that you want to remove and click the **Delete** button . Alternatively, in the Edit Page pane, select the portlet that you want to remove, and click the **Remove Portlet From Page** button .
2. Click **OK** to confirm deletion. The portlet is removed from the Edit Page pane and Dashboard page tree.

Reference

Working with Dashboard Pages

The following buttons are available at the top of a Dashboard page:

Button	Description
	The **Favorites** button enables you to add the current page to your favorites, or to open the Manage Favorites page.
	The **View Module Comments** button enables you to view the comments that the administrator entered for the current module (available only if the page is public and is part of a module defined by the administrator).
	The **Page Rotation** button enables you to determine the refresh rate for the current page.
	The **Export Dashboard Page to PDF** button enables you to create a PDF containing the data on the current page.
	The **Personalize** button enables you to open the Personalize screen and personalize the Dashboard. Clicking this button opens the current portlet for editing. For details, see Personalize the Dashboard.

If the page is a public page and the administrator has configured access to the page for a number of users, the words **Shared Page** appear in the top right-hand corner of the page.

Part VI: Administration

Release Control Configuration Overview

This chapter includes:

Concepts

- Release Control Data Flow
- The Configuration Process - Basic Overview

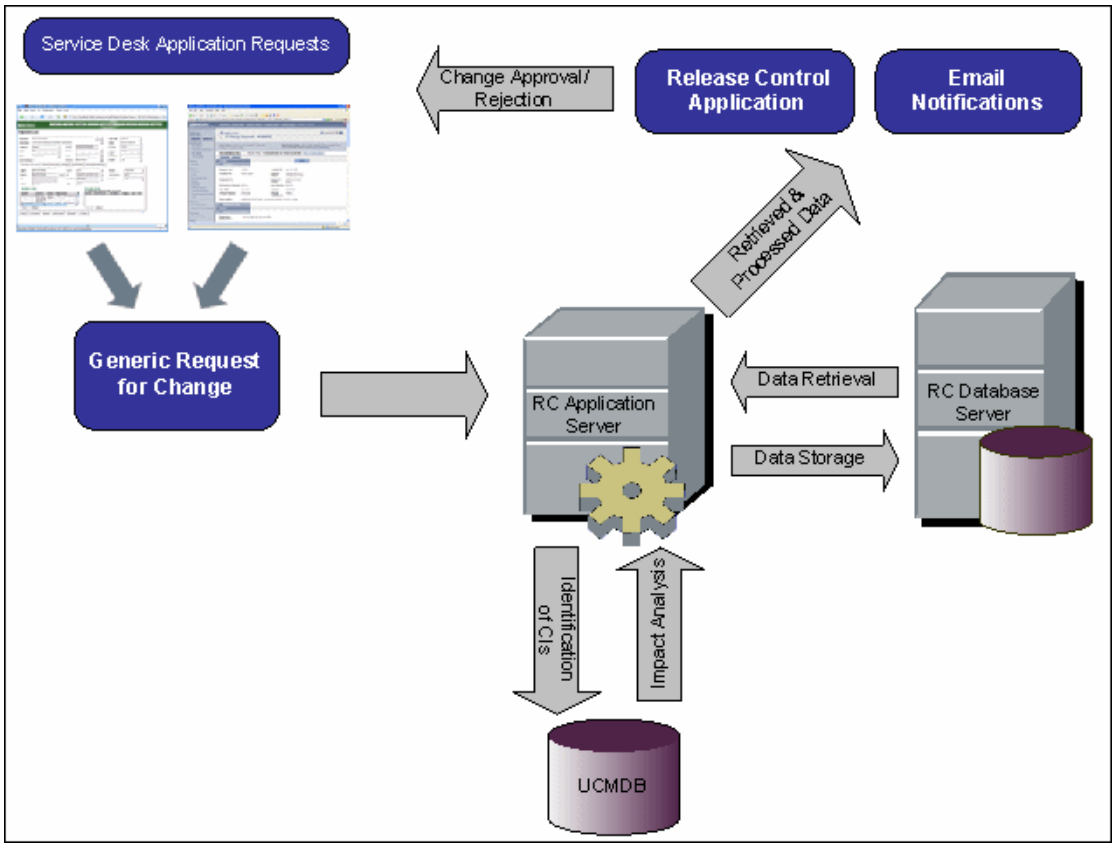
Tasks

- Deploy Release Control
- Configure the Analysis of Change Requests
- Configure the Review and Collaboration Settings
- Configure General Settings and System Preferences

Concepts

Release Control Data Flow

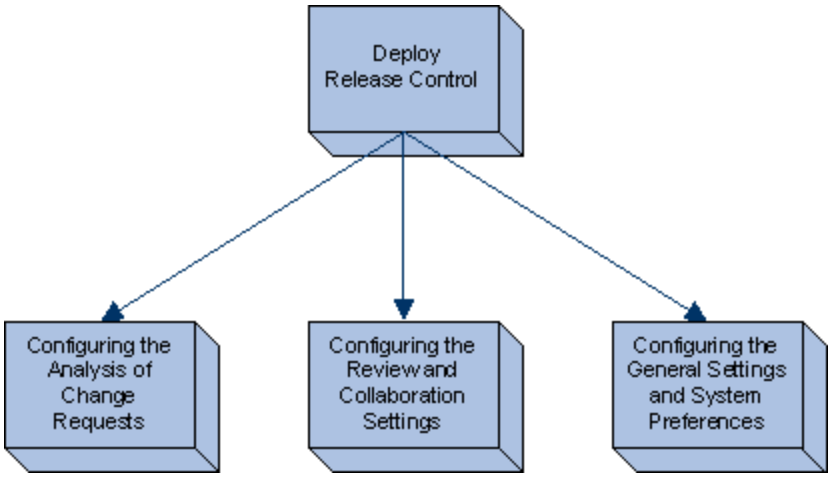
The following diagram illustrates the data flow when running Release Control:



- Change requests originate in the Service Desk application and are converted into generic requests.
- Release Control sends the requests to Universal CMDB for analysis and to determine the relationships between configuration items (CIs).
- Release Control takes the data from Universal CMDB and performs impact analysis.
- Release Control further analyzes change requests, performing calculations such as risk and collision analysis.
- The information is stored on the Release Control 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 Release Control configuration process:



1. Deploy Release Control
2. Configure the Analysis of Change Requests
3. Configure the Review and Collaboration Settings
4. Configure General Settings and System Preferences

Tasks

Deploy Release Control

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

Configure the Analysis of Change Requests

This task includes the steps for configuring the analysis of change requests in Release Control:

This task includes the following steps:

Step 1: Perform the initial configuration

Step 2: Analyze the collected requests

Step 3: Calculate impact analysis for the requests

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

Step 5: Configure the collision calculation settings

Step 6: Calculate risk analysis for the requests

Step 7: Configure Similar Changes

Step 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 are collected.

1. Configure how often change requests are collected by selecting **Module** > **administrator** > **Configuration** tab > **Change Process** in the configuration tree. In the **Collection Frequency** box, enter the required value. For details, see Change Process Pane.
2. Calculate certain pre-change request processing or post-change request processing factors by using the **preChangeProcess** and **postChangeProcess** functions in the **change-flow.js**script in **Module** > **administrator** > **Configuration** tab > **Change Process** > **change flow script**.
   For example, if you want to define a risk factor based on the amount of time that a change request is in the Release Control system without being processed, you can use the **preChangeProcess** function to calculate the time at which the change request first enters 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 Release Control. You would then instruct 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. (To access the API Reference, select **Start** > **Programs** > **Release Control 9.60** > **Documentation** and open the **pdfs** directory).

Step 2: Analyze the collected requests

To analyze the collected requests, 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 Release Control to use, see Impact Analysis Rules Pane.

Step 3: Calculate impact analysis for the requests

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 Impact Analysis Rules Pane.

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

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 Release Control determines whether a change request is included in a defined time period category. For details, see Define Time Periods.

Step 5: Configure the collision calculation settings

Release Control identifies and calculates collisions between requests according to properties that you define for the requests that you instruct Release Control to include in the collision calculation. For details on configuring Release Control's collision calculations, see Calculating Change Request Collisions.

Step 6: Calculate risk analysis for the requests

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 Risk Analysis.

Step 7: Configure Similar Changes

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 Similar Changes Analysis.

Configure the Review and Collaboration Settings

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

This task includes the following steps:

Step 1: Determine the conditions for which action items should be automatically created

Step 2: Configure the change request approval/retraction/denial operation

Step 3: Configure email notifications

Step 4: Configure the Post Implementation Review (PIR) feature

Step 1: Determine the conditions for which action items should be automatically created

By default, 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 Configure the Automatic Creation of Action Items.

Step 2: Configure the change request approval/retraction/denial operation

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 Configure Release Control for Request Approval.

Step 3: Configure email notifications

You can configure 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 Release Control sends notifications, see Configuring Notifications Overview.

Step 4: Configure the Post Implementation Review (PIR) feature

The 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. For details, see Post Implementation Review Dialog Box.

Configure General Settings and System Preferences

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

This task includes the following steps:

Step 1: Configure the general settings

Step 2: Configure the business settings

Step 3: Configure the user settings

Step 1: Configure the general settings

Configure the following:

- **The SNMP mail server** and the **Release Control server**. For more details, see Server Pane.
- **Calendar settings.** For more details, see Calendar Pane.
- **Dashboard settings.** For more details, see Dashboard Pane.

Step 2: Configure the business settings

You can associate users with Business CIs, and configure the business CI details which are displayed in the user interface. For details on configuring this operation, see Business CI Configuration Overview.

Step 3: Configure the user settings

Configure the user settings such as user names, passwords, and user authentication. For more details, see User Configuration and Release Control User Authentication Overview.

Working with the Configuration Tab

This chapter includes:

Concepts

- Configuration Tab Overview

Tasks

- Configure Files in the Configuration Tab
- Save and Apply Configuration Changes
- Resolve a Configuration Setting Validation Problem

Reference

- Configuration Tab User Interface

Concepts

Configuration Tab Overview

The Configuration tab in the Administrator module enables you to define the configuration settings needed to set up your environment.

A configuration set contains the properties you defined for the system in the **Module** > **Administrator** > **Configuration** tab. All the configuration for the system is done in the Configuration tab. You can create any number of configuration sets and then select one with which to run your system. Release Control maintains a history of all the configuration sets created. For details on how to display a list of all the existing configuration set versions, see Open Configuration Set Dialog Box.

Release Control enables you to move configuration sets from one system to another. You can:

- Export a configuration set to your local directory.
- Import a configuration set from your local directory to another system. For example, from a test to a production environment.

A new configuration set is initially saved as a draft. A draft is a configuration set that has not yet been activated. A draft can be edited only until it is first activated. Only after a draft is activated, are the new configuration properties applied to Release Control. For details on how to activate a draft, see Save and Apply Configuration Changes.

If you need to edit a configuration set after it has been activated, you must create a new draft. You can create a new draft based on any configuration set.

For details on how to create a draft, see Save as Draft Dialog Box.

For details on how to work with the Configuration tab, see Configuration Tab.

Tasks

Configure Files in the Configuration Tab

Certain configuration settings are defined in configuration files (for example, scripts and XML files) that are available in the Configuration tab. This task describes how to modify these files.

1. Select **Module** > **Administrator** > **Configuration** tab and click on the file to be configured. Content of this file is displayed in the right pane.
2. After making the required modifications to the file, click the **Save current editable configuration set** button to open the Save as Draft dialog box and save the modified configuration set as a draft.

Save and Apply Configuration Changes

This task describes how to save configuration changes and then apply the new configuration properties to Release Control.

1. Select **Module** > **Administrator** > **Configuration** tab and make the required configuration changes.
2. In the left pane, click the **Save current editable configuration set** button to open the Save as Draft dialog box and save the modified configuration set as a draft. A draft is a configuration set that has not yet been activated. After a draft is activated, the new configuration properties are applied to Release Control.
3. In the **Draft name** box, enter the name of the draft and click **Save**.

4. In the left pane, click **Open Configuration Set** to open the Open Configuration Set dialog box.
5. Click the **Drafts** button to display only the existing drafts.
6. Select the required draft and click **Open**. The name of the currently selected configuration set appears at the top of the left pane.
7. In the left pane, click the **Activate current configuration set** button to activate the selected draft and apply the new configuration properties to Release Control.

Resolve a Configuration Setting Validation Problem

When defining the configuration settings needed to set up your environment, certain errors prevent you from activating your configuration set.

This task describes how to define a collision cause by creating a custom filter by which only change requests that are opened by `John Smith` are included in the collision calculation. For the purposes of this task, the field which needs to contain the value `John Smith` is left empty.

This task illustrates how Release Control:

- Notifies you of an error in the configuration
- Informs you exactly what the problem is
- Creates a link to the place in the application where the problem is located

Step 1: Specify a field you want to define as a collision cause

1. Select **Module** > **Administrator** > **Configuration** tab > **Change Process** > **Collisions** > **Prerequisites**. In the Fields value prerequisites pane, you want to create a custom filter by which only change requests that are opened by John Smith are included in the collision calculation.
2. Click the **Add configuration to configuration set** button to add a field to be used in the filter.
3. Click the downward arrow in the **Field name** column and select **opened-by**. A value must be specified for this field, but for the purposes of this task, we are leaving the **Value** field empty.

For more information on the Prerequisites pane, see Prerequisites Pane.

Step 2: Save the configuration set

In the left pane, click the **Save the current editable configuration set** button to save the configuration set. Release Control calculates the configuration validation and determines that a value should have been defined for the selected field.

The **Activate current configuration set** button in the left pane is disabled and following appears in the Problems pane:

- A description of the problem in the **Description** column
- An **Error** icon in the **Problem severity level** column
- A link to the Prerequisites pane in the **Code** column

Problems

Code		Description
RC-00001		Value is required for property Values in configuration Field value prerequisites.

Step 3: Define a value for the opened-by field

In the Fields value prerequisites pane, click inside the **Value** box and enter `John Smith`.

Step 4: Save the configuration set

In the left pane, click the **Save the current editable configuration set** button to save the configuration set. The Problems pane is now cleared and the **Activate current configuration set** button is enabled.

Step 5: Activate the configuration set

In the left pane, click the **Activate current configuration set** button to activate the configuration set.

Reference

Configuration Tab User Interface

This section includes:

- Configuration Tab
- Open Configuration Set Dialog Box
- Save as Draft Dialog Box

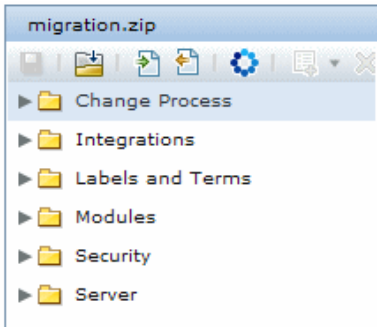
Configuration Tab

This tab enables you to define the configuration settings needed to set up your environment by creating configuration sets.

A configuration set contains the properties you defined for the system. For more information about configuration sets, see Configuration Tab Overview.

To access	Select **Module** > **Administrator** > **Configuration** tab.
Relevant tasks	• Resolve a Configuration Setting Validation Problem • Configure Files in the Configuration Tab • Save and Apply Configuration Changes

<Left Pane>



This pane displays a configuration tree. The tree contains the nodes whose properties need to be defined to set up your Release Control environment. The properties are divided into categories. The configuration fields for each selected node in the tree are displayed in the right pane.

Important Information	The name of the current configuration set appears at the top of the left pane.

User interface elements are described below:

UI Elements (A-Z)	Description
	Save the current editable configuration set. Enables you to create a draft of a new configuration set. A draft is a configuration set that has not yet been activated and can still be edited. This button is enabled when you make a change to the currently activated configuration set. For details, see Save as Draft Dialog Box.
	Open configuration set. Displays a list of all the existing configuration set versions. For details, see Open Configuration Set Dialog Box.
	Import configuration set. Enables you to import a configuration set from your local directory to another system. Opens the Import Configuration set dialog box.
	Export configuration set to a zip file. Enables you to Export a configuration set to your local directory as a zip file. Opens the Opening exported_configuration.zip dialog box.
	Activate current configuration set. Applies the configuration properties in the draft/configuration set to Release Control and becomes the active configuration set. > **Note:** Only one configuration set is considered active at any given point of time.
	Add configuration to configuration set. This button is only enabled when you select a node on the configuration tree that allows you to add a child configuration.
	Remove configuration from configuration set. This button is only enabled when you select a node on the configuration tree that allows you to delete a child configuration.
	Denotes a configuration category. > **Note:** The arrow next to each category enables you to expand or collapse the lower-level categories.
<Configuration tree>	Contains the configuration categories. The configuration fields for each selected node in the tree are displayed in the right pane. The configuration categories are: • **Change Process.** For details, see Change Process Configuration. • **Integrations.**For details, see Universal CMDB-Related Setting Configuration and Field and Enumeration Setting Configuration.

UI Elements (A-Z)	Description
	• **Labels and Terms.** For details, see Label and Term Configuration. • **Modules.** For details, see Module Configuration. • **Security.** For details, see Security Configuration. • **Server.** For details, see Server Configuration.

To export part of a configuration set to your local directory:

1. Select **Module** > **Administrator** > **Configuration** tab > **Export configuration set to a zip file** in the left pane. The Export configuration set tree appears.
2. In the tree, select the configuration nodes whose changes you want to export.
3. Click **Export**.

Things need your attention when performing partial import:

When importing a partially exported configuration set from the same version of Release Control, to an existing configuration set:

- Import of configuration overrides ONLY those parts which exist in the zip file that you are trying to import.
- You cannot delete an existing configuration that is missing from the imported configuration set.

For example:

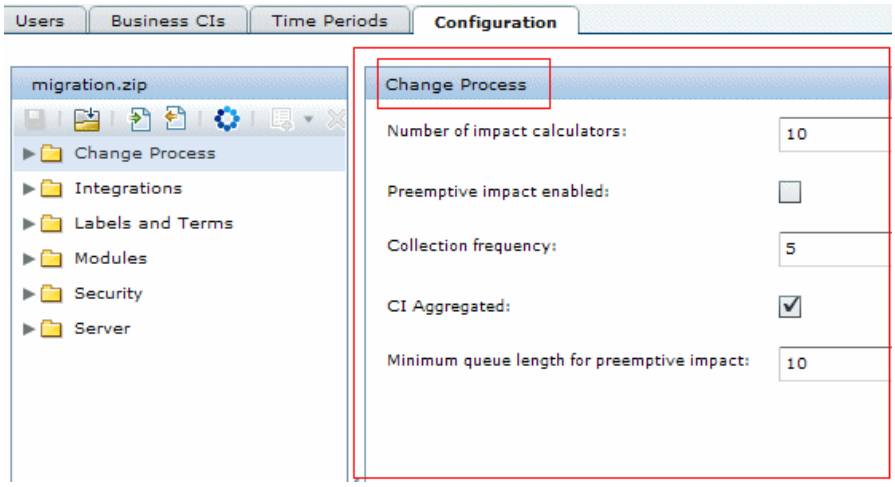
1. Select **Module** > **Administrator** > **Configuration** tab > **Modules** > **Analysis** > **Calendar**.
2. In the Calender color mapping pane, remove the field value **very_low** and its associated color.
3. Export that configuration set.
4. Import that configuration set into another draft where the field value **very_low** exists.

You will find the field value **very_low** is not deleted from the draft by the import operation. It only overrides other existing entries or adds new entries to that draft. To delete the entry, you must do it manually.

> **Notes:**
>
> - If you want to import a configuration set while working with a configuration set which has not yet been activated (a draft), the imported configuration set overrides the current draft.

> - If you want to import a partially exported configuration set while working with a configuration set which has already been activated, you must provide a different draft name in the Draft name field in the Import Configuration Set dialog box to create a draft.

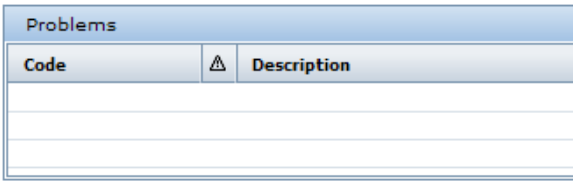
<Right Pane>



This pane displays the configuration fields of the selected node in the left pane.

Important Information	The top of the pane displays the name of the selected node in the configuration tree.

Problems Pane



Release Control calculates the validation of the configuration setting and identifies the problems in the configuration—for example, a field with a missing value. If a problem is found, Release Control displays a description of the problem, a link to the configuration pane in which the problem was found, and an icon that indicates the severity of the problem.

For an example that illustrates how Release Control notifies you of a configuration error, see Resolve a Configuration Setting Validation Problem.

Configuration validation is performed after the following operations:

- Saving a configuration set
- Opening a configuration set

- Importing a configuration set

User interface elements are described below:

UI Elements (A-Z)	Description
	Indicates the severity level of the problem. The following icons appear: • . Indicates that there is an error in the configuration settings. In this case, Release Control does not allow you to activate the configuration set and the **Activate current configuration set** button is disabled. • . Indicates a warning. In this case, Release Control allows you to activate the configuration set. • . Provides an informative message. In this case, Release Control allows you to activate the configuration set.
Code	Contains a link to the pane containing the problem. When you click the link, the relevant node in the configuration tree is selected and its relevant pane appears on the right.
Description	Contains a description of the problem.

Open Configuration Set Dialog Box

This dialog box displays a list of all the existing configuration set versions.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Open Configuration Set** in the left pane.
Important Information	You cannot change the name of any of the configuration set versions.
Relevant tasks	• Resolve a Configuration Setting Validation Problem • Save and Apply Configuration Changes • Configure Files in the Configuration Tab

User interface elements are described below:

UI Elements (A-Z)	Description
	Currently active configuration set. Denotes the currently activated configuration set.

UI Elements (A-Z)	Description
	Previously active configuration set. Denotes a previously active configuration set.
	Draft. Denotes a draft, that is, a configuration set that has not yet been activated. The changes in the draft are only applied and saved in Release Control's history after the draft is activated. For details on how to activate a draft, see Save and Apply Configuration Changes.
Activated	Displays the currently activated configuration set.
All	Displays all existing configuration sets and drafts.
Drafts	Displays all existing drafts.
Last Activated By	The name of the user who last activated the draft/configuration set.
Last Activated On	The time and date on which the draft/configuration set was last activated.
Last Modified By	The name of the user who last modified the draft/configuration set.
Last Modified On	The time and date on which the draft/configuration set was last modified.

Save as Draft Dialog Box

This dialog box enables you to create a draft of a new configuration set. A draft is a configuration set that has not yet been activated. It can be edited only until it is first activated. When the draft is activated, the configurations properties are applied to Release Control. For details on how to activate a draft, see Configuration Tab.

If you need to edit a configuration set after it has been activated, you must create a new draft.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Save** in the left pane.
Important Information	You cannot change the name of an existing draft.
Relevant tasks	• Resolve a Configuration Setting Validation Problem • Save and Apply Configuration Changes • Configure Files in the Configuration Tab

User interface elements are described below:

UI Elements (A-Z)	Description
<List of existing drafts>	Displays a list of all existing drafts.
Draft name	Enter a unique name for the new draft.
Last Modified By	The name of the user who last modified the draft.
Last Modified on	The time and date on which the draft was last modified.
Name	The name of the draft.

Change Process Configuration

This chapter includes:

Concepts

- Collision Configuration
- Calculating Change Request Collisions
- Impact Analysis
- Risk Analysis
- Similar Changes Analysis

Tasks

- Configure an Impact Analysis Rule
- Configure Risk Analysis
- Configure the Automatic Creation of Action Items

Reference

- Change Process Configuration User Interface

Concepts

Collision Configuration

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

Determining Which Change Requests to Include in Collision Calculations

You can configure 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 are included in the collision calculation. For details, see Prerequisites Pane.

- Custom filters can include either:
  - Change requests that have specified values for a specified field
  - Change requests that have matching values for a specified field
- You can configure predefined filters to filter the change requests to be included in the collision calculation based on change request status or duration. For details, see Collisions by Field Pane.

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 Release Control identifies and calculates change request collisions in the Types Pane.

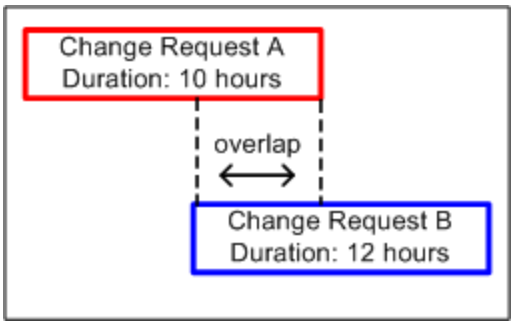
This section also includes:

- Configuring Collision Proximity Levels
- Configuring Causes of Collisions
- Configuring Collisions Severity Levels

Configuring Collision Proximity Levels

The proximity level of two change requests can be defined in one of the following ways:

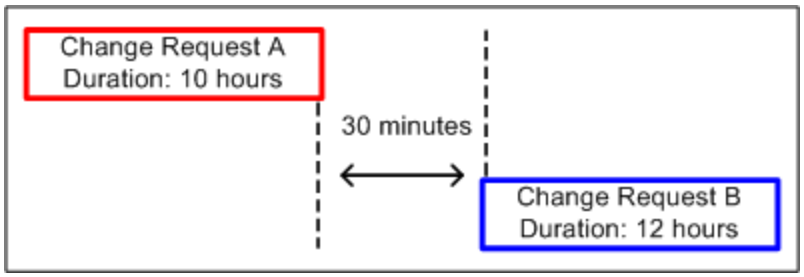
- **Overlap.** The two change requests have overlapping schedules.



- **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** by setting a value for the **Warning ratio** in the Collisions pane. For details on how to configure the **Warning ratio**, see Warning ratio.

When you set a value for the **Warning ratio**, you define the time gap according to which Release Control determines whether two change requests are in close proximity (proximity level of **Overlap Warning**).

Configuring Causes of Collisions

Two change requests in close proximity to each other are not necessarily considered colliding changes.

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 Release Control without 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 a 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.
- **Multi-value string.** Two change requests have one or more common values. For example, a change request containing the values Finance,IT,Application, and a change request containing the values QA,Finance. In this case, they both have the value Finance in common. For information on value delimiters, which enable you to recognize each value in a field as a separate value, see Field Attributes - Field Definitions Tab.

Configuring Collisions Severity Levels

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

Elements Causing Collisions	Proximity Level	
	Overlap	**Overlap Warning**
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**.

Notes:

- If there is more than one element causing a collision, the severity is determined by the collision with the highest severity.
- You can also configure a custom-defined collision severity level by defining one or more fields as collision causes. In this case. 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. For details about specifying fields as collision causes, see Collisions by Field Pane.

You can change the way in which Release Control determines the severity level for any combination of collision cause and proximity level. For details, see Types Pane.

Impact Analysis

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

For information on how to set up and configure Release Control to calculate impact analysis, see Configure an Impact Analysis Rule.

Determining When to Calculate Impact Analysis

Calculating impact analysis uses significant system resources. Release Control can be configured to minimize the instances in which impact analysis is performed to optimize system resource usage.

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.

- You can select the Change Process Pane pane to instruct Release Control to calculate impact analysis for each new change request that was retrieved in initial load.
- Impact analysis is not calculated if the list of Universal CMDB CIs related to the ticket has not changed and the **Calculate impact only if analyzed CIs updated** check box is selected.

> **Note:** You can use the **shouldCalcImpact** function within the **change-flow.js** script (located in **Module** > **Administrator** > **Configuration** tab > **Change Process** > **change flow script**) to instruct Release Control to override the configurations for the **Always calculate impact for initial load** and the **Calculate impact only if analyzed CIs updated** options. For more information about the **change-flow.js** script, see Change Flow Script Pane.

Risk Analysis

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.

For details on the formula Release Control uses to calculate the relative risk value for each request, and a detailed example of the process involved, see Risk Analysis.

This section also includes:

- Configuring Risk Calculation Properties
- Adding Operations before Risk Analysis

Configuring Risk Calculation Properties

You can change the definitions for which risk should be calculated using the **shouldCalcRisk** function within the **change-flow.js** in **Module** > **Administrator** > **Configuration** tab > **Change Process** > **change flow script**.

For example, by default, risk is always calculated for all statuses. You can instruct 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(prevChange, newChange) {

return true;

}
```

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

```
if (prevChange==null)

        shouldCalc= true;
```

You can use the **overrideRisk** function in the **change-flow.js** script to instruct Release Control to override the standard risk calculation. For example, you can instruct 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.

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 affects the risk analysis.

To add operations that need to be performed before each risk analysis, select **Module** > **Administrator** > **Configuration** tab > **Change Process** > **change flow script**. The **preCalcRisk** function within the **change-flow.js** script contains the location in which you can add operations to be performed.

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.

Similar Changes Analysis

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.

Understanding How the Similarity Calculation Works

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, the changes are considered to be similar for the purposes of the Similar Changes feature. If the proximity value is less than the threshold, 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.

For details on how you can customize the way in which Release Control identifies and calculates similar changes, see Similarity Pane.

Tasks

Configure an Impact Analysis Rule

This task describes how to configure an impact analysis rule.

It includes the following steps:

Step 1: Configure CI search directives - Optional

Step 2: Determine when impact analysis is calculated - Optional

Step 3: Configure an analysis rule

Step 1: Configure CI search directives - Optional

By default, when Release Control calculates impact analysis, it searches for changed CIs of the types **host** or **ip**, whose format matches one of the Universal CMDB attributes listed in the **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Universal CMDB** > **CI Analysis Lookup Directive** pane.

You can modify this list if you want Release Control to search for CIs of different types and attributes. For details, see CIs Analysis Lookup Directive Pane.

Step 2: Determine when impact analysis is calculated - Optional

By default, Release Control calculates impact analysis for every ticket that is created. In addition, impact analysis is also recalculated in some cases in which a change was made to an old ticket/change request.

To save system resources, you may decide that calculating impact analysis is not always necessary. To determine when impact analysis is recalculated, select **Module** > **Administrator** > **Configuration** tab > **Change Process** > **change flow script**. The **shouldCalcImpact** function within the **change-flow.js** script contains the protocol which determines when impact must be recalculated. For details on how to determine when impact analysis is calculated, see Determining When to Calculate Impact Analysis.

Step 3: Configure an analysis rule

1. (Optional) Aggregate the CIs of the change requests and its tasks. By default, Release Control calculates the CIs of a task together with the CIs of the parent request. To instruct Release Control to calculate the CIs separately, select **Module** > **Administrator** > **Configuration** tab >

Change Process. In the Change Process pane on the right, clear the **CI Aggregate** check box. For details, see CI aggregated.

2. Define an analysis rule for each CIT you want Release Control to recognize. Select **Module** > **Administrator** > **Configuration** tab > **Change Process** > **Impact Analysis Rules**. In the CI Analysis Rules pane, click the **Add Rule** button. In the CI Analysis Rule Definition pane, configure the new rule. For details on the CI Analysis Rules and CI Analysis Rule Definition panes, see Impact Analysis Rules Pane.
3. Test the new rule you defined. Select **Module** > **Administrator** > **Configuration** tab > **Change Process** > **Impact Analysis Rules**. In the Test Selected Analyzer pane, click the **Test Analyzer** button. For more information on the Test Selected Analyzer pane, see Impact Analysis Rules Pane.
4. Apply the analysis rule to change request fields. Select **Module** > **Administrator** > **Configuration** > **Integrations** > **Fields**. In the Field Attributes pane on the right, click the **Field Attributes - CI Analysis Rules** tab and choose the level (**Change** or **Task**) at which you want to apply the rule. For details, see Field Attributes - CI Analysis Rules Tab.

Configure Risk Analysis

This task describes how to configure risk analysis on a change request.

> **Note:** Since risk analysis depends on other configurations, such as impact analysis, collisions, similar changes, time period conflicts, and so forth, it is recommended that you leave the configuration of risk analysis as the last step in the configuration process.

Step 1: Configure risk calculation properties - Optional

Change the definitions for which risk should be calculated using the `shouldCalcRisk` function within the **change-flow.js** in **Module** > **Administrator** > **Configuration** tab > **Change Process** > **change flow script**. For details, see Configuring Risk Calculation Properties.

Step 2: Add operations before performing risk analysis - Optional

Add operations that need to be performed before each risk analysis using the `preCalcRisk` function within the **change-flow.js** script in **Module** > **Administrator** > **Configuration** tab > **Change Process** > **change flow script**. For details, see Adding Operations before Risk Analysis.

Step 3: Configure a risk factor

Define a **Potential Damage** or **Probability of Failure** risk factor. Select **Module** > **Administrator** > **Configuration** > **Change Process** > **Risk Factors**. In the Risk Factors pane, click either the

Potential Damage or **Probability of Failure** tab and then click the **Add Factor** button. In the Factor Definition pane, configure the new risk factor. For details, see Factor Definition Pane.

Step 4: Test the risk factor - Optional

1. Test the risk factor before saving it by importing sample change requests and running the risk calculations on it. Select **Module** > **Administrator** > **Configuration** tab > **Change Process** > **Risk Factors**. In the Test Risk Factors pane, click the **Add Sample Change Request** button to open the Add Sample Change Requests dialog box. Select sample change requests to test the risk factor. For details, see Risk Factors Pane.
2. Run the test to simulate the risk calculation for all change requests based on your new settings. In the Test Risk Factors pane, click the **Simulate Risk Calculation** button. For details, see Test Risk Factors Pane.

Step 5: Recalculate the Risk Factor - Optional

> **Note:** Before implementing this step, save and apply the new settings you configured by clicking the **Save current editable configuration set** button in the left pane. For details, see Save and Apply Configuration Changes.

Recalculate the risk factor based on your new settings by manually running the recalculation process. For details, see Launch Manual Change Process Dialog Box.

Configure the Automatic Creation of Action Items

By default, Release Control automatically creates action items from certain change requests and assigns these items to specific Release Control users. This task describes how to modify the conditions for the automatic creation of action items **addActionItemsOnChange** function in the **change-flow.js** script.

1. Select **Module** > **Administrator** > **Configuration** tab > **Change Process** > **Change flow script**. Content of this file is displayed in the right pane.
2. Locate the **addActionItemsOnChange** function. By default, the **addActionItemsOnChange** function instructs 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 to or greater than a specified severity and the calculated risk increased beyond a specified threshold, 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);

        }

    }

}
```

3. Modify the following properties, which are assigned to the action item, as required:
   - **Assignee.** By default, the user associated with the business CIs affected by the change request.
   - **Creator.** By default, the 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. (To access the API Reference, select **Start** > **Programs** > **Release Control 9.60** > **Documentation** and open the **pdfs** directory).
4. After making the required modifications, save and apply your changes.

Reference

Change Process Configuration User Interface

This section includes:

- Change Process Pane
- Change Flow Script Pane
- Collisions Pane
- Prerequisites Pane
- Types Pane
- Impact Analysis Rules Pane
- Risk Factors Pane
- Similarity Pane

Change Process Pane

This pane enables you to:

- Specify whether the impact of CIs in tasks (second-level requests) are calculated separately from the changes to which the tasks belong, or included in the impact analysis of the tasks' respective changes. For details, see CI aggregated.
- Configure the preemptive impact feature. For details, see Preemptive impact enabled.
- Modify the request collection frequency as required. For details, see Collection frequency.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Change Process**.
See also	• Working with the Configuration Tab • Configuring Collision Proximity Levels • Types Pane

User interface elements are described below:

UI Elements (A-Z)	Description
Always collect impact for initial load	Release Control always calculates impact analysis for each new change request that is retrieved in initial load.
Calculate impact only if analyzed CIs updated	Release Control recalculates impact analysis only if the list of Universal CMDB CIs related to the ticket is updated.
CI aggregated	Enables you to specify whether the impact of CIs in tasks (second-level requests) are calculated separately from the changes to which the tasks belong, or included in the impact analysis of the tasks' respective changes. By default, an impact analysis of a task triggers 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 instruct Release Control to calculate the CIs separately, clear the **CI Aggregate** check box.
Collection frequency	Describes the interval (measured in seconds) that indicates how often Release Control collects change requests for processing. **Default:** 5
Manual change process	The maximum percentage of processing time dedicated for manual

UI Elements (A-Z)	Description
processing share(%)	change processing. The value of this property determines the balance between processing changes from the Service Desk Integration (SDI) module queue to changes from the manual procedure. For details, see Launch Manual Change Process Dialog Box.
Minimum queue length for preemptive impact	The size of queue that is required for the preemptive impact feature to be activated.
Number of impact calculators	The number of calculators that are used to calculate impact analysis.
Preemptive impact enabled	By default, Release Control processes change requests one at a time because of the possibility of a dependency between changes. As a result, changes pile up in the queue as they wait for their turn to be analyzed. However, since the impact calculation phase is an independent part of the analysis calculation, impact analysis can be run in parallel. Preemptive impact enhances Release Control performance by launching several calculators at a time to precalculate the impact of changes in the queue. By default, the preemptive impact feature is not enabled. Select this check box to enable it.
Suggest time analysis valid statuses	The selected statuses are used to determine whether or not Release Control calculates time suggestion on a change request. For details, see Updating Suggest Time Analysis in Service Manager.

Change Flow Script Pane

This pane contains the **change-flow.js**, which include the functions that allow fine-grained customization and control of the Release Control analysis process, enabling you to introduce business logic down to the field level.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Change Process** > **Change flow script**. **Note:** For details about editing this file, see "Configure Files in the Configuration Tab" on page 181.
Important information	For a detailed explanation of the objects that can be included in the script functions, refer to the **API_Reference.chm** file. (To access the API Reference, select **Start > Programs > Release Control 9.60 > Documentation** and open the **pdfs** directory).

See also	Working with the Configuration Tab

User interface elements are described below:

UI Elements (A-Z)	Description
<Functions included in the change-flow.js script>	• **preChangeProcess** and **postChangeProcess**. Enable you to calculate certain pre-change request processing or post-change request processing factors. For details, see Configure the Analysis of Change Requests. • **shouldCalcImpact.** Enables you to determine when impact analysis is recalculated. For details, see Determining When to Calculate Impact Analysis. • **preCalcRisk.** Enables you to add operations that need to be performed before each risk analysis. For details, see Adding Operations before Risk Analysis. • **shouldCalcRisk.** Enables you to determine for which change request risks should be calculated. For details, see Configuring Risk Calculation Properties. • **overrideRisk.** Enables you to instruct Release Control to override the standard risk calculation. For details, see Configuring Risk Calculation Properties. • **addActionItemsOnChange.** Enables you to modify the conditions for the automatic creation of action items. For details, see Configure the Automatic Creation of Action Items. • **getUsersToNotify.** Enables you to determine which users should get a notification during the change process. For details, see Configuring Notifications Overview. • **shouldCalcSimilar**. Enables you to determine whether or not to calculate similar changes. For details, see Similarity Pane. • **shouldCalcSuggestTime.** Enables you to determine whether or not suggest time analysis is calculated. For details, see Updating Suggest Time Analysis in Service Manager.

Collisions Pane

This pane enables you to include a change request in collision calculations based on the change request duration, and configure the definition of an **Overlap Warning**.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Change Process** > **Collisions**.
See also	• Working with the Configuration Tab

	• Collision Configuration • Calculating Change Request Collisions • Types Pane • Assess > Collisions Tab

User interface elements are described below:

UI Elements (A-Z)	Description
Collision count fuse	The maximum number of collisions for which Release Control calculates collision results. If the number of collisions exceeds the specified value, collision calculation results are ignored. **Note:** Specify 0 to disable the Collision count fuse feature.
Maximum change duration (days)	Enables you to 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, Release Control does not include that change request in collision calculations. Define a new maximum duration value (in days). To disregard change request duration, that is, if any duration is acceptable, set this value to 0. **Default value:** 7 **Note:** By default, a change request is included in collision calculations as long as its duration does not exceed seven days.
Warning ratio	Enables you to configure the definition of an **Overlap Warning**. For a description of what an Overlap Warning is, see Configuring Collision Proximity Levels. By setting a value for the **Warning ratio** option, you define the time gap according to which Release Control determines whether two change requests are in close proximity (proximity level of **Overlap Warning**). **Default value:** 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**.

Prerequisites Pane

This pane enables you to:

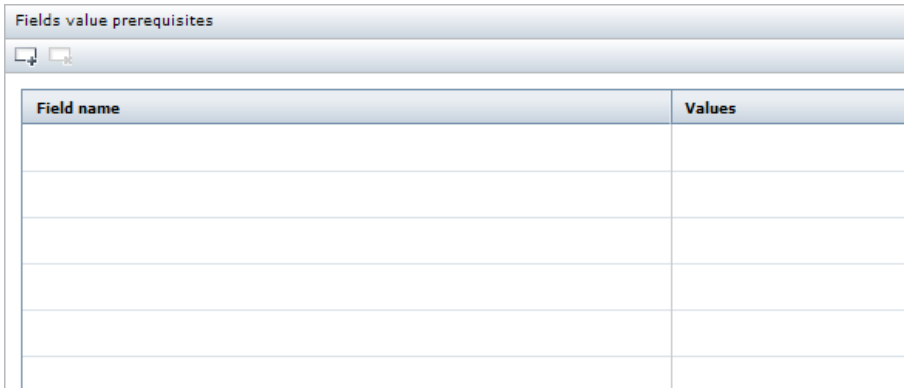
- Determine whether to include a change request in collision calculations based on the change request status.
- Create a custom filter that determines whether a change request is included in the collision calculation. There are two types of custom filters:
  - A custom filter by which only change requests that have specified values for a specified field are included in the collision calculation.
  - A custom filter by which only change requests that have matching values for a specified field are included in the collision calculation.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Change Process** > **Collisions** > **Prerequisites**.
Important Information	If you include both filters, Release Control applies the criteria of both filters to the change requests.
See also	• Working with the Configuration Tab • Calculating Change Request Collisions

User interface elements are described below:

UI Elements (A-Z)	Description
Calculated collision statuses	Enables you to determine whether to include a change request in collision calculations based on the change request status. **Note:** By default, change requests of all statuses are included in collision calculations. Select one or more required change request statuses: • **Pre-approval** • **Pending Approval** • **Approved** • **In Progress** • **Evaluation and Closure** • **Closed** • **Unknown**

Field Value Prerequisites Pane



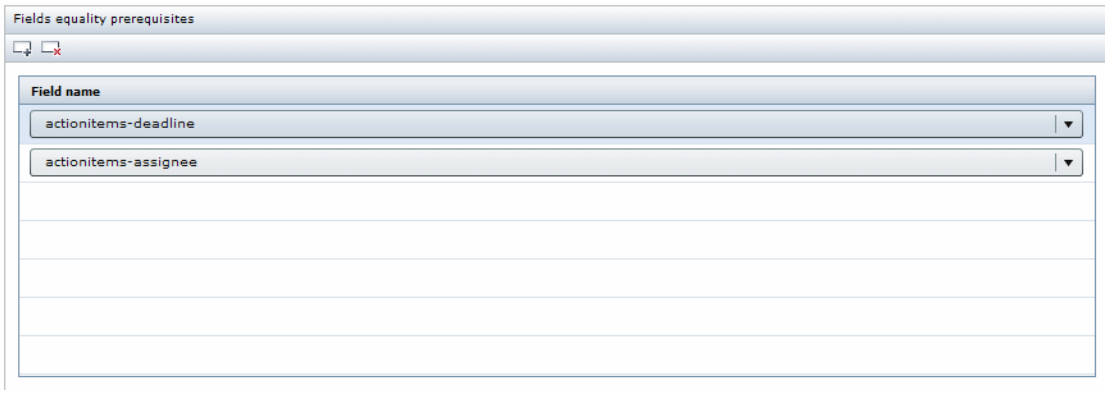
This pane enables you to create a custom filter by which only change requests that have specified values for a specified field are included in the collision calculation.

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, Release Control only calculates collisions among second-level (child) requests.

User interface elements are described below:

UI Elements (A-Z)	Description
	Add configuration to configuration set. Enables you to add another field to be used in the filter.
	Remove configuration from configuration set. Enables you to delete the selected field.
Field name	Select the required field name from the drop-down list. If a change request contains the value specified for this field, the change request is included in the collision calculation.
Value	Enter one or more values for the selected field. If a change request contains the value specified, the change request is included in the collision calculation.

Field Equality Prerequisites Pane



This pane enables you to create a custom filter by which only change requests that have matching values for a specified field are included in the collision calculation. For example, you could use this filter to only include change requests that have matching values for the **region** field. In this case, 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**. Release Control calculates collisions between **NY1** and **NY2** and between **LON1** and **LON2** but it does not calculate collisions across regions, for example, between **NY1** and **LON1**.

User interface elements are described below:

UI Elements (A-Z)	Description
	Add configuration to configuration set. Enables you to add another field to be used in the filter.
	Remove configuration from configuration set. Enables you to remove the selected field.
Field name	Select the required field name from the drop-down list. If the value of the field matches a value in the change request, the change request is included in the collision calculation.

Types Pane

Release Control determines the severity of a collision based on the elements causing the collision and the proximity between the colliding change requests. This pane enables you to change the way in which Release Control determines the severity level for any combination of collision cause and proximity level.

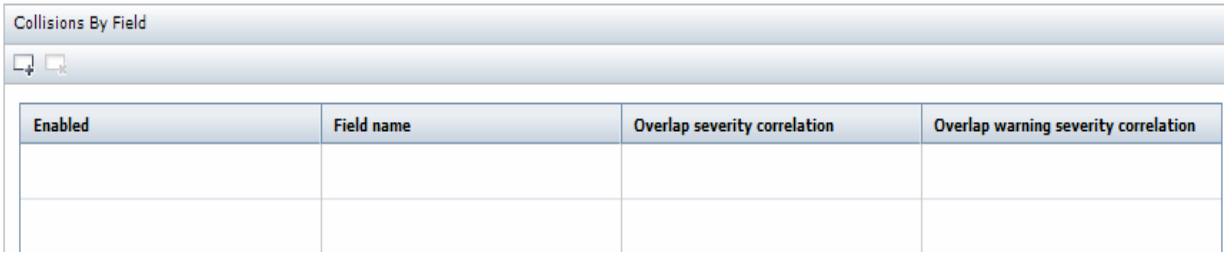
You can configure the default collision severity levels or specify a certain field you want to define as a collision cause.

For each collision cause defined, you specify a proximity level and an associated severity level by defining the following:

- **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.
- **Severity.** The severity level of the collision. For details, see Configuring Collisions Severity Levels.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Change Process** > **Collisions** > **Types**.
See also	• Working with the Configuration Tab • Calculating Change Request Collisions • Collision Configuration

Collisions by Field Pane



This pane enables you to configure a customer-defined collision severity level by specifying the field you want to define as a collision cause. A specified field has the same value in both change requests.

Important Information	• You must enter the field name as it is defined in the Administrator's module's Field tab. For details on defining field names, see Fields Pane. • 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.

User interface elements are described below:

UI Elements (A-Z)	Description
	Add configuration to configuration set. Enables you to add a field you want to define as a collision cause.
	Remove configuration from configuration set. Enables you to delete the selected field.
Enabled	• If selected, the predefined collision type is included in the collision calculations. • If cleared, the predefined collision type is not included in the collision calculations.
Field name	Specify the field you want to define as a collision cause.
Overlap severity correlation	A proximity level indicating that two change requests have overlapping schedules. The severity level of the collision can be defined as **Low**, **Medium**, **High**, **Critical**, or **Unknown**.
Overlap warning severity correlation	A proximity level indicating that two change requests are scheduled in close proximity to one another. The severity level of the collision can be defined as **Low**, **Medium**, **High**, **Critical**, or **Unknown**.

Predefined Collision Types Pane

This pane enables you to configure the default collision severity levels.

User interface elements are described below:

UI Elements (A-Z)	Description
Enabled	• If selected, the predefined collision type is included in the collision calculations. • If cleared, predefined collision type is not included in the collision calculations.

UI Elements (A-Z)	Description
	By default, the predefined collision type containing the **ACI_ACI** type-name is disabled. This means that if two change requests involve a common ACI, Release Control, by default, does not consider this to be a collision. **Caution:** If a predefined collision type is not included in the collision calculations, 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.
Name	The element causing the collision. The following collision causes are defined by default: • **ACI/ACI.** Two change requests involve at least one common affected CI (ACI). • **CCI/ACI.** The same CI is changed by one change and affected by another. • **CCI/CCI.** Two change requests involve at least one common changed CI (CCI). • **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). • **IMPLEMENTOR.** The same implementor is responsible for implementing both change requests.
Overlap severity correlation	A proximity level indicating that two change requests have overlapping schedules. The severity level of the collision can be defined as **Low**, **Medium**, **High**, **Critical**, or **Unknown**.
Overlap warning severity correlation	A proximity level indicating that two change requests are scheduled in close proximity to one another. The severity level of the collision can be defined as **Low**, **Medium**, **High**, **Critical**, or **Unknown**.

Impact Analysis Rules Pane

To analyze the impact of the collected change requests, Release Control must first identify the location and format of the CIs contained in the requests. This is done by the analysis rules. This pane enables you to define the analysis rules you want Release Control to use.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Change Process** > **Impact Analysis Rules**.
Relevant tasks	Configure an Impact Analysis Rule
See also	Working with the Configuration Tab

CI Analysis Rules Pane

This pane contains the list of analysis rules you apply to a change request field. You can edit the fields of the existing rules or add new rules. You configure the fields for rules in the CI Analysis Rule Definition Pane. Release Control must have a separate analysis rule for each CIT that you want to recognize.

Important Information	• The names of the top-level and second-level requests are configurable in **Module** > **Administrator** > **Configuration** tab > **Labels and Terms** > **enumeration-labels.properties** file. For details, see Labels and Terms Pane. • 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 details, see Field Attributes - Field Definitions Tab. • For each analysis rule that you selected, choose the level (**Change** or **Task**) at which you want to apply the rule. For details, see Field Attributes - CI Analysis Rules Tab.

User interface elements are described below:

UI Elements (A-Z)	Description
	Add Rule. Add a new CI analysis rule. **Note:** You configure the fields for the rule. For details, see CI Analysis Rule Definition Pane.
	Delete Rule. Delete an existing CI analysis rule.

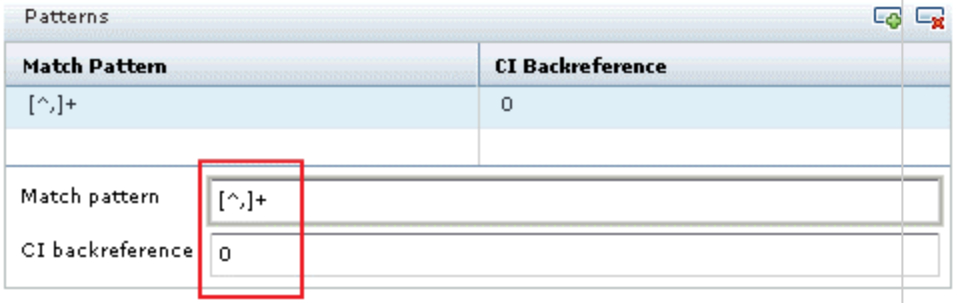
UI Elements (A-Z)	Description
	Refresh and Undo Modifications. If you are not satisfied with your changes, you can undo any changes you made by clicking the **Refresh and Undo Modifications** button before you save your changes. **Note:** When you click this button, all the changes you made since the last time you saved your settings are lost.
	Predefined CI Analysis Rule. Denotes a default rule provided by Release Control.
	Custom CI Analysis Rule. Denotes a user-defined rule.
<Analysis rules>	A list of the available analysis rules. By default, the following analysis rules are available: • **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 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. **Note:** 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 Universal CMDB CIs. • The **mam-ticket** analysis rule locates CIs using change request IDs. **Note:** These rules cannot be edited or deleted.
Description	The description of the CIT. See CI Analysis Rule Definition Pane.
Name	The name of the CIT. See CI Analysis Rule Definition Pane.

CI Analysis Rule Definition Pane

This pane enables you to define an analysis rule. It contains the definitions of the selected rule in the CI Analysis Rules pane.

User interface elements are described below:

UI Elements (A-Z)	Description
	Add Pattern. Add a new pattern.
	Delete Pattern. Delete an existing pattern.
Analyzer class	• If your CIT is **not** IP-Range, select **Use rule name as CI class type**. • If your CIT is IP-Range, select **Use the IP-Range analyzer**.
Description	A description of the CIT that you want Release Control to locate in the collected requests.
Name	The name of the CIT that you want 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. **Notes:** • The name of the CIT must appear as it is defined in **Module** > **Administrator** > **Configuration** tab > **Universal CMDB** > **CIs Analysis Lookup Directive** pane (if you are working with Universal CMDB). For details, see CIs Analysis Lookup Directive Pane. • The **ip-range** analysis rule is an exception to the above specifications, as it corresponds to the **ip** CIT in Universal CMDB.
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. 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 Release Control to use the entire pattern in locating the CI. **To support multi-language characters in CI names:**

UI Elements (A-Z)	Description
	1. Change the **Match Pattern** to [^,]+.  2. Restart the Release Control server for the change to take effect.

Test Selected Analyzer Pane

This pane enables you to manually test analysis rules. You enter a string and run the patterns on it.

User interface elements are described below:

UI Elements (A-Z)	Description
	Test Analyzer. Tests the analysis rule.
All patterns	Enables you to perform the test using all defined patterns.
Match candidate with UCMDB	When the test is run, the ticket text is broken up into strings. This option instructs Release Control to check these strings for valid CIs using Universal CMDB.
Selected pattern	Enables you to perform the test using the selected pattern.
Test value	Enter a string to test the analysis rule. The test results appear in the graph window, which is accessed from the Analyzed CIs pane.

Analyzed CIs Pane

User interface elements are described below:

UI Elements (A-Z)	Description
	Open Graph Window. Opens the Impact Graph window. Displays a visual representation of the impact relationships of the selected change request. For details on the Impact Graph Window, see Impact Graph Window.

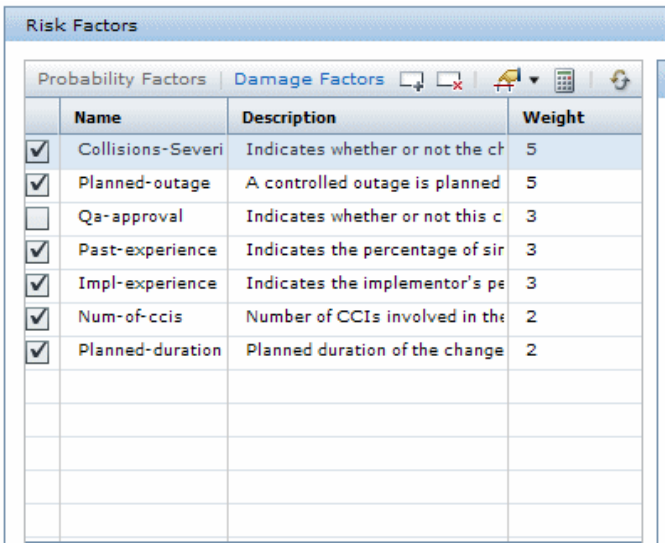
UI Elements (A-Z)	Description
	Note: This button is enabled when the string entered in the **Test Value** box contains one or more CIs from Universal CMDB.

Risk Factors Pane

This pane enables you to define risk factors to be used in the risk calculation.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Change Process** > **Risk Factor**.
Relevant tasks	Configure Risk Analysis
See also	• Working with the Configuration Tab • Risk Analysis

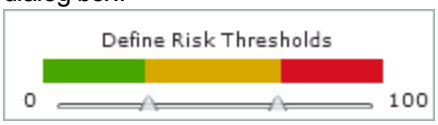
Probability/Damage Factors Pane



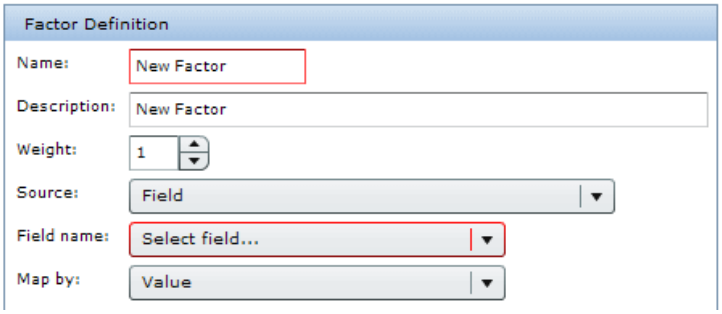
This pane contains a list of the available **Potential Damage** and **Probability of Failure** risk factors. When you select a risk factor in the table, the definitions of that risk factor are displayed in the Factor Definition pane.

Important Information	For a risk factor to be included in the risk calculation, the check box next to the risk factor must be selected.

User interface elements are described below:

UI Elements (A-Z)	Description
	Add Factor. Creates a risk factor. Select either the **Damage Factors** or **Failure Probability** tab, depending on the type of risk factor you want to create or modify. You define or modify the risk factor properties in the Factor Definition pane.
	Delete Factor. Deletes an existing risk factor.
	Risk Thresholds. When risk factors are calculated, the risk factor's numeric value is associated to a risk level (**low**, **medium**, or **high**). This button enables you to configure which numeric values correspond to which levels. Opens the **Define Risk Thresholds** dialog box.  • The green section corresponds to the **low** risk level. • The yellow section corresponds to the **medium** risk level. • The red section corresponds to the to **high** risk level. Drag and drop the arrows to adjust the thresholds for each level. **Note:** If you change the thresholds, these changes will only be effective for new change requests that enter Release Control. Existing change requests will maintain the risk level that they were assigned when they entered the system.
<Factor weight distribution pie chart>	Displays a graphic representation of the weight of each factor in the risk calculation.
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.
Name	The name of the risk factor. This is the name displayed in the Analysis module's **Risk** tab.
Weight	The relative weight of the risk factor to be used in the risk calculation.

Factor Definition Pane

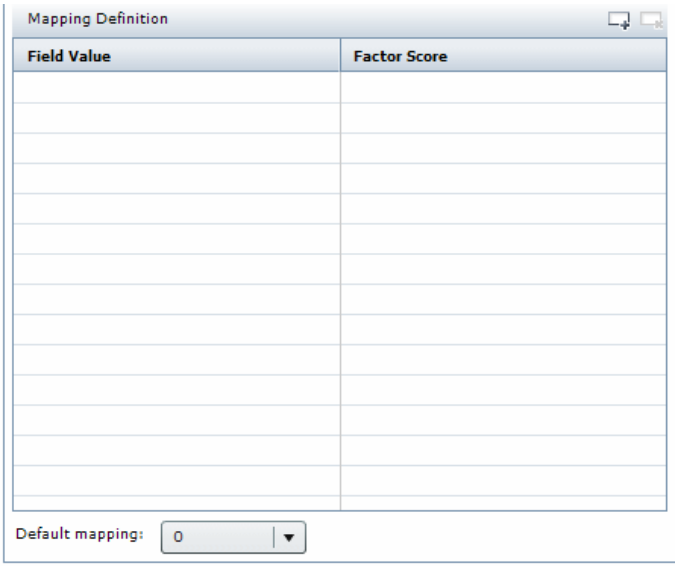


This pane enables you to define or modify the properties of the risk factor selected in the Risk Factors pane.

User interface elements are described below:

UI Elements (A-Z)	Description
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.
Field name	A specific change request field whose data originates in the service desk application. If you have chosen **Field** as your source of data, select the name of the required change request field.
Name	The name of the risk factor. This is the name displayed in the Analysis module's **Risk** tab.
Map by	You can map either 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.
Source	Choose the required source used in creating the risk factor. For a list of the data sources you can use and their description, see Data Sources Used in Creating a Risk Factor.
Weight	The relative weight of the risk factor to be used in the risk calculation.

Mapping Definition Pane



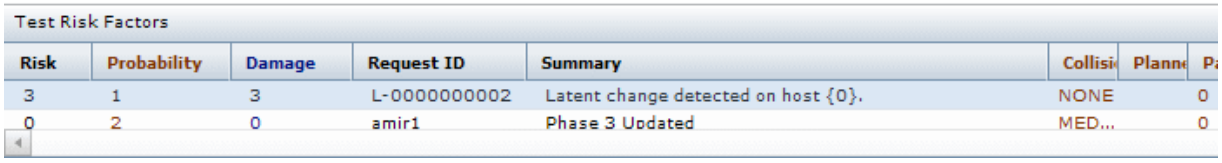
This pane enables you to define mapping rules for the selected risk factor that translate the source data into factor values between **0** and **10**.

Important Information	• The columns that appear in this pane depend on the source used to create the risk factor in the Factor Definition pane. • 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 details, see the Test Risk Factors pane below.

User interface elements are described below:

UI Elements (A-Z)	Description
	Add Entry. Creates a new mapping definition entry. You can define the mapping definitions in the new row that is created.
	Delete Entry. Deletes an existing mapping entry.
Default mapping	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**.

Test Risk Factors Pane



This pane enables you to test risk factors before saving them by importing sample change requests and running the risk calculations on them. Simulating risk calculations can help you understand the implications of your risk factors before deciding whether or not to save them.

User interface elements are described below:

UI Elements (A-Z)	Description
	Add Sample Change Requests. Enables you to 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. Select one of the following options from the Add Sample Change Requests dialog box that opens: • **By change request ID.** Enter the ID of the change request you want to use for the simulation. • **By Filter.** Select the change requests that are included in a specific filter. **Note:** Only the first 10 requests of the specified filter are displayed in the Test Risk Factors pane.
	Delete Selected Sample Change Request. Deletes the selected sample change request.
	Simulate Risk Calculation. Runs the test on the change requests and updates the risk calculations. 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.

Data Sources Used in Creating a Risk Factor

This section contains a list of the data sources in the **Source** list in the Factor Definition pane, from which you can choose to create or modify a risk factor.

- **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.

- **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.

- **Planned Duration (Hours).** The planned duration of the change request (from the planned start to the planned end). This is calculated by Release Control.
- **Number of CCIs.** The number of CIs that are directly affected as a result of the change request. This is calculated by Release Control.
- **Importance of:**
  - **Directly affected business CIs.** The overall importance of the business CIs that are directly affected by the change.
  - **Indirectly affected business CIs.** The overall importance of the business CIs that are indirectly affected by the change.

  > **Note:** When using Universal CMDB 10.20, the Business Criticality attribute is defined in Universal CMDB. If you defined the importance level in Release Control working with Universal CMDB 7.x and upgraded to 10.20 or later, you can use the **ApplicationImportanceExporter.bat** utility to export the Business Criticality attribute from Release Control to Universal CMDB. For details, see Export Application Importance.

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

  > **Note:** Release Control does not support risk factor calculations of time periods that were defined in versions earlier than 4.10.

Similarity Pane

This pane determines which common elements 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.

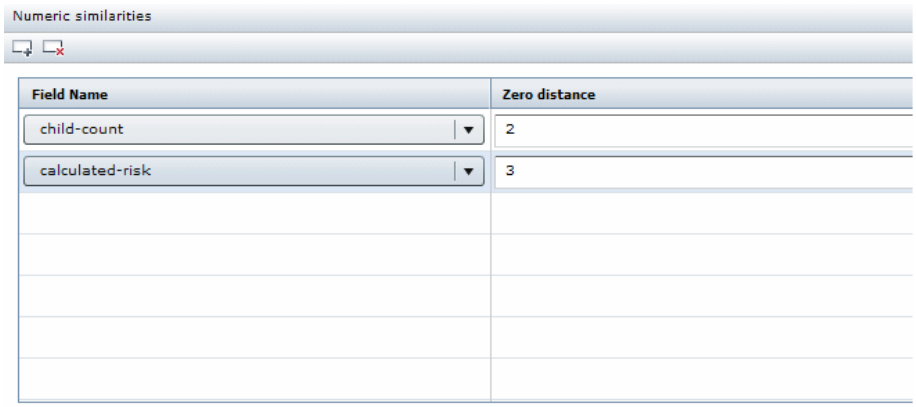
To access	Select **Module** > **Administrator** > **Configuration** tab > **Change Process** > **Similarity**.
See also	• Working with the Configuration Tab

	• Similar Changes Analysis

User interface elements are described below:

UI Elements (A-Z)	Description
Enable similarity analysis	Enables/disables the Similar Changes calculation.
Changed CIs set enabled	Determines whether or not the change CIs set is a part of the similarity calculation.
Directly affected business CIs set enabled	Determines whether or not the directly affected business CIs set is a part of the similarity calculation.
Indexing frequency	Describes the interval (measured in seconds) that indicates how often the similarity index is updated. **Default:** 300
Similarity based on text field	Select the common elements 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.
Threshold	Defines the minimum level of proximity between requests that can be considered similar. You enter a value that is greater than **0** and less than or equal to **1**, 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.

>Numeric Similarities Pane



This pane enables you to define the range in which numeric values between changes are to be considered similar.

User interface elements are described below:

UI Elements (A-Z)	Description
	Add configuration to configuration set. Enables you to add a numeric field.
	Remove configuration from configuration set. Enables you to delete the selected field.
Field name	Select the required numeric field as defined in your system settings.
Zero distance	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 changes that have risk value greater than **5** and less than **15** get non-zero proximity.

Creating In-House Documentation

This chapter includes:

Concepts

- In-House Documentation Overview

Reference

- In-House Documentation Pane

Concepts

In-House Documentation Overview

The In-House Documentation feature enables you to add your own customized documentation (text or a URL) to the existing online help.

Users access this documentation by clicking the **help** button in the relevant area of the product. A link to a page displaying your documentation appears in the product Help under the heading **In-House Documentation**.

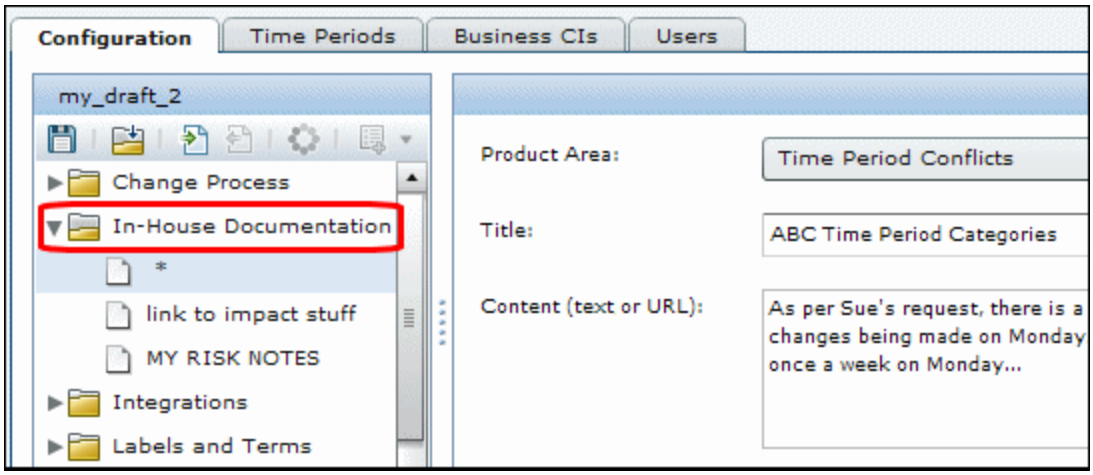
You create in-house documentation in the **Administrator** module In-House Documentation pane. For details, see In-House Documentation Pane.

Example:

John is an Release Control administrator in organization ABC. Sue, the Web administrator tells John that she will be performing Website maintenance every Monday and asks John to create a time period category in Release Control that restricts anybody from making changes to the company's Web site on Mondays.

John creates a time period category called **Web_blackout**. When Release Control users go into the Analysis module **Asses > Time Period Conflicts** tab, they may discover that their scheduled change is in conflict with this **Web_blackout** time period. John wants a way of explaining to users why this time period category exists and decides to write in-house documentation.

He goes into the In-House documentation pane, (**Module** > **Administrator** > **Configuration tab** > **In-House Documentation**), he selects **Time Period Conflicts** from the **Product Area** pane, and he submits the documentation by filling out the required fields and saving his changes:



When users go into the Analysis module **Asses > Time Period Conflicts** tab and click the **help** button , a link to John's documentation explaining the new time period is displayed in the product help.

When users click the link, it opens in a separate page displaying the content that John submitted. John could have also decided to document the time period on the internal company Web site and instead of submitting text in the In-House documentation pane, he could have inserted a URL. In this case the link would open the URL directly.

Reference

In-House Documentation Pane

This pane enables you to add your own customized documentation (text or a URL) to the existing online product help.

To access	• Select **Module** > **Administrator** > **Configuration** tab > **In-House Documentation**. • To add a new topic, select the **In-House Documentation** node and click the **Add configuration to configuration set** button in the left pane.
See also	In-House Documentation Overview

User interface elements are described below:

UI Elements (A-Z)	Description
Product Area	Select the area of the product to which you want to add your own in-house documentation. Users access this documentation by clicking the **help** button in the relevant area of the product (usually one of the tabs in the Analysis module). A link to a page displaying your documentation appears in the product Help under the heading **In-House Documentation**.
Title	The text you enter in the title is displayed in the link that opens your in-house documentation. This text also appears as the heading of your in-house documentation page.
Content	• If you want to link to an existing page, enter the URL of that page. The URL must include "http://". • If you want to create a new page, enter the content of the page as either plain text or HTML.

Field and Enumeration Setting Configuration

This chapter includes:

Concepts

- Field Configuration
- Enumerations Overview

Reference

- Valid Display Formats
- Preconfigured Change Request Fields
- Field and Enumeration Settings Configuration User Interface

Concepts

Field Configuration

You can configure the change request fields for which you want to view data in the Release Control application. You can define the properties of each field in the Fields pane in the **Administrator** module, and the way in which the field appears in your application. For details about how to configure the change request fields, see Fields Pane.

> **Note:** For a list of pre-configured change request fields included in Release Control, see Preconfigured Change Request Fields.

In Release Control, service desk adapters are used to retrieve change requests from the originating service desks and to convert these requests from their service desk application formats to a generic format. The conversion scripts within the service desk adapters are responsible for mapping fields from the originating service desk to corresponding Release Control fields. For more information, see Writing Conversion Scripts.

Enumerations Overview

Release Control contains a default application display mapping scheme which defines the enumeration fields to be used and the order in which the enumeration entries are displayed.

You can modify the way in which Release Control displays each of the enumeration fields and the default order display.

Example:

You can define the priority levels for the **Priority** column in the Change Request pane as follows:

Low	**1**
Normal	**2**
High	**3**
Immediate	**4**

In this case, when you sort the priority levels in ascending order in this column:

- All the change requests that have a **Low** priority appear in the first group
- All the change requests that have a **Normal** priority appear in the second group
- All the change requests that have a **High** priority appear in the third group
- All the change requests that have an **Immediate** priority appear in the fourth group

Start	Priority ▲	Status
10/14/09	Low	Closed
10/15/09	Low	Closed
09/26/09	Low	Closed
10/06/09	Normal	Closed
10/09/09	Normal	Closed
10/02/09	Normal	Closed
09/16/09	Normal	Closed
10/12/09	Normal	Closed
10/07/09	High	Closed
11/04/09	High	Closed
10/30/09	High	Closed
10/15/09	High	Closed
11/04/09	Immediate	Closed

For details on how to modify the way in which Release Control displays each of the enumeration fields and the default order display, see Enumerations Pane.

> **Caution:** If you modify an enumeration setting, all the conversion scripts that refer to this enumeration setting must be modified accordingly. For details on referring to enumeration settings within conversion scripts, see Writing Conversion Scripts. If you modify the way in which the enumeration setting is displayed in the Release Control application, you need not modify your conversion scripts.

Preconfigured Change Request Fields

Release Control contains a default set of pre-configured 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 Release Control.

This section includes:

- Predefined Fields
- Custom Fields

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 Release Control:

Name	Description
actionitems-assignee	The user to whom the action items were assigned.
actionitems-creator	The user who created the action items.
actionitems-deadline	The day by which the creator determined that the action items must be completed.
actionitems-modified	The date (including the day and hour) on which the action item was last modified.
actionitems- pending	The user whose action is being awaited
actionitems- priority	The priority levels of the change requests.
actionitems- status	The statuses of the change requests.
actual-end-time	The actual change activity's completion time.
actual-start-time	The actual change activity's start time.

Name	Description
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.
calculated-risk-severity	Based on the value of the **calculated-risk** field, this field maps to enum values of **Low**, **Medium**, or **High**.
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 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 Release Control.
is-abnormal	Used to determine if a change request is considered normal in terms

Name	Description
	of the time period in which it was or should be implemented.
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-end-date	The latest date by which to implement 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's (the person who opened the request ticket) satisfaction of 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).
source-itil-entity	The ITIL entity out of which the change request was created (incident, problem, requirement).
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 Release Control analysis features. The following **Custom** fields are included in 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 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.
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.
scheduled-downtime-end	The change activity's planned downtime end time.

Name	Description
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.
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.

Reference

Valid Display Formats

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

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

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%%** returns 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 is displayed

Display Type	Display Format
	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**, use the following date format: `EEE DD MMM YYYY LL:NNA`
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.

Field and Enumeration Settings Configuration User Interface

This section includes:

- Enumerations Pane
- Fields Pane

Enumerations Pane

This pane enables you to define the enumeration values for the fields used by Release Control and the order in which the enumeration entries are displayed in the drop-down lists.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Enumerations**.
Important Information	If you modify an enumeration setting, all the conversion scripts that refer to this enumeration setting must be modified accordingly. For details on referring to enumeration settings within conversion scripts, see Writing Conversion Scripts. If you modify the way in which the enumeration setting is displayed in the Release Control application, you need not modify your conversion scripts.
See also	• Working with the Configuration Tab • Enumerations Overview

User interface elements are described below:

UI Elements (A-Z)	Description
	Add configuration to configuration set. Enables you to add an enumeration entry for the selected field.
	Remove configuration from configuration set. Enables you to delete an enumeration entry for the selected field.
Default entry name	The initial default value.
Name	The name of the enumeration entry for the selected field.
Unknown entry name	The value that is provided for an unknown state.
Value	The numeric value that determines the order in which the enumeration entries are displayed in Release Control.

The Enumerations panes are described below:

UI Elements (A-Z)	Description
ActionItemPriority	A priority assigned to the request by the user creating the action item in the Add/Edit Action dialog box. For details, see Add/Edit Action Item Dialog Box.
ChangeType	The type of change. For details, see Change Type Matching CI Type Pane.

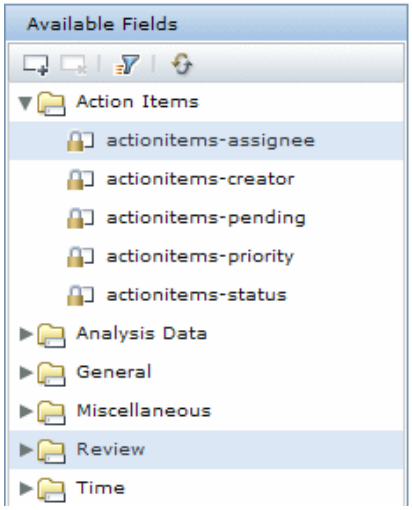
UI Elements (A-Z)	Description
CustomerSatisfaction	The customer (the person who opened the request ticket) satisfaction level of the change request. For details, see the Post Implementation Review Dialog Box.
EstimatedRisk	The risk level of the change request as evaluated by the creating user. For details, see the Preview > Details Tab.
ImplementingOutcome	The level of the implementation outcome as evaluated by the implementor. For details, see Report Activity As Finished Dialog Box.
Level	The level (**Change** or **Task**) at which you want to apply each analysis rule.
Opinion	The votes posted by discussion initiators for a change request. For details, see New Discussion Thread Dialog Box.
Outcome	In the Director module, the possible outcome options from which you can choose in the **Outcome** box when updating the Actual end activity status. For details, see Activity Information Dialog Box.
PlanningSatisfaction	The level of planning satisfaction for the change request from the drop-down list in the Post Implementation Review Dialog Box.
Priority	The Release Control priority level of an action item, activity, or change request.
Severity	The severity level of a collision. For details, see Assess > Collisions Tab.
Status	The status of a change request.

Fields Pane

This pane enables you to configure change request fields for which you want to view data in the Release Control application.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Fields**.
See also	Working with the Configuration Tab

Available Fields Pane



This pane contains a list of all the change request fields. A field selected in this pane can be modified in the Field Attributes pane. For filtering purposes, fields are organized into the following default categories: **Action Items, Analysis Data**, **General**, **Miscellaneous**, **Review**, and **Time**. Fields defined as filterable appear in the Activity/Change Request Filter dialog box (see Activity/Change Request 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.

User interface elements are described below:

UI Elements (A-Z)	Description
	Add Field. Creates a new field. You configure the fields in the Field Attributes pane.
	Delete Field. Deletes an existing field. • You can delete Custom fields that are provided by 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 Release Control application, cannot be deleted. **Note:** The field is only deleted once you create a new configuration set and then save it. For details on how to create a new configuration set, see "Configuration Tab" on page 184. 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.

UI Elements (A-Z)	Description
	Caution: When you delete a change request field, all data related to the field is removed.
	Manage Quick Filter Display. Enables you to define which fields appear in the Filters pane in the Analysis module. Opens the Quick Filter Display dialog box. For details, see Quick Filter Display Pane. For details on the Filters pane, see Quick Filter Display Pane.
<Available Fields>	There are two types of change request fields that appear in this pane: • **Predefined fields.** Denotes a field based on ITIL standards, which are common to most service desk applications. Some of these fields are integral to the proper functioning of the 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.** Denotes a field that is recommended for use to optimize 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 Release Control.

Field Attributes - Field Definitions Tab

This pane enables you to define or modify basic properties of the field.

Important Information	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.

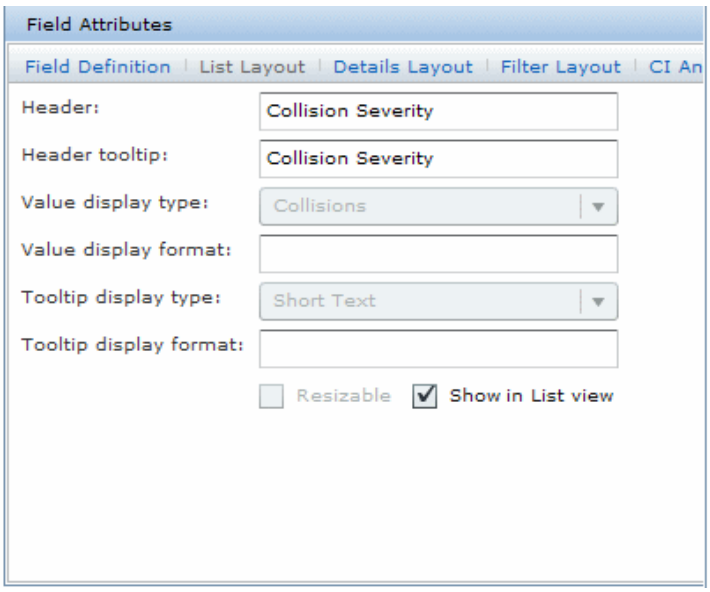
User interface elements are described below:

UI Elements (A-Z)	Description
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**

UI Elements (A-Z)	Description
	CIs or **Union Filters** filter categories.
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.
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.
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.
Listable	Indicates whether the selected field is of a type that can be displayed in the Analysis module's List view. **Note:** This check box is not editable.
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:** When you define a customized field (except for fields of type **Long Text**), a new column is added to the Release Control database for this field. Data for **Long Text** fields is stored in a different table.
Sample value	Enables 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:** You 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).
Sortable	Indicates whether 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.

UI Elements (A-Z)	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. > **Note:** For custom fields, the maximum length of the string depends on the language used. For example, the maximum length available for English is 2000 characters. For Asian languages, it is 500 characters. • **Long Text.** The request field's value is a simple text string with an unlimited number of characters. > **Note:** 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.
Value Delimiter	Enables the filter to recognize each value in a field as a separate value, such as in a multi-value string. In the following example, a "," (comma) is used as a delimiter to separate the values that appear in the following string: `Finance,IT,Application` > **Note:** This field is only available when using the **Short Text** field value type.

Field Attributes - List Layout Tab



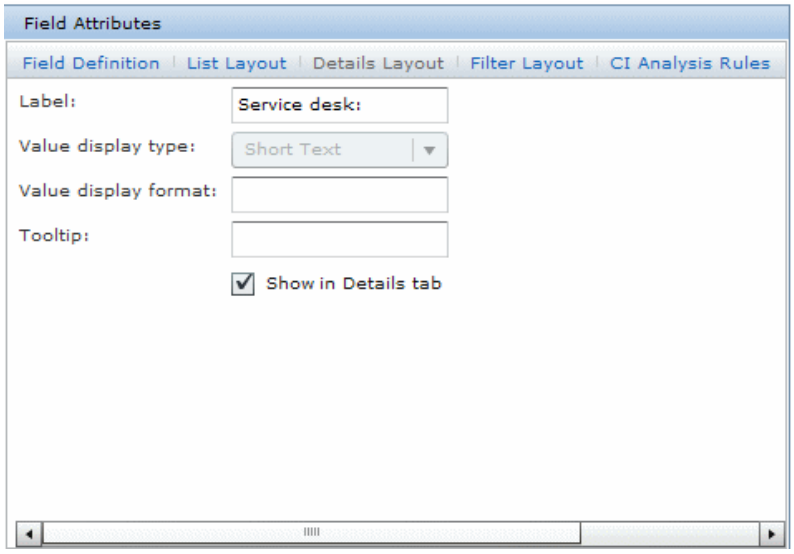
If the **Listable** check box in the Field Definition tab is selected, this pane enables you to define the way in which the field appears in the Analysis module's List view. For details, see Change Requests - List View.

User interface elements are described below:

UI Elements (A-Z)	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 appears 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.
Resizable	Indicates whether the column width is adjustable. For more information about resizing columns, see <Bottom Pane> - List tab.
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 <Bottom Pane> - List tab pane displays a preview of the way in which the field appears in List view. To see how a sample value is displayed, type a sample value in the Field Definition tab's **Sample value** box.
Tooltip display format	The text and format of the tooltip that appears when you hold your cursor over the field value. For information about valid formats for each value type, see Valid Display Formats.
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.
Value display format	The format in which the field appears. For information about valid formats for each value display type, see Valid Display Formats.

UI Elements (A-Z)	Description
	Note: You cannot define a value display format for Boolean value display types.
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.

Field Attributes - Details Layout Tab



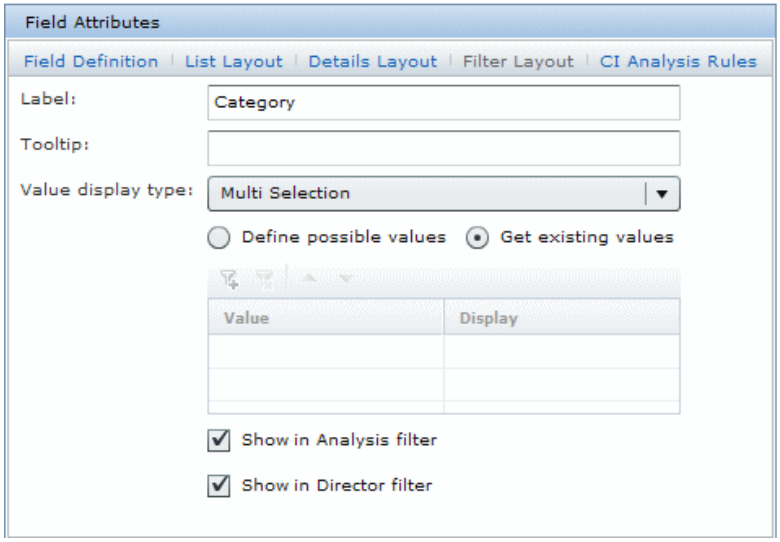
This tab enables you to define the way in which the field appears in the Analysis module's Preview > Details tab. For details, see Preview > Details Tab.

User interface elements are described below:

UI Elements (A-Z)	Description
Label	The text to appear as the label preceding the displayed field value in the Preview > Details tab.
Show in Details tab	Indicates whether the field should be displayed in the Analysis module's Preview > Details tab.

UI Elements (A-Z)	Description
	Note: If you select **Show in Details tab**, the Preview pane displays a preview of the way in which the field appears 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.
Tooltip	The text of the tooltip that appears when you hold your cursor over the label.
Value display format	The format in which the field appears. For information about valid formats for each value display type, see Valid Display Formats. **Note:** You cannot define a value display format for Boolean or Long Text value display types.
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 wraps. • **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.

Field Attributes - Filter Layout Tab



If the **Filterable** check box in the Field Definition tab is selected, this tab enables you to define the way in which the field appears in the Activity/Change Request Filter Dialog Box.

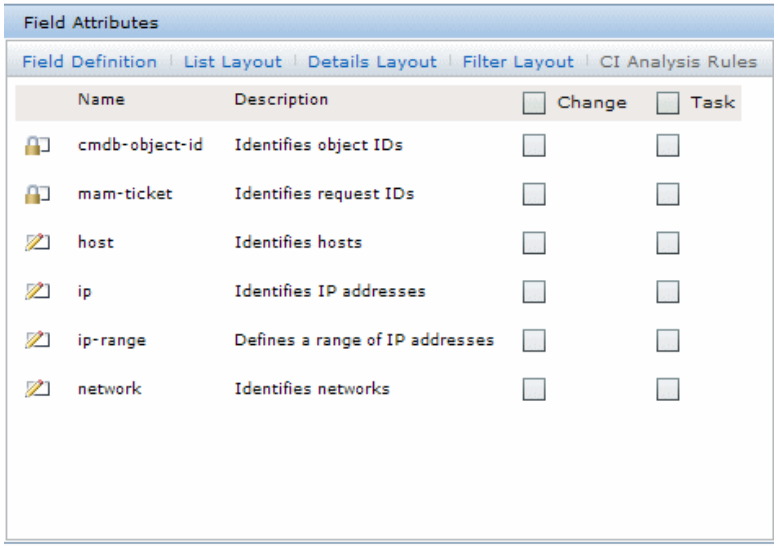
User interface elements are described below:

UI Elements (A-Z)	Description
	Add Filter Value. Enables you to 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. **Note:** This button is only available when you select **Single Selection**, **Multi Selection** or **Editable Selection** from the **Value display type** list and then the **Define possible values** option.
	Delete Filter Value. Delete an existing filter value.
	Move Up and **Move Down**. Changes the order in which the filter values appear in the drop-down list box.
Define possible values	Enables you to 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. If you select this option, you must define the filter value options you want the drop-down list box to contain. To define a value, click the **Add Filter Value** button. **Note:** This button is only available when you select Single Selection, Multi Selection, or Editable Selection from the Value display type list and then the Define possible values option.

UI Elements (A-Z)	Description
Display	Enter the display label of the value.
Get existing values	Instructs Release Control to get the values to be displayed in the drop-down list box directly from the database. **Note:** This option is only available when you select **Single Selection**, **Multi Selection** or **Editable Selection** from the **Value display type** list.
Label	The text to appear as the label preceding the displayed field value in the Activity/Change Request Filter dialog box. For details, see Activity/Change Request Filter Dialog Box.
Show inAnalysis Filter	Indicates whether the field appears as one of the filter criteria in the Analysis module.
Show in Director Filter	Indicates whether the field appears as one of the filter criteria in the Director module.
Tooltip	The text of the tooltip that appears when you hold your cursor over the label.
Value	Enter the required value of the option.
Value display type	Determines the way in which the selected field operates 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. This option 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 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 are a 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

UI Elements (A-Z)	Description
	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.

Field Attributes - CI Analysis Rules Tab



This tab enables you to apply analysis rules to the change request field. These are the rules according to which you want Release Control to identify the location and format of CIs contained in the field's text.

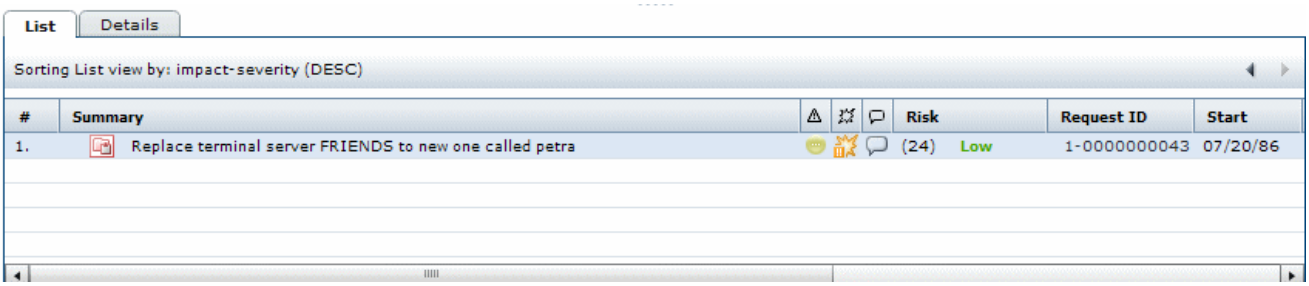
For each analysis rule that you selected, choose the level (**Change** or **Task**) at which you want to apply the rule.

Important Information	• 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. • You can select both **Change** and **Task** if you want the analysis rule to apply to all requests in which the selected field appears. • If any field is invalid, an icon is displayed in the Available fields pane next to the invalid field.

User interface elements are described below:

UI Elements (A-Z)	Description
<CI analysis rules>	A list of the available analysis rules. By default, the following analysis rules are available: • **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 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. 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 Universal CMDB CIs. • The **mam-ticket** analysis rule locates CIs using change request IDs. These rules cannot be edited or deleted. **Note:** The CI Analysis Rules tab contains all the analysis rules specified in the CI Analysis Rules pane in Administrator > Configuration tab > Change Process > Impact Analysis Rules > CI Analysis Rules pane. When you add a rule to the CI Analysis Rules pane, it appears as the last rule in the CI Analysis Rules tab.
Change	The analysis rule is applied to the field only when the field belongs to a top-level request.
Description	A description of what the analysis rule does.
Name	The name of the analysis rule.
Task	The analysis rule is applied to the field only when the field belongs to a second-level request.

<Bottom Pane> - List Tab

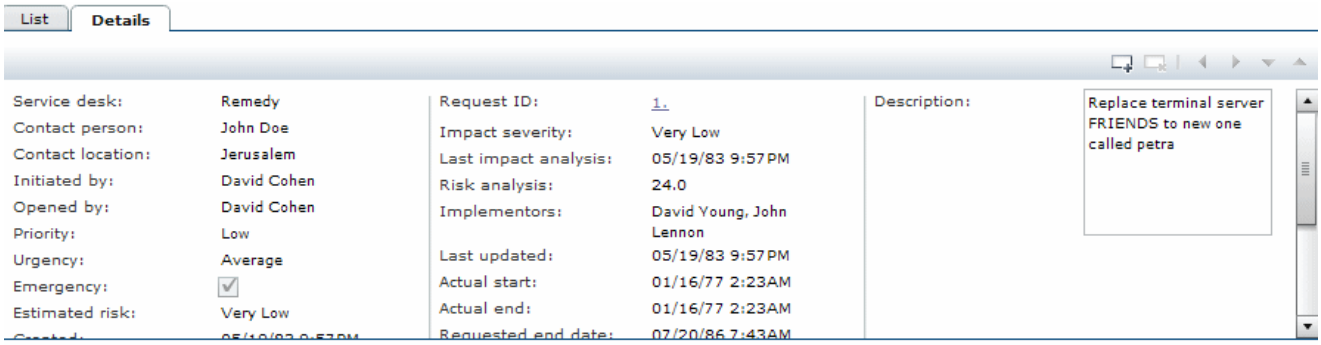


This tab enables you to customize the layout of the Analysis module's List view. The fields in this tab are those for which you selected the **Show in List view** option in the List Layout tab.

User interface elements are described below:

UI Elements (A-Z)	Description
	Enables you to determine 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.
<Adjust the column width>	Enables you to adjust the width of a column. 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:** You can adjust the width of the column only if you selected **Resizable** for the selected column in the List Layout tab.
<Sort the List view according to a specific column>	Enables you 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:** You can select a column to sort by only if you selected **Sortable** for the column in the Field Definition tab.

<Bottom Pane> - Details Tab



This tab enables you to customize the layout of the Analysis module's Preview > Details tab. The fields in this tab are those for which you selected the **Show in Details tab** option in the Details Layout tab is displayed. You can add or delete columns, as well as move a selected field to a different column.

User interface elements are described below:

UI Elements (A-Z)	Description
	Add column. Enables you to add additional empty columns to be displayed in the Preview > Details tab.
	Delete column. Enables you to delete a column. **Note:** To delete a column, you need to select the relevant column by clicking inside the column—but not on a particular field—until the whole column is highlighted. The fields that were included in this column move over to another column.
	Move Rightor **Move Left**. Enables you to move the field to a different column by selecting the relevant field and clicking either the **Move Right** or **Move Left** button.
	Move Up or **Move Down**. Enables you to move the fields up or down within the columns by selecting the relevant field and clicking either the **Move Up** or **Move Down** button.

Universal CMDB-Related Setting Configuration

This chapter includes:

Concepts

- Configuring Universal CMDB-Related Settings Overview
- Working in Standalone Mode Overview
- Configuring Latent and Detected Changes
- Configuring Impact Analysis (Correlation) Rules
- Release Control Federation Adapters Overview
- The Change Federation Adapter

Tasks

- Configure Universal CMDB 10.20 or Later
- Increase the Number of CI Property Conditions forImpactAnalysis using the JMX Console
- Configure Advanced Universal CMDB Settings
- Upgrade the Universal CMDB Version
- Manually Configure Universal CMDB Patches
- Configure Release Control to Work in Standalone Mode
- Configure KPIs as Federated in Business Availability Center 8.x or Business Service Management 9.x
- Add Custom Fields to the Federation Adapter
- Encrypt a Password Using the JMX Console
- Configure Release Control and Universal CMDB to Work with LDAP Using the JMX Console
- Import Business CIs from Universal CMDB

Reference

- Integration Configuration User Interface

Concepts

Configuring Universal CMDB-Related Settings Overview

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

Notes:

1. During the change process, Release Control may return the following (sample) error that is written to the **<Release Control installation directory>\server-0\logs\cmdb-90\cmdb-90_general.log** file:

   ```
   Caused by:

   com.mercury.topaz.cmdb.shared.tql.exception.TqlValidationException:
   [ErrorCode [122] Properties condition exceeded maximum variables
   allowed]

   Properties condition exceeded maximum variables allowed! number of vars:
   100 maximum vars allowed :50
   ```

   If this exception occurs, you need to increase the maximum number of variables allowed for impact analysis using the Universal CMDB JMX console 9.01 (see Increase the Number of CI Property Conditions forImpactAnalysis using the JMX Console). Ensure that you update the maximum number allowed to the number written in the error message. In the example above, it is 100. Setting the maximum to larger than that may affect the performance of Universal CMDB.

2. For information about settings that must be configured for Universal CMDB to interact with Release Control, see the *Release Control Deployment Guide*.

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

Working in Standalone Mode Overview

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

In a regular Release Control deployment, when your service desk application is synchronized with the CMDB server, 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 **cmdb-mock.js**script to configure how Release Control identifies CIs and how the CIs are used in impact analysis calculations.

To configure Release Control to work in standalone mode, see Universal CMDB Pane.

To configure the **cmdb-mock.js**script, see Configure Release Control to Work in Standalone Mode and Standalone Universal CMDB Script Pane.

Configuring Latent and Detected Changes

Release Control contains all the changes that are scheduled to take place in your environment.

If you are working with Universal CMDB, you can configure it to periodically discover actual changes to your environment and send data about these changes to 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 Release Control (**scheduled changes**).

For information on how to configure the latent change feature, see Latent Changes Pane.

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 (**LATENT_AND_DETECTED** mode) is fully activated. For more information about the different work modes, see Latent Changes Pane.

When a change is discovered, Release Control tries to match the discovered change with scheduled changes according to the following criteria:

- **Time period.** 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, 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, Release Control checks whether the changed CI (CCI) in the discovered change is the same as the scheduled change. If the CCI's are not the same, 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), 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 hardware or software (by default either **HW_ADD** or **SW_ADD**).

> **Note:** To ensure that the system does not disregard latent changes due to an unknown value for **change-type- orig** field, add this field to the **convertChange.js** file, located in **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Service Desk Adapters** > **<service desk application>**.

For more details, see Change Type Matching CI Type Pane.

Handling the Discovered Change

Release Control handles the discovered change in one of the following ways, depending on the extent to which the above matching criteria were met:

- 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 Release Control as a **detected change**.
  Detected changes are displayed with the corresponding change request in the Analysis module's Review > Verification tab.
- 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 Release Control as a **latent change**.

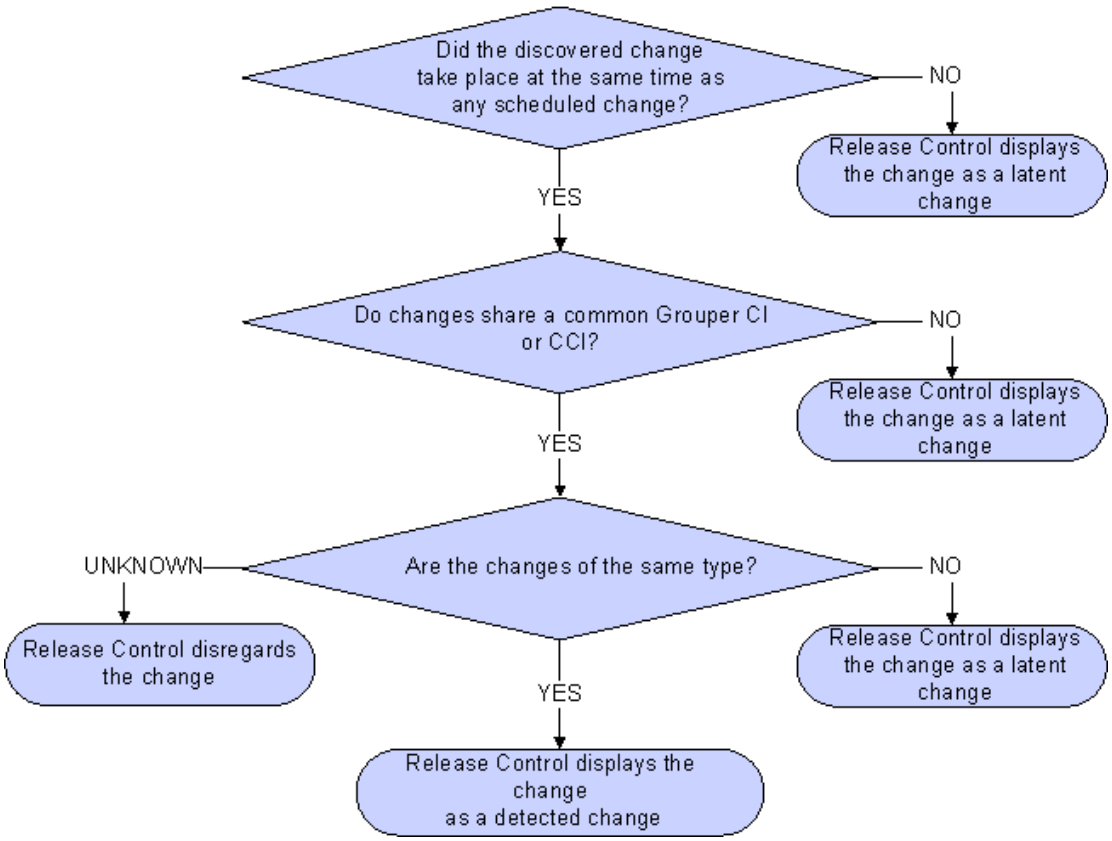
  > **Note:** To ensure that the system does not disregard latent changes due to an unknown value for change-type- orig field, add this field to the convertChange.js file, located in Module > Administrator > Configuration tab > Integrations > Service Desk Adapters > <service desk application>.

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.

- 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), Release Control disregards the discovered change and the change is not displayed.

The following flow chart summarizes the way in which Release Control handles a discovered change:



Example:

Assume, for example, that **NewChange** is the name of a discovered change that was detected by Universal CMDB and **CCMrequest1**, **CCMrequest2**, and **CCMrequest3** are all the scheduled changes included in Release Control.

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, Release Control checks whether **NewChange** and **CCMrequest2** have identical CIs. If they do not have identical CI's, Release Control checks to see if they link to a common grouper CI. If they do, 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 Release Control cannot identify the change type of **CCMrequest2**, then **NewChange** is disregarded and is not displayed anywhere.

Configuring Impact Analysis (Correlation) Rules

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

After Impact Analysis rules are defined in Universal CMDB, Release Control imports selected rules 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. You can define the Impact Analysis rules that determine the impact relationships of CIs.

If you are working with Universal CMDB 10.20 or later, 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 Impact Analysis rules. For details, see Impact Pane.

Release Control Federation Adapters Overview

The Release Control Federation adapter supports the retrieval of data from Release Control. Every request to Release Control to calculate a federated query is made through these adapters.

There are two types of Release Control Federation adapters:

- **Change Federation adapter.** For details, see The Change Federation Adapter.
- **KPI Federation adapter.** For details, see Configure KPIs as Federated in Business Availability Center 8.x or Business Service Management 9.x.

> **Note:** For details on how to configure the Release Control Federation adapters, refer to Universal CMDB documentation.

The Change Federation Adapter

The Change Federation adapter supports the **Request For Change** CI type. You use **Membership** links to create a query in Universal CMDB to view all the planned changes for a system or business CIs.

The adapter ID for the Change Federation adapter is **RcChangeAdapter**.

The following use cases describe how the adapter can be employed:

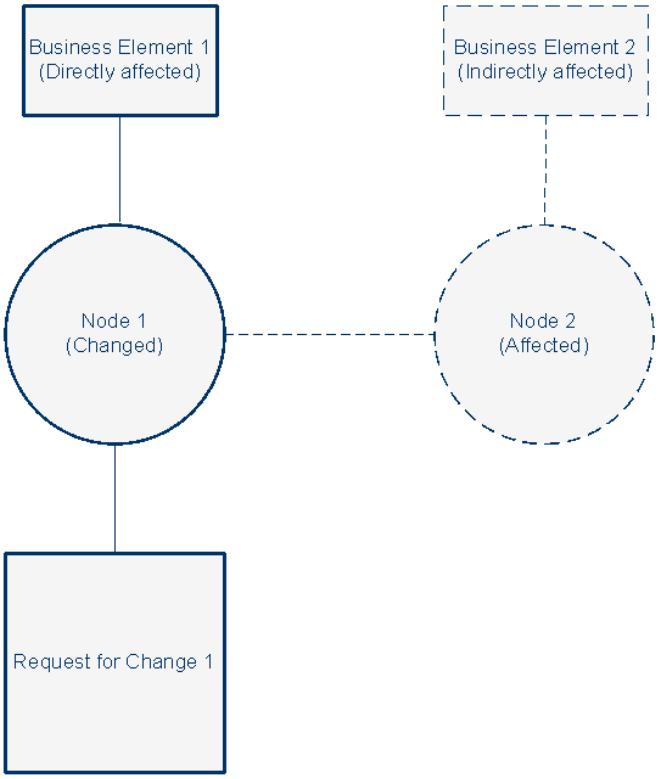
- A user can query **Requests for Change** connected to any CI within a specific time frame.
- A user can query **Requests for Change** connected to specified Infrastructure Element CIs.
  In this case, Universal CMDB retrieves changes that directly change system CIs and not changes that indirectly affect system CIs.
- A user can query **Requests for Change** connected to a specified Business Element CI.
  In this case, Universal CMDB retrieves changes that directly affect business CIs and not changes that indirectly affect business CIs.

In all of the above cases, Universal CMDB retrieves parent changes and independent tasks. 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 Release Control, **Request For Change 1**will be performed on **Node 1**. **Business Element 1** runs on **Node 1** and is therefore directly affected by the change.

Node 2 is connected to **Node 1** and may be affected by **Request for Change 1** but no actual change is made to **Node 2**. **Business Element 2** runs on **Node 2** and may be indirectly affected by the change.



If the user runs a query to retrieve planned changes to **Node 1** or **Business Element 1**, Universal CMDB will display **Request for Change 1**, because this change directly affects those CIs.

If the user runs a query to retrieve planned changes to **Node 2** or **Business Element 2**, Universal CMDB will not display any changes because there are no changes that directly affect those CIs.

> **Note:** For details about how to add custom fields to the Federation adapter, see Add Custom Fields to the Federation Adapter

Tasks

Configure Universal CMDB 10.20 or Later

The following steps describe the recommended configuration for Universal CMDB 10.20 or later.

Step 1: Configure CI search directives

Step 2: Configure system-business CI relationships

Step 3: Convert system CITs to business CITs

Step 4: Configure Impact Analysis (Correlation) rules

Step 5: Triggered CI to changed CI Impact Analysis (Correlation) rules

Step 1: Configure CI search directives

When a ticket is received, it is parsed using the analysis rules. These parsed strings are then used to search Universal CMDB for valid CIs. As entries are searched in Universal CMDB, only specified attributes of each entry are searched. In this step, you specify which attributes are searched for each CIT. For details, see CIs Analysis Lookup Directive Pane.

Step 2: Configure system-business CI relationships

The relationships that exist between CIs are important in calculations such as impact analysis. To understand how a change request on one CI affects other CIs, you must understand which CIs are linked. The links between different system CIs are detected automatically by Universal CMDB. However, if there is a relevant connection between a system CI and a business CI, it must be manually defined in Universal CMDB.

To configure system-business CI relationships, you need to model the business CI using the Universal CMDB Modeling Studio. For more information, refer to the documentation for the Universal CMDB version you are using.

Step 3: Convert system CITs to business CITs

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

To import a system CIT as a business CIT:

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

Step 4: Configure Impact Analysis (Correlation) rules

Impact Analysis (Correlation) rules define the relationships between CIs. They are defined in Universal CMDB and can be custom-defined to work with Release Control. Impact analysis is built on Impact Analysis 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 Impact Analysis rules which determine these impact relationships of CIs are defined in the Impact pane. For details, see Impact Pane.

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

To define a new Impact Analysis rule:

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

Step 5: Triggered CI to changed CI Impact Analysis (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.

In this step, you specify the Impact Analysis rules that define the relationship that defines triggered CIs and CCIs. For details, see Directly affected correlation rules group.

Increase the Number of CI Property Conditions forImpactAnalysis using the JMX Console

During the change process, Release Control may return the following (sample) error that is written to the **<Release Control installation directory>\server-0\logs\cmdb-90\cmdb-90_general.log** file:

```
Caused by:
com.mercury.topaz.cmdb.shared.tql.exception.TqlValidationException:
[ErrorCode [122] Properties condition exceeded maximum variables allowed]
 Properties condition exceeded maximum variables allowed! number of vars:
100 maximum vars allowed :50
```

If this exception occurs, you need to increase the maximum number of variables allowed for impact analysis using Universal CMDB JMX console 9.01. Ensure that you update the maximum number allowed to the number written in the error message. In the example above, it is 100. Setting the maximum to larger than that may affect the performance of Universal CMDB.

The following steps describe how to increase the number of CI property conditions Release Control uses for impact analysis.

1. Launch your Web browser and enter the following address: **http://<server_name>:8080/jmx-console**, where **<server_name>** is the name of the machine on which Universal CMDB is installed.
2. Under UCMDB, click **UCMDB**:**service=Settings Services**
3. Locate **setSettingValue**.
4. In the **Value** box for the parameter **customerId**, enter the customer ID.
5. In the **Value** box for the parameter **Name**, enter `tql.validation.max.vars.propertiescondition`.
6. In the **Value** box for the parameter **Value**, enter the number written in the error message (above).
7. Click **Invoke**.
8. Restart the Universal CMDB server.

Configure Advanced Universal CMDB Settings

The following steps describe advanced configuration options for Universal CMDB.

Step 1: Configure CI attribute displays

Step 2: Configure synchronization frequency

Step 3: Configure the connection settings

Step 4: Map Release Control to Universal CMDB impact severity levels

Step 1: Configure CI attribute displays

When viewing CI details in Release Control, the only attribute that is displayed by default is **name**. In this step, you can specify which CIT attributes you want to display in Release Control. For details, see CIs Display Pane.

Step 2: Configure synchronization frequency

In this step, you can configure how often Release Control synchronizes with the Universal CMDB database. For details, see Synchronization Pane.

Step 3: Configure the connection settings

In this step, you define the type of connection between Release Control and Universal CMDB.

To set the connection type:

1. Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Universal CMDB** > **Connection**.
2. In the **Connection type** box, set the value to **RMI**, **HTTP**, or **HTTPS**.
3. If you specified HTTPS, perform the following steps:
   a. Copy the Universal CMDB certificate to the **<Release Control installation directory>\java\bin** directory.
   b. From the command line, go to the **<Release Control installation directory>\java\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>\java\lib\security\cacert –storepass changeit
```

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

Step 4: Map Release Control to Universal CMDB impact severity levels

Universal CMDB and Release Control use different severity level scales. In this step, you map the severity levels that are imported from Universal CMDB to impact severity levels in Release Control. For details, see Severity Enum Mapping Pane.

Upgrade the Universal CMDB Version

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

Step 1: Install or upgrade the new version of Universal CMDB

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

Step 2: Disable business CIs synchronization

> **Caution:** If you are upgrading from Universal CMDB 7.x to 10.20 or later, you must perform this step, which disables the synchronization between Release Control and the CMDB database. Not performing this step results in a loss of data.

Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Universal CMDB** > **Synchronization** and clear the **Synchronize business CIs** check box.

Step 3: Define the DNS name of the Universal CMDB server

Define the DNS name of the server on which Universal CMDB is installed. For details, see <Available Connections Panes>.

Step 4: Configure the connection setting

Define the type of connection between Release Control and Universal CMDB, as described in Configure the connection settings.

Step 5: Select the required upgraded version of Universal CMDB you want to work with Release Control

Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Universal CMDB** and choose the required version of Universal CMDB. The valid versions are: **No Universal CMDB** and **10.20 and above**. If you have installed a patch on one of the above versions and your version number does not match any of the above, see How to Manually Configure Universal CMDB Patches.

Step 6: Redeploy the Release Control package

Redeploy the **ccm_package.zip** file located in the **<Release Control installation directory>\MAM\mam-<version>.zip**, where **<version>** is the new version of Universal CMDB. For more information about deploying packages, see the Universal CMDB documentation.

Step 7: Export the application importance property (when upgrading from Universal CMDB 7.x to Universal CMDB 10.20 or later)

When using Universal CMDB versions 7.5, the importance level of business CIs is configured in Release Control (**Module** > **Administrator** > **Business CIs** tab).

When using Universal CMDB 10.20 or later, the importance level of business CIs is defined in Universal CMDB.

You can export the data from this property in Release Control to Universal CMDB as follows:

1. Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Universal CMDB** > **Synchronization** and clear the **Synchronize business CIs** check box to disable the synchronization between Release Control and the CMDB database.
2. Make sure that the Universal CMDB and Release Control servers are up and running.
3. Run the **ApplicationImportanceExporter.bat** file located in the **<Release Control installation directory>\bin** directory. For details about the **ApplicationImportanceExporter.bat** file, see Export Application Importance.

Step 8: Enable Business CI synchronization

> **Caution:** If you are exporting the application importance property, you must complete step 7 before doing this step. Performing these steps out of order can result in loss of data.

Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Universal CMDB** > **Synchronization** and select the **Synchronize business CIs** check box to enable the synchronization between Release Control and the CMDB database.

Manually Configure Universal CMDB Patches

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

To manually configure Release Control integration with Universal CMDB:

1. Back up and delete all of the .jar files listed above from the **<Release Control installation directory>\apps\cmdb-adapter-<version>\WEB-INF\lib** directory.
2. Copy the .jar files from Universal CMDB to the **<Release Control installation directory>\apps\cmdb-adapter-<version>\lib** directory. Rename them to match the Release Control file names above.
3. Restart the Release Control server.

Configure Release Control to Work in Standalone Mode

This task describes how to configure the **cmdb-mock.js** script to enable Release Control to work in standalone mode. This file is located in **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Universal CMDB** > **Impact** > **Standalone UCMDB script**.

For more information on using Release Control in standalone mode, see Working in Standalone Mode Overview.

This task includes the following steps:

Step 1: Analyze the CI configuration

Step 2: Determine the behavior of CIs during impact analysis calculations

Step 3: Synchronize the application configurations

Step 1: Analyze the CI configuration

Release Control uses analysis rules to locate names of CIs within collected requests. You use the

following functions in the **Analyze CI config** section of the **cmdb-mock.js** script to generate a unique ID for the CI names that were located and to determine how the CIs appear in the Release Control user interface.

- **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 Release Control. This ensures that each CI is uniquely analyzed within the system.

- **getCiLabel.** This function defines the way the CI appears in the Release Control user interface. By default, this function returns the name of the CI as it appears in the request.

```
function getCiLabel(ciName, ciType){

        return ciName;

}
```

Step 2: Determine the behavior of CIs during impact analysis calculations

You use the following functions in the **Impact config** section of the **cmdb-mock.js** script to determine the behavior of CIs during Impact Analysis calculations:

- **isSystem.** This function determines whether the CIs defined above in the **Analyze CI config** section are classified as business or as system CIs (hardware). In the Release Control user interface, 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 java script 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 **<Release Control installation directory>\conf\enumerations.settings** file.

Step 3: Synchronize the application configurations

In a regular Release Control deployment, 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 Release Control user interface.

In standalone mode, you can determine whether you want 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 are defined as obsolete.

You use the following functions in the `Synchronize Application config` section in the **cmdb-mock.js** script to define this functionality:

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

  ```
  function showObsolete(){

          return false;

  }
  ```

  By default, this function is set to **false** and the 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 are 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 Release Control server for the changes to take effect.

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

Configure KPIs as Federated in Business Availability Center 8.x or Business Service Management 9.x

If Release Control is integrated with Business Availability Center 8.x or Business Service Management 9.x, you can view Key Performance Indicators (KPIs) for the CIs impacted by the selected activity.

To enable KPI viewing in Release Control:

1. Set up the **BACKPIsAdapter**. For information on how to set up the **BACKPIsAdapter**, refer to the *Universal CMDB Developer Reference Guide*.
2. Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Universal CMDB** > **Monitoring** and then select the **Enable KPI** box.
3. In the Director module, you can view all the KPIs from each KPI federation adapter that was configured in Universal CMDB. For example, **BACKPIsAdapter** or **RCKpiActualChangeAdapter**.

To configure Release Control adapters:

Release Control provides the following adapters:

- **RCKpiActualChangeAdapter.** Measures the number of changes on a specific CI in the last 24 hours (starting from this moment).
- **RCKpiPlannedChangeAdapter.** Measures the number of planned changes on a specific CI in the last 24 hours (starting from this moment).
- **RCKpiLatentChangeAdapter.** Indicates the status of a specific CI. The status can be one of the following:
  - **Critical** - There was at least one latent change (unauthorized change) in the last 24 hours (starting from this moment).
  - **OK** - There were no latent changes in the last 24 hours (starting from this moment).

To configure these adapters, you must deploy the relevant package for each adapter. The packages are located in the **<Release Control installation directory>\uCmdb\ucmdb-<version number>\extensions\federation** directory.

Add Custom Fields to the Federation Adapter

This task explains how to add custom fields to the Federation adapter. (For more information on Federation adapters, see The Change Federation Adapter and Release Control Federation Adapters Overview.)

1. In Release Control, add the relevant fields in **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Fields**. For more information about adding custom fields, see Fields Pane.
2. In Universal CMDB, go to the **Request for 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 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 **<Universal CMDB root directory>\UCMDBServer\runtime\fcmdb\CodeBase\RcChangeAdapter** directory.
3. (Optional) If you want to use attribute values for a specific attribute that are different from the values used in Universal CMDB, you must do the following:
   a. Add the attribute name to the **convertfields.properties** file if it does not yet appear there.
   b. Create a file and map the Release Control field values to the Universal CMDB attribute values. The name of the file must be identical to the name of the attribute as it appears in Universal CMDB. For example, if you want to map different attribute values for a field called **priority**, then the name of the file must be called **priority.properties**. In the following example, the **priority.properties** file displays mapped values for the **priority** field.

```
# File format:
# RC priority value=uCMDB priority value
IMMEDIATE=1_critical
HIGH=2_high
NORMAL=3_average
LOW=4_low
#UNKNOWN= there is no available value in uCMDB: 'it_process_priority_enum'
```

> **Note:** The file containing the mapped values must be located under the same folder as the **convertfields.properties** file.

Encrypt a Password Using the JMX Console

If you open the CI Selector within Universal CMDB, you need to encrypt the password contained in the URL link to Universal CMDB. This task describes how to use the JMX console to encrypt a password.

> **Note:** If you are using Universal CMDB 9.0, the CI Selector works only if the Release Control and Universal CMDB servers are under the same domain.

1. Launch your web browser and enter the following address: **http://<server_name>:8080/jmx-console,** where **<server_name>** is the name of the machine on which Universal CMDB is installed.
2. Under **MAM**, click **service=MAM Security Services** to open the JMX MBEAN View page.
3. Launch your web browser and enter the following address: **http://<server_name>:8080/jmx-console,** where **<server_name>** is the name of the machine on which Universal CMDB is installed.
4. Locate **java.lang.String getUser**.
5. In the **ParamValue** box for the parameter **customerId**, enter the customer ID.
6. In the **ParamValue** box for the parameter **userName**, enter the user name.
7. In the **ParamValue** box for the parameter **password**, enter the password.
8. Click **Invoke** to encrypt the password. The encrypted password appears.
9. Copy the encrypted password and paste it into the **Encrypted Password** box in the Available Connection pane. For details, see <Available Connections Panes>.

Configure Release Control and Universal CMDB to Work with LDAP Using the JMX Console

> **Note:** This task is relevant if you are working with Universal CMDB version 8.x or later.

This task describes how to use the JMX console to enable both Release Control and Universal CMDB to work with LDAP.

1. Launch your web browser and enter the following address: **http://<server_name>:8080/jmx-console,** where **<server_name>** is the name of the machine on which Universal CMDB is

installed.

2. Under **MAM**, click **service=MAM Security Services** to open the JMX MBEAN View page.
3. Locate **java.lang.String createIntegrationUser**.
4. In the **ParamValue** box for the parameter `customerId`, enter the customer ID.
5. In the **ParamValue** box for the parameter `userName`, enter the administrator's username as specified in the **ldap.properties** file located in **Module** > **Administrator** > **Configuration** tab > **Security** > **Authentication** > **LDAP Mode** > **LDAP Server Properties**.
6. In the **ParamValue** box for the parameter `password`, enter the administrator's password as specified in the **ldap.properties** file located in **Module** > **Administrator** > **Configuration** tab > **Security** > **Authentication** > **LDAP Mode** > **LDAP Server Properties**.
7. In the **ParamValue** box for the parameter `dataStoreOrigin`, enter **RC**.
8. Click **Invoke** to generate the required user name and password.
9. Copy the user name and password and paste them into the **Username** and **Password** boxes in **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Universal CMDB** > **Available Connections**. For details see, <Available Connections Panes>.

Import Business CIs from Universal CMDB

Release Control enables you to view details of the business CIs affected by the change requests processed by Release Control. You can also assign importance levels to these business CIs, and associate specific users with them (**Module** > **Administrator** > **Business CIs** tab).

You can use the following methods to import business CIs from the Universal CMDB:

- Import CIs of type application using a predefined view
- Import specific CIs by dragging them into a predefined view
- Import specific CIs by using qualifiers in Universal CMDB

Import CIs of type application using a predefined view

As part of the Release Control deployment package, Universal CMDB includes a predefined view called **AllApplicationsCIs**. This view defines all CIs of type **Application** as business CIs. You can configure Release Control to import all CIs defined in this view.

To import all CIs defined in the AllApplicationsCIs view:

1. Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Universal CMDB** > **Impact** > **Business CIs**.
2. In the **Business CIs name view** box, type `AllApplicationsCIs`.

> **Note:** For more information about Universal CMDB views, refer to the Universal CMDB documentation.

Import specific CIs by dragging them into a predefined view

As part of the Release Control deployment package, Universal CMDB includes a predefined view called **ccmApplications**. By default, this view is empty. You can drag specific CIs into this view and configure Release Control to import only CIs included in this view.

To import only CIs included in the ccmApplications view:

1. In Release Control, select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Universal CMDB** > **Impact** > **Business CIs**.
2. In the **Business CIs name view** box, type `ccmApplications`.
3. In Universal CMDB, in the **ccmApplications** view, add the specific CIs that you want Release Control to import as business CIs.

> **Note:** For more information about Universal CMDB views, refer to the Universal CMDB documentation.

Import specific CIs by using qualifiers in Universal CMDB

In Universal CMDB you can define a qualifier that you associate with specific CI types. You can configure Release Control to define all CIs associated with this qualifier as business CIs.

> **Note:** If you use qualifiers to define business CIs, Release Control does not automatically import all the business CIs from Universal CMDB. The business CIs are only imported in Release Control when they are included in a change request.

To import CIs using Universal CMDB qualifiers:

1. In Universal CMDB, define a qualifier and associate it with CI types that you want Release Control to define as business CIs.
2. In Release Control, select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Universal CMDB** > **Impact**.
3. In the **Business CI qualifier** box, type the name of the qualifier you defined in Universal CMDB.

> **Note:** For more information about Universal CMDB qualifiers, refer to the Universal CMDB documentation.

Reference

Integration Configuration User Interface

This section includes:

- Universal CMDB Pane
- <Available Connections Panes>
- CIs Analysis Lookup Directive Pane
- CIs Display Pane
- Impact Pane
- Applications Pane
- Business CI Name Attributes Pane
- Severity Enum Mapping Pane
- Latent Changes Pane
- Change Type Matching CI Type Pane
- Monitoring Pane
- Synchronization Pane
- Standalone Universal CMDB Script Pane
- Standalone Universal CMDB KPI Script Pane

Universal CMDB Pane

This pane enables you to select the version of Universal CMDB you want to work with Release Control.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Universal CMDB**.

Relevant tasks	Upgrade the Universal CMDB Version
See also	• Working with the Configuration Tab • Working in Standalone Mode Overview

User interface elements are described below:

UI Elements (A-Z)	Description
UCMDB version	Select the Universal CMDB version you want to work with Release Control. **Note:** If your are working with Release Control in standalone mode without using Universal CMDB, select No Universal CMDB (standalone).

<Available Connections Panes>

This pane enables you to define the type of connection between Release Control and Universal CMDB.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Universal CMDB** > **Available Connections**.
Important Information	The options that appear in this pane vary according to the Universal CMDB version you selected in the Universal CMDB Pane.
Relevant tasks	Configure Advanced Universal CMDB Settings
See also	Working with the Configuration Tab

User interface elements are described below:

UI Elements (A-Z)	Description
Connection type	Select the required connection type. The options are: • **RMI.** Only valid for Universal CMDB version 7.5. • **HTTP.** Only valid for Universal CMDB version 10.20 and later. • **HTTPS.** Only valid for Universal CMDB version 10.20 and later. **Note:** If you specified **HTTPS**, you need to perform step 3 in Configure the connection settings.
>Encrypted password	Enter an encrypted password if you open the CI Selector within Universal CMDB.

UI Elements (A-Z)	Description
	Note: If you are using Universal CMDB 9.0, the CI Selector works only if the Release Control and Universal CMDB servers are under the same domain. Use the JMX console to generate the encrypted password. For details, see How to Encrypt a Password Using the JMX Console.
Locator connection type	You only need to specify this option when you want to integrate with Business Availability Center and you do not know the Universal CMDB server name. In this case, you do the following: • In the **Universal CMDB server name** box, enter the Business Availability Center server name. • In the **Connection type** box, select the required connection type. • In the **Locator connection type** box, select the same connection type as you selected in the **Connection type** box. The **Locator connection type option** discovers the name of the Universal CMDB server name. If you are not integrating with Business Availability Center, set the **Locator connector type** as **None**. **Default:** RMI **Note:** Relevant only to Universal CMDB version 7.5.
Modeling Studio link	The URL that opens the Modeling Studio from Release Control. **Note:** Relevant to Universal CMDB version 8.x or later.
Port	The port used by the Universal CMDB server.
Universal CMDB server name	The DNS name of the server on which Universal CMDB is installed.
Password	The password needed to log on to Universal CMDB. Use the JMX console to generate the required password. For details, see How to Configure Release Control and Universal CMDB to Work with LDAP Using the JMX Console. **Note:** Relevant to Universal CMDB version 8.x or later.
Username	The user name needed to log on to Universal CMDB. Use the JMX console to generate the required user name. For details, see How to Configure Release Control and Universal CMDB to Work with LDAP Using the JMX Console.

UI Elements (A-Z)	Description
	Note: Relevant to Universal CMDB version 8.x or later.

UCMDB Custom ID to Tenant Mapping Area

If you are configuring Release Control for multi-tenancy, you use this area to map tenants to Universal CMDB Customer IDs. For details about multi-tenancy, see Multi-Tenancy Configuration Overview.

User interface elements are described below:

UI Elements (A-Z)	Description
	Add configuration to configuration set. Enables you to add a new tenant-Customer ID mapping.
	Remove configuration from configuration set. Enables you to delete the selected tenant-Customer ID mapping.
Universal CMDB Customer ID	The Universal CMDB Customer ID associated with the corresponding tenant in the Tenant Name column.
Tenant Name	The name of the tenant that corresponds to the ID specified in the Universal CMDB Customer ID column. You specify tenant names in the Multi-tenancy pane. For details, see Multi-Tenancy Pane.

CIs Analysis Lookup Directive Pane

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

By default, Release Control searches for changed CIs that belong to the **host** or **ip** CITs and whose format matches one of the Universal CMDB attributes listed in the CIs Analysis Lookup Directive pane.

If you want Release Control to search for CIs that belong to a different CIT, you must add this CIT and its relevant attributes to the CIs Analysis Lookup Directive pane.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Universal CMDB** > **CIs Analysis Lookup Directive**.
Important Information	This pane does not appear if you are using Release Control in standalone mode.

Relevant tasks	Configure Universal CMDB 10.20 or Later (Recommended)
See also	Working with the Configuration Tab

User interface elements are described below:

UI Elements (A-Z)	Description
	Add configuration to configuration set. Enables you to add a CIT whose format matches one of the attributes in Universal CMDB.
	Remove configuration from configuration set. Enables you to delete the selected row.
Attributes	Enables you to configure which attributes are searched for each CIT. For example, to locate an **ip** CIT by domain, in addition to locating it by address or DNS name, add ip_domain. **Note:** You must select at least one attribute. Only string type attributes are supported.
CI type	The CIT in Universal CMDB for which Release Control searches. **Default**: **BusinessElement**, **Node** and **IpAddress**

CIs Display Pane

When viewing CI details in Release Control, the only attribute that is displayed by default is **name**. This pane enables you to specify which CIT attributes you want to display in Release Control.

> **Note:** This pane is available for Universal CMDB 8.x and earlier versions only.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Universal CMDB** > **CIs Display**.
Important Information	• Release Control also displays the attributes of the CIT based on the Universal CMDB CIT hierarchy. For example, if the displayed CIT is a router, the attributes of the router's host are also displayed. • This pane does not appear if you are using Release Control in standalone mode.
Relevant tasks	Configure Advanced Universal CMDB Settings
See also	Working with the Configuration Tab

User interface elements are described below:

UI Elements (A-Z)	Description
	Add configuration to configuration set. Enables you to add the CIT attributes you want to display in Release Control.
	Remove configuration from configuration set. Enables you to delete the selected row.
Attributes	The CIT attributes you want to display in Release Control. **Note:** You must select at least one attribute.
CI type	The CIT whose attributes you want to display in Release Control.

Impact Pane

This dialog box enables you to define which Impact Analysis (Correlation) rules Release Control imports for the purposes of impact analysis.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Universal CMDB** > **Impact**.
Important Information	This pane is empty if you are using Release Control in standalone mode.
Relevant tasks	Configure Universal CMDB 10.20 or Later (Recommended)
See also	• Configuring Impact Analysis (Correlation) Rules • Working with the Configuration Tab

User interface elements are described below:

UI Elements (A-Z)	Description
Business CI qualifier	The initial categorization of CITs into business and system CIs is performed by Universal CMDB. When importing a CIT from Universal CMDB, the category is carried over to Release Control. However, you can configure a system CIT in Universal CMDB to be imported as a business CIT in Release Control. You do this by adding the **MODELING_ENABLED** qualifier in Universal CMDB versions 8.x or later. For more information, refer to the Universal CMDB documentation.
Directly affected	Triggered CIs are those mentioned explicitly on the ticket. Change

UI Elements (A-Z)	Description
correlation rules group	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. This option enables you to specify the Impact Analysis (Correlation) rules that define the relationship that defines triggered CIs and CCIs. • For Universal CMDB 10.20 or later: When you define a new Impact Analysis rule in Universal CMDB, select **RC_DIRECTLY_AFFECTED** for the **Correlation Rule Groups** option to indicate that this correlation defines an Impacted by (Directly) relationship.
Folding correlation rules group	Defines the organizational structure of the business CIs and system CIs in Assess > Impact Tab. **Note:** By default, the CIs are connected by an Impacted by (Directly) relationship. You can modify this if you want to override the system default, but it is recommended that the default be used.
Impact correlation rules group	• For Universal CMDB 10.20 or later: Enables you to define which Impact Analysis rules determine the impact relationships of CIs. When you define a new Impact Analysis rule in Universal CMDB, you must select **RC_IMPACT** for the **Correlation Rule Groups** option. It indicates that this correlation is relevant to impact in Release Control.

Applications Pane

This pane enables you to define the Universal CMDB view that Release Control uses to import business CIs.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Universal CMDB** > **Impact** > **Applications**.

User interface elements are described below:

UI Elements (A-Z)	Description
Applications name view	The name of the view in Universal CMDB that defines the business CIs that are imported into Release Control. **Default Value**: ccmApplications

Business CI Name Attributes Pane

This pane enables you to edit the way in which business CIs are displayed in Release Control.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Universal CMDB** > **Impact** > **Business CIs** > **Business CI Name Attributes**.

User interface elements are described below:

UI Elements (A-Z)	Description
Business CI Name Attributes	Edit the **Business CI Name Attributes** file to change the way in which business CIs are displayed in Release Control.

Severity Enum Mapping Pane

Universal CMDB and Release Control use different severity level scales. When severity levels are imported from Universal CMDB to Release Control, there must be a mapping to convert the scales. This pane enables you to modify this mapping scheme. For the default mapping scheme, see Default Mapping Scheme below.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Universal CMDB** > **Impact** > **Severity Enum Mapping**.
Important Information	This pane does not appear if you are using Release Control in standalone mode.
See also	Working with the Configuration Tab

User interface elements are described below:

UI Elements (A-Z)	Description
Release Control Value	Release Control impact severity level.
Universal CMDB value	The maximum value in Universal CMDB for the corresponding impact severity level in Release Control.

Default Mapping Scheme

The following table shows the default mapping scheme.

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

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

Latent Changes Pane

This pane enables you to configure the latent change feature in Release Control.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Universal CMDB** > **Latent Changes**.
Important Information	• All nodes in the TQL must be set to visible (property visible = true). • This pane does not appear if you are using Release Control in standalone mode.
See also	• Configuring Latent and Detected Changes • Working with the Configuration Tab • Universal CMDB documentation for more information about TQL queries.

User interface elements are described below:

UI Elements (A-Z)	Description
Detect changes duration (hours)	Defines the block of time for which Release Control requests information from Universal CMDB about newly discovered changes. **Default:** 24 hours (measured in hours), meaning that Universal CMDB discovers changes that occurred in the last 24 hours.
Detected changes queries	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.

UI Elements (A-Z)	Description
Detect changes recovery duration (hours)	When the 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). This option enables you to define how far back in time Release Control should calculate change detection. **Default:** One month (measured in hours)
Detect changes schedule	Defines the schedule for Release Control's request of information from Universal CMDB about newly discovered changes. **Note:** This value is entered as a cron expression.

Latent changes mode	Enables you to work with the latent change feature by defining a value for this element. You can define one of the following values:
	
	• **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.
	• **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.
	• **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.
	• **DISABLED.** The latent change feature is inactivated. Release Control does not receive information about new changes in your environment.
	
	Default: DISABLED

UI Elements (A-Z)	Description
Latent changes level	Latent changes are displayed as separate changes in the Analysis module. Defines whether you want latent changes to be displayed as top-level (parent) change requests or second-level (child) requests.
Latent change Request ID format	Define a format for the latent change request ID.
Latent change Request ID initial value	Define the number that is included in the Request ID for the first latent change recorded in your system.

Change Type Matching CI Type Pane

This pane enables you to defines on which CI types to activate the latent change feature.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Universal CMDB** > **Latent Changes** > **Change Type Matching CI Type** > **Added Hardware** and **Added Software**.
Important Information	• This pane is relevant only if you are using the **LATENT_AND DETECTED** or **LATENT_CONSIDER_CHANGE_TYPES** modes in the Latent Changes pane. For details, see Latent Changes Pane. • To enable 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 attribute values is selected for each CIT within Universal CMDB: **Change Monitored**, **Comparable**, **Asset Data**. > **Note:** By default, all such CITs whose relevant attributes are updated, are considered to be detected changes. If you want to limit the CITs that are considered to be detected changes, select the required attributes from the Attributes list. • This pane does not appear if you are using Release Control in standalone mode.
See also	• Working with the Configuration Tab • Configuring Latent and Detected Changes.

User interface elements are described below:

UI Elements (A-Z)	Description
	Add configuration to configuration set. Enables you to add a CI type on which to activate the latent change feature.
	Remove configuration from configuration set. Enables you to delete the selected CI type.
Action type	The type of action performed on the CI in Universal CMDB that caused the discovered change. The valid values are: • update • add **Note:** Universal CMDB does not support the **remove** action type.
Attribute	The specific attribute of the CI type that was changed. By default, all CIT attributes that are defined as **Change Monitored**, **Comparable**, **Asset Data** in Universal CMDB are checked for changes. You can use the **Attribute** list to specify only those attributes you want checked for changes.
Change Types	The type of discovered change. The change type can be one of the following: • **Hardware - Add.** A change that involves adding hardware. **Note:** This change type is not supported by Universal CMDB. • **Hardware - Remove.** A change that involves removing hardware. • **Hardware - Update.** A change that involves updating hardware. • **Software - Add.** A change that involves adding software. • **Software - Remove.** A change that involves removing software. **Note:** This change type is not supported by Universal CMDB. • **Software - Update.** A change that involves updating software. **Note:** To enable 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

UI Elements (A-Z)	Description
	type. You then need to map this field to the possible values—**HW_ADD** or **SW_ADD**—in the **change-type-orig** field. For more information about converting and mapping service desk application fields, see Converting Change Requests Overview.
CI Type	The CI type of the discovered change.

The Change Type Matching CI Type panes are described below:

UI Elements (A-Z)	Description
Hardware - Add pane	Enables you to configure on which CI types to activate the latent change feature when a change occurs that involves hardware.
Software - Add pane	Enables you to configure on which CI types to activate the latent change feature when a change occurs that involves software.

Monitoring Pane

If Release Control is integrated with Business Availability Center 8.x or later, you can view Key Performance Indicators (KPIs) for the CIs impacted by the selected activity. To enable KPI viewing in Release Control, the KPIs need to be configured as federated in Business Availability Center. For details on how to configure KPIs as federated in Business Availability Center, see How to Configure KPIs as Federated in Business Availability Center 8.x or Business Service Management 9.x.

In this pane, you can enable/disable KPI viewing.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Universal CMDB** > **Monitoring**.
Important Information	This pane appears if you are: • Using Release Control in standalone mode • Working with Universal CMDB 8.x or later
Relevant tasks	Configure Release Control to Work in Standalone Mode
See also	• Working with the Configuration Tab • Working in Standalone Mode Overview

User interface elements are described below:

UI Elements (A-Z)	Description
Enable KPI	• If you are using Release Control in standalone mode, then selecting this enables you to create simulated KPIs. For details, see Standalone Universal CMDB KPI Script Pane. • If you are working with Universal CMDB 8.x or later, then use this feature to enable/disable KPI viewing in Release Control.

Synchronization Pane

This pane enables you to configure how often Release Control synchronizes with the CMDB database.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Universal CMDB** > **Synchronization**.
Important Information	This pane does not appear if you are using Release Control in standalone mode.
See also	Working with the Configuration Tab

User interface elements are described below:

UI Elements (A-Z)	Description
Synchronize business CIs	Enable/disable synchronization between Release Control and the CMDB database. **Default:** Selected
Synchronization frequency (minutes)	The frequency at which Release Control synchronizes with the CMDB database. **Default:** 2 hours (measured in seconds)

Standalone Universal CMDB Script Pane

In this pane you configure the **cmdb-mock.js** script to enable Release Control to work in standalone mode.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Universal CMDB** > **Impact** > **Standalone UCMDB script**.
Important Information	This screen is only relevant if you are using Release Control in standalone mode.

Relevant tasks	Configure Release Control to Work in Standalone Mode
See also	• Working with the Configuration Tab • Working in Standalone Mode Overview

Standalone Universal CMDB KPI Script Pane

In this pane, you configure the **mock-kpi.js** script to create simulated KPIs for the standalone version of Release Control.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Universal CMDB** > **Monitoring** > **Standalone UCMDB KPI script**.
Important Information	• This pane is only relevant if you are using Release Control in standalone mode. • To be able to create simulated KPIs, you must select the **Enable KPI** check box in the Monitoring Pane.
See also	• Working with the Configuration Tab • Working in Standalone Mode Overview

Service Desk Configuration

This chapter includes:

Concepts

- Converting Change Requests Overview
- Adapter Configuration Overview
- Writing Conversion Scripts
- Linking to Release Control Interfaces from the Service Desk
- Updating Approval Status in the Service Desk
- Updating Suggest Time Analysis in Service Manager

Tasks

- Configure the Initial Service Desk Integration
- Retrieve Tickets from the Service Desks
- Modify Service Desk Adapter Properties
- Configure Release Control to Update Service Manager with Analysis Information
- Configure Release Control and Service Manager with LW-SSO
- Configure Release Control for Request Approval
- Create a Link to the Release Control Application
- Create a Link to the Release Control Calendar
- Create a Link to the Release Control Assess Tab
- Create a Link to a Single Change Request
- Create a Link Using Time Zone and Locale Parameters
- Create a Link Using Tenant Parameters
- Generate Links to Service Manager Tickets
- Update the SDI Operations Script to Support the DenyFunction

Reference

Concepts

Converting Change Requests Overview

Change requests are converted from their service desk application formats to a generic format using service desk application-specific adapters. The generic requests are then transferred to the Release Control server.

Each service desk application-specific adapter contains two single-level adapters—one to convert top-level changes, and the other to convert second-level changes. Each single-level adapter contains the following subcomponents:

- **Connector**. Collects new top-level/second-level change requests from the service desk applications.
- **Converter**. Converts the top-level/second-level change requests from their service desk application formats to a generic format that Release Control can recognize. For details, see Writing Conversion Scripts.

Each single-level adapter also contains a **pre-conversion filter** and a **post-conversion filter**. Using these filters, you can control which requests are sent to the Release Control server. The pre-conversion filter filters requests before they are converted to a generic format, while the post-conversion filter filters requests after conversion, but before they are transferred to the Release Control server.

Adapter Configuration Overview

To convert service desk application requests, you must configure the appropriate adapter for each service desk application.

To configure an adapter, you must:

- Set up the adapter configuration file using the **SdiConfigurer** utility. (For details, see the *Release Control Deployment Guide*.)
- Modify the conversion scripts to be used by the adapter.

> **Note:** You can configure more than one adapter per service desk application. This enables you to import requests from different versions of the same service desk application.

Adapter Configuration File

The adapter configuration file is an XML file that contains the following:

- The adapter attributes, such as the adapter name, the name of the service desk application in which the requests were created, the number of requests to be processed at one time, the frequency with which the adapter polls the service desk application, and the request types to be converted.
- The connector attributes, which enable the adapter to connect to the service desk application. You specify the connector attributes separately for each single-level adapter—that is, for each request type included in the adapter configuration file.
- The converter attributes, which call the conversion script files where the field mapping and filter functions are defined. The converter attributes differ for each single-level adapter.

> **Note:** For details on modifying the adapter properties, see Modify Service Desk Adapter Properties.

Conversion Scripts

Conversion scripts are called by the adapter and are responsible for the actual conversion of change requests from their service desk application format to a generic format that can be handled by Release Control.

Each script must contain certain functions. For a detailed list and explanation of these functions, see Writing Conversion Scripts.

Writing Conversion Scripts

In Release Control, service desk adapters are used to retrieve change requests from the originating service desks and to convert these requests from their service desk application formats to a generic format. The conversion scripts within the service desk adapters are responsible for mapping fields from the originating service desk to corresponding Release Control fields.

When you run the initial configuration of your service desk, default conversion scripts are created. To access the conversion scripts in Release Control, go to **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Service Desk Adapters** > **<adapter name>** node and select the relevant configuration file. Content of this file is displayed in the right pane (for example, **convertTask.js** or **convertChange.js**).

To make changes to the scripts, see Configure Files in the Configuration Tab.

> **Note:** Make sure that no line within a script exceeds 256 characters.

Enumerations

In particular, it is important that the conversion scripts contain a detailed mapping scheme for the service desk application enumeration fields. Each Release Control enumeration field appears by default in the conversion scripts in the following format (upper case letters):

```
<enumeration field type>_<Release Control enumeration name>
```

For example:

```
genericRFC.setField("priority", PRIORITY_HIGH);
```

If a script refers to an enumeration field that does not exist, an error message is recorded in the script log file (see Log Files).

For details about creating Release Control enumeration fields, see Enumerations Pane.

Functions

The functions that each script must contain are explained in detail below. For an explanation of the objects that can or should be included in each function, refer to the **GenericTicketImpl** class in the *API_Reference.chm* file. (To access the API Reference, select **Start** > **Programs** > **Release Control 9.60** > **Documentation** and open the **pdfs** directory).

- **convert.** This function maps the fields of the service desk application to generic request fields. For example:

```
function convert(remedyRFC, genericRFC)
```

> **Note:** For a list of preconfigured change request fields included in Release Control, see "Preconfigured Change Request Fields" on page 231.

> **Note:** If Release Control is working in standalone mode, set the value of the isStandalone variable in convertChange.js and convertTask.js to `True` so that Release Control fetches the CI display name as the CI name. Otherwise, if Release Control is integrated with the UCMDB server, set isStandalone to `False` so that Release Control fetches the UCMDB ID of a CI to get the CI from the UCMDB server.

- **preFilter.** This function filters the change requests before they are converted, ensuring that no unnecessary requests are converted and sent to the Release Control server. The function is written using the terminology of the service desk application. For example, if you do not want to convert requests with a **Low** priority, you could use the following **preFilter** function. This function specifies that BMC Remedy Action Request System requests with a **Low** priority not be converted and that all other requests be converted:

```
function preFilter(remedyRFC){

    if (remedyRFC.get("Request Urgency")==ARS_PRIORITY_LOW)

        return false;

    else

        return true;
```

- **postFilter** This function filters the converted requests, ensuring that only required requests are transferred to the Release Control server. The function is written using Release Control request terminology. For example, the following **postFilter** function specifies that only generic requests with the status **Approved** be transferred to the Release Control server:

```
function postFilter(genericRFC){

    ccmStatus==genericRFC.get("status");

    if (ccmStatus==STATUS_APPROVED)

        return true;

    else

        return false;
```

> **Notes:**
>
> - It is recommended that you optimize network load and space consumption by converting only necessary request columns. Specify these columns in your SELECT query or use the relevant connector property.
> - If you are converting requests from Project and Portfolio Management/IT Governance Center, or a database service desk application, refer to all column names using lower case letters.
> - You can use logging objects in the conversion scripts to log statements from the request conversion process. For details, see Log Files.

Log Files

If you want to view log messages describing the activity taking place during the request conversion process, you can include logging objects in your conversion scripts. During the conversion process, you can view the log messages in the conversion script log files, located in the **<Release Control installation directory>\servers\<server name>** directory.

A logging object can be included within any of the script functions. Its syntax should be as follows:

```
logger.<type of message>("<log message>");
```

The following message types can be used:

- **info.** Records all processing activity that is performed.
- **warn.** Records warning messages.
- **error.** Records error messages.
- **debug.** Records all activity in detail

For example, you can include a logging object such as the following:

```
logger.info("converting request #3001");
```

If you want the conversion script log files to display a list of all service desk application fields, you can include the following logging object in your conversion script:

```
logger.info(BeanUtils.describe(ticket));
```

If you use the above logging object, ensure that the following line is included at the top of the conversion script:

```
importPackage(Packages.org.apache.commons.beanutils);
```

Linking to Release Control Interfaces from the Service Desk

You can create links to Release Control from your service desk. You can create a link to the whole Release Control 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 Release Control Calendar and view the scheduled changes for the relevant time frame.

> **Note:** If you do not have LW-SSO installed, you are prompted for your Release Control credentials when you access these links.

- You can create links to the following areas of Release Control:
  - **Release Control application.** You can create a customized link to the Release Control application to be used from outside of Release Control. The link can be customized to display the relevant view using the filter, timestamp, and perspective of your choice.
    For details, see Create a Link to the Release Control Application.
  - **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 Release Control is limited. For example, you cannot set filters or user preferences and you cannot access the various change analysis tabs.
    For details, see Create a Link to the Release Control Calendar.
  - **Release Control Assess tab**. You can create a link to the 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 Release Control.
    For details, see Create a Link to the Release Control Assess Tab.
  - **Single change request in Release Control.** Release Control opens displaying the specified change request. When you access Release Control using this link, you can access all other areas of Release Control.
    For details, see Create a Link to a Single Change Request.

- You can add time zone and locale parameters with any direct link to the Release Control application to specify the time zone you want Release Control to use and the language in which you want the user interface to be displayed. For details, see Create a Link Using Time Zone and Locale Parameters.

Updating Approval Status in the Service Desk

In the Analysis module **Collaborate > Resolution** tab, users with **approveChange** permissions can approve, deny, or retract approval from change requests. In certain cases, the approval status of the request is updated in the originating service desk.

You can update the approval status of requests in the following service desks:

- Service Manager
- Project and Portfolio Management / IT Governance Center

You can retract and deny the approval of requests in the following service desks:

- Service Manager

> **Note:** For details about configuring approval, see Configure Release Control for Request Approval.

Updating Suggest Time Analysis in Service Manager

In the Change Planner dialog box in the Analysis module, users can suggest a next possible time for implementing a change, which is either within a **Change Window** and outside a **Blackout** period associated with the change request. For details, see Change Planner Dialog Box.

When Release Control receives a change request from Service Manager, Release Control performs suggest time analysis on the request that contains a next suggested time for implementing the request only if:

- The status of the change request is one of the statuses selected in the **Module** > **Administrator** > **Configuration** tab > **Change Process** > **Suggest time analysis valid statuses** box. For detals, see Change Process Pane.

- The **shouldCalcSuggestTime** function in the **change-flow.js** script is set to **true**. For detals, see <Functions included in the change-flow.js script>.
- The **suggested-end-time** and **suggested-start-time** fields in **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Fields** > **Available Fields** > **Time** contain empty values. For details, see Fields Pane.

Once these conditions are met, Release Control calculates suggest time analysis and the request is updated in Service Manager.

Tasks

Configure the Initial Service Desk Integration

As part of your initial configuration of Release Control, you configure your service desk application to work with Release Control.

To configure the service desk integration you use the **SdiConfigurer** utility. For a detailed description of how to configure your service desk, see the relevant section in the *Release Control Deployment Guide*.

Retrieve Tickets from the Service Desks

The following steps describe how to retrieve tickets from your service desk application.

Step 1: Retrieve change requests on a regular basis

By default, your service desk adapter is configured to retrieve change requests on a regular basis. You can modify the schedule according to which the service desk application is polled for change requests in the service desk adapter file.

To modify the polling schedule:

1. Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Service Desk Adapters** > **<adapter name>** node. Select the **<adapter name>-adapter.settings** file and its content is displayed in the right pane.
2. Modify the **polling-schedules** property to suit your needs. For a detailed description of this

property, see Common Adapter Attributes.

3. Save and activate your configuration changes (see Save and Apply Configuration Changes).

Step 2: Retrieve all change requests from a specified date (from all service desks except Service Manager and database service desk applications)

In certain cases, you may want to retrieve all the change requests from your service desk starting from a specific point in time:

1. Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Service Desk Adapters** > **<adapter name>** node. Select the **<adapter name>-adapter.settings** file and its content is displayed in the right pane.
2. In the file, uncomment the **initial-load-state** property and enter the desired date from which you want to retrieve change requests. For a detailed description of this property, see Common Adapter Attributes.
3. Save and activate your configuration changes (see Save and Apply Configuration Changes).
4. Stop the Release Control service:
   a. From the Windows menu, select **Start** > **Run** and type **services.msc**.
   b. In Services window, select **Release Control 9.60 <server name>** and click **Stop Service**.
5. Delete the database persistency by running the **SDI Persistency Cleanup** utility. For details, see SDI Persistency Cleanup.
6. Start the Release Control service again.
7. Allow the service desk adapter to run until it has retrieved all the tickets.
8. Return the service desk adapter to a regular polling schedule by commenting out the **initial-load-state** property and saving the changes.

Step 3: Retrieve all change requests from a specified date (from Service Manager and database service desk applications only)

In certain cases, you may want to retrieve all the change requests from your service desk starting from a specific point in time. Optionally, you can also limit the time the adapter retrieves tickets from the service desk.

1. Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Service Desk Adapters** > **<adapter name>** node. Select the **<adapter name>-adapter.settings** file and its content is displayed in the right pane.

2. In the file, define a value for the following properties in the **<connection-properties>** section:
   a. **startFrom**. Indicates the past time and date from which to start fetching tickets. For example, `01/13/00 00:00:00 EST`.
   b. (Optional) **upperLimitDelta**. Defines the interval that indicates how often Release Control fetches tickets. The value is defined in milliseconds.
   In the following example, Release Control starts retrieving tickets from January 1, 2009 at 12:00 midnight, and then at 36000000 milliseconds (ten hour) intervals. That is, Release Control starts retrieving tickets on January 1, 2009 at 12:00 midnight until January 1, 2009 at 10:00. Then from January 1, 2009 at 10:00 until 01/01/2009 20:00, and so on.

```
<connection-properties>

userName=<username>

password=<password>

startFrom=013/01/2009 00:00:00 EST

upperLimitDelta=36000000

</connection-properties>
```

   > **Note:** By default, the upperLimitDelta property does not appear in the <adapter name>-adapter.settings file. If you want to define a value for it, you must add the property manually to the file in the <connection-properties> section.

3. Save and activate your configuration changes (see Save and Apply Configuration Changes).
4. Delete the database persistency by running the **SDI Persistency Cleanup** utility. For details, see SDI Persistency Cleanup.
5. Starting from the next polling job, the service desk adapter begins to retrieve the tickets from the date provided for the **startFrom** value in the **<adapter name>-adapter.settings** file. If you did not define a value for the **upperLimitDelta** property, then Release Control retrieves change requests indefinitely.

Modify Service Desk Adapter Properties

When you perform the initial configuration of your service desk using the service desk configuration utility (**SdiConfigurer.bat**), a service desk adapter configuration file is created containing all the service desk integration properties.

This task describes how to modify the service desk adapter properties.

1. Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Service Desk Adapters** > **<adapter name>** node. Select the **<adapter name>-adapter.settings** file and its content is displayed in the right pane.
2. Modify the service desk adapter properties. For a description of the properties, see Service Desk Adapter Properties.
3. Save and apply your configuration changes (see Save and Apply Configuration Changes).

Configure Release Control to Update Service Manager with Analysis Information

This task describes how to configure Release Control to update Service Manager with Analysis information. For each request inside Service Manager, you can view the risk, impact, and collision severity. You can also see whether there is a time period conflict.

1. Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Service Desk Adapters** > **<adapter name>** node. Select the **<adapter name>-adapter.settings** file and its content is displayed in the right pane.
2. In the `<request-type level="1">` element, under the `<operations>` element, comment out the `operation name=updateAnalysisData` sub-element.
3. In the `<request-type level="2">` element, under the `<operations>` element, comment out the `operation name=updateAnalysisData` sub-element.
4. Save and apply your configuration changes (see Save and Apply Configuration Changes).

Configure Release Control and Service Manager with LW-SSO

When initially configuring your service desk, you may not have configured Service Manager and Release Control to use Lightweight Single Sign-On (LW-SSO). This task describes how to enable login to Service Manager and Release Control without entering the required credentials.

1. In the Service Manager documentation, perform the steps in the task that describes how to configure LW-SSO in Release Control and Service Manager.

2. In the **connection-properties** section of the adapter configuration file, set the **requiresUserCredentials** parameter to `false` to enable login to Service Manager without entering the required credentials, and modify the **serviceURL** parameter to enable connection to the Service Manager server.
   In the example below:
   - The **requiresUserCredentials** parameter is set to `false`, enabling login to Service Manager without entering the required credentials.
   - The **serviceURL** parameter specifies the URL that connects to the required Service Manager server.

```
<connection-properties>

serviceUrl=http://<smweb-
tierhostname:portnumber>/SymphonyAdapter/inbound/ws

requiresUserCredentials=false

</connection-properties>
```

   For more information, see Common Adapter Attributes.

Configure Release Control for Request Approval

This task describes how to configure Release Control so that when users approve, deny, or retract approval from change requests in Release Control, the approval status of the request is updated in the service desk.

This task is relevant for the following service desks:

- Service Manager
- Project and Portfolio Management / IT Governance Center

Step 1: Define conditions for allowing change approval

For certain operations, Release Control sends information to the integrated service desk according to the conditions defined in the **sdOperations.js** script.

In this script, you can define when the **Approve** button in the Analysis module **Collaborate** > **Resolution** tab is enabled. By default, it is enabled for all requests with the status of **pending approval**. For details about the **sdOperations.js** script, see SDI Operations Script.

Step 2: Assign user permissions

Assign **approveChange** permissions to the users who are meant to approve requests. For details on assigning permissions, see User Configuration.

Step 3: Ensure the service desk is configured for change request approval

If you are working with Service Manager, the ability to update the approval status in the originating service desk is configured by default.

If you are working with Project and Portfolio Management/IT Governance Center, you can configure this option during the initial configuration of your service desk using the **service desk configuration utility**. If you did not configure this option during the initial configuration, follow the manual instructions below:

To manually configure **Project and Portfolio Management/IT Governance Center** for approval:

1. Before you configure request approval, make sure that the user with which you instruct Release Control to connect to the Project and Portfolio Management/IT Governance Center database has write permissions to the database.
2. Select the **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Service Desk Adapters** > **<adapter name>** node. Select the **<adapter name>-adapter.settings** file and its content is displayed in the right pane.
3. Locate the **approve** operation in both the **<request-type level="1">** and **<request-type level="2">** elements and ensure that **<connector-type>itgApprove</connector-type>** is included in an **approve** operation for both levels.
4. Define the following properties within the **<properties>** element:

Property Name	Description
dbUrl (mandatory)	The URL of the Project and Portfolio Management/IT Governance Center database.
username (mandatory)	The user name with which Release Control connects to the Project and Portfolio Management/IT Governance Center database.
password (mandatory)	The password with which Release Control connects to the Project and Portfolio Management/IT Governance Center database. **Note:** The password can be encrypted. For details, see "Password Encryption" on page 427.
driverClassName (mandatory)	The name of the JDBC driver. **Default value:** oracle.jdbc.OracleDriver

Property Name	Description
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.**
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 Project and Portfolio Management/IT Governance Center application in order for the request to be approved.

5. To ensure that the updated approved requests are of a high priority in the queue of requests being sent to Release Control, specify **updateOperation=true** within the **<sender-properties>** element.
6. Save and apply your configuration changes (see Save and Apply Configuration Changes).

Create a Link to the Release Control Application

You can create a customized link to the Release Control application to be used from outside of 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 Release Control application:

From an internet browser, enter the following URL:

```
http://localhost:8080/ccm?requestOrigin=EXTERNAL&<customizable parameters>
```

For a list of the customizable parameters, see URL Parameters for Customized Links.

> **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 for Creating Links to Release Control.

Example:

In the following example, a link is created to the Release Control application. Release Control opens in the Calendar view on the specified date. 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
```

Create a Link to the Release Control Calendar

You can create a customized link to the 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 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 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>
```

For a list of the customizable parameters, see URL Parameters for Customized Links

> **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 for Creating Links to Release Control.

Example:

In the following example, a link is created to the 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&filter
Name=any&field-calculated-risk=20,80&field-status=APPROVED,
CLOSED&timestamp=1225648800000
```

Create a Link to the Release Control Assess Tab

You can create a link to the 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 Release Control.

To create a link to the Assess tab:

From an internet browser, enter the following URL:

```
http://<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.

Create a Link to a Single Change Request

You can create a link to a single change request in Release Control. Release Control opens displaying the specified change request.

When you access Release Control using this link, you can access all other areas of Release Control.

To create a link to a single change request in 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
```

Create a Link Using Time Zone and Locale Parameters

You can create a link that opens Release Control to a specific time zone and displays the user interface in a specified language.

To create a link to the Release Control application:

From an internet browser, enter the following URL:

```
http://<RC installation home>/ccm?requestOrigin=EXTERNAL&<customizable
parameters>
```

> **Caution:** The URL must contain at least one **filterName** or **field-<field name>** parameter.

Example:

In the following example, a link is created to the Release Control application. Release Control opens in the Calendar view on the specified date. Release Control displays only the requests with a status of APPROVED and a risk level between 20-80, uses local Australian time, and displays the user interface in French.

```
http://localhost:8080/ccm?requestOrigin=EXTERNAL&filterName=any& field-
calculated-risk=20,80&field-
status=APPROVED&perspective=calendar&timestamp=1225648800000
&timezone=Australia\Currie&locale=fr_FR
```

> **Notes:**
>
> - The time zone is Java time zone.
> - If you make a mistake when entering the time zone in the URL, Release Control uses the GMT time zone as its default.
> - In case you misspell the locale's language code, Release Control uses the language selected in **Select Preferences** > **User Preferences** > **User Workspace** > **Language** box. If the selected language is not supported, Release Control uses the default language in the **System language** box in **Module** > **Administrator** > **Configuration** > **Integrations** > **Server**.
> - The language you want to use needs to have already been added to Release Control.

Create a Link Using Tenant Parameters

The Release Control server can be configured to serve multiple tenants. You can create a link that opens Release Control to a specific tenant.

To create a link to the Release Control application:

From an internet browser, enter one of the following URLs:

```
http://<RC installation home>/ccm?requestOrigin=EXTERNAL&<customizable
parameters>&<tenant_field_val>
```

or

```
http://<RC installation home>/ccm?requestOrigin=EXTERNAL&<customizable
parameters>&<tenant>
```

where

- **tenant** is the tenant name as defined in Release Control.
- **tenant_field_val** is the tenant allocation field whereby change request tickets from the service desk application are allocated to tenants in Release Control based on the value of this field.

> **Note:** You can only use one of the parameters at a time in the URL.

For example:

```
http://localhost:8080/ccm?requestOrigin=EXTERNAL&filterName=any&
perspective=calendar&tenant_field_val=CompanyX
```

> **Caution:** The URL must contain at least one **filterName** or **field-<field name>** parameter.

Generate Links to Service Manager Tickets

This task describes how to create links to Service Manager tickets via the Web tier.

Step 1: Allow access to Service Manager via URL links

By default, Service Manager 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 Service Manager via URL links. For more information, see Allow Access to Service Manager via URL Links.

> **Note:** You can also disable this secure query requirement in the Web.xml file (**querySecurity** in Service Manager.

Step 2: Configure the URL for the request-id Field

Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Fields**.

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

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?
  smOperation=edit&IsmFromSystem=ReleaseControl&IsmSubject=125
  &IsmEntityType=Change&IsmToSystem=ChangeManager
  &IsmProtocolVersion=1.0&IsmEntityID=%%request-id%%
  ```

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

  ```
  <Service Manager 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:

  ```
  %%origin-url%%
  ```

Save and apply the configuration set. For details, see Save and Apply Configuration Changes.

Allow Access to Service Manager via URL Links

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

To generate a secure URL query:

1. In Service Manager, add a new change request field named **url**. This field contains 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	

   e. Create a **Format Control Calculation** entry that generates 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.

i. Select **Tailoring** > **Format Control**.

ii. In the **Name** box, type the record name:
   - For cm3r records, type `cm3r`.
   - For cm3t records, type `cm3t`.

   A. 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.getURLFromQuery", "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.getURLFromQuery", "cm3t", $query, $title)

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

   B. Save your modifications to the Format Control table.

3. Check that the exact machine name (**My Computer** > **Properties** > **Computer Name**) is properly defined (case sensitive) in the following places:
   - On the 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`).
4. Restart the Service Manager server.
5. Regenerate the Web Services stub file (**.jar**):
   a. Run the **ServiceManagerWsdlGen.bat** utility in the **<Release Control Installation directory>\bin** directory.
   b. Copy the **tomcat** folder from the **<Release Control installation directory>\bin\result** directory, and paste it into the **<Release Control installation directory>\apps\SDI-<adapter name>\WEB-INF\lib**directory.

6. Map the **url** field that you created in Service Manager to the **origin-url** field in Release Control by editing the conversion scripts for changes and tasks.
   For example, in the **convertChange.js** file and the **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"));

         ....

}
```

7. Continue with configuring the URL for the request-id field, as described in step 2 of Generate Links to Service Manager Tickets.

Update the SDI Operations Script to Support the Deny Function

Perform the following steps to configure the integrated service desk to support the **Deny** function. For information about the Deny function in the SDI operations script, see SDI Operations Script.

1. Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Service Desk Adapters** > **SDI operations script** and download the SDI operations script file in the right pane.
2. Add the following function to the script:

```
function canDeny(genericRFC, userLoginName) {

return canApprove(genericRFC, userLoginName);

}
```

3. Save and activate your configuration changes (see Save and Apply Configuration Changes).

Reference

SDI Operations Script

This pane contains the **sdOperations.js** script. For certain operations, Release Control sends information to the integrated service desk according to the conditions defined in the **sdOperations.js** script.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Service Desk Adapters** > **SDI operations script**. **Note:** For details about editing this file, see Configure Files in the Configuration Tab.
Important information	This script is only relevant for the following service desks: • Service Manager • Project and Portfolio Management / IT Governance Center
Relevant tasks	Updating Approval Status in the Service Desk

User interface elements are described below:

UI Elements (A-Z)	Description
<Functions included in the sdOperations.js script>	• **canApprove**. Defines when the **Approve** button in the Analysis module **Collaborate > Resolution** tab is enabled. (Applies to Service Manager and Project and Portfolio Management / IT Governance Center) • **canRetract**. Defines when the **Retract** button in the Analysis module **Collaborate > Resolution** tab is enabled. (Applies to Service Manager) • **canDeny**. Defines when the **Deny** button in the Analysis module **Collaborate > Resolution** tab is enabled. (Applies to Service Manager) **Note:** To support the canDeny function, you must update the sdOperations.js script. For details, see "Update the SDI Operations Script to Support the Deny Function" on the previous page. • **canUpdateReview**. Defines when the **Review** button in the Analysis module **Review > Conclusions** tab is enabled.

UI Elements (A-Z)	Description
	(Applies to Service Manager) • **canUpdateStatus**. Defines when you can update the actual start and end time of an activity in the Director and Implementor modules. These times are automatically updated in the originating service desk ticket. (Applies to Service Manager) • **canUpdatePlannedTimes**. Defines when you can save the updated start and end times in the Analysis module Change Planner. These times are automatically updated in the originating service desk ticket. (Applies to Service Manager) • **canClose**. Defines when the **Close** button in the Analysis module **Review > Conclusions** tab is enabled. (Applies to Service Manager) **Note:** For a detailed explanation of the objects that can be included in the script functions, refer to the **API_ Reference.chm** file. (To access the API Reference, select **Start** > **Programs** > **Release Control 9.60** > **Documentation** and open the **pdfs** directory).

Service Desk Adapter Properties

When you perform the initial configuration of your service desk using the service desk configuration utility (**SdiConfigurer.bat)**, a service desk adapter configuration file is created containing all the service desk integration properties.

This section describes the properties of the adapter configuration file that you can modify to suit your needs.

For details about modifying the service desk adapter, see Modify Service Desk Adapter Properties.

This section also includes:

- Common Adapter Attributes
- BMC Remedy Action Request System Connector Settings
- XML Connector Settings
- Service Manager Connector Settings
- Service Desk Connector Settings
- Project and Portfolio Management/ IT Governance Center Web Services Connector Settings

- Server Automation Connector Settings
- Network Automation Connector Settings
- Database Connector Settings

Common Adapter Attributes

The top section of the adapter configuration file contains the following adapter attributes, which are common to all service desk applications. You can modify the following properties:

Property Name	Description

connection-properties	Lists the common properties for request-type levels 1 and 2 so that these properties do not have to be duplicated.
	• If you had not initially configured both Service Manager and Release Control to use Lightweight Single Sign-On (LW-SSO), you can set the **requiresUserCredentials** parameter to enable login without entering the required credentials. For example, if a change request ticket has been submitted and a user wants to update Service Manager with an approval of the request.
	The parameter options are:
	  ○ **False** Enables you to log in to the system without being asked to enter your credentials.
	  ○ **True (default)** You are prompted to enter your credentials when logging in to the system.
	• You also need to modify the **serviceURL** parameter to enable connection to the Service Manager server.
	To see an example, see Configure Release Control and Service Manager with LW-SSO.

number-of-tickets	Sets the number of requests that are processed at a time, ensuring that Release Control and service desk application resources, such as memory and network bandwidth, are not over-used. The **number-of-tickets** can be as high as required, although you should be careful not to overload Release Control or your service desk application. It must be high enough to retrieve all requests from the service desk application and must exceed the expected number of requests that the service desk application updates in one measurement time slot. For example, if the service desk application updates 50 requests in one second, the **number-of-tickets** must exceed 50. In processing requests, Release Control attempts to use the **number-of-tickets**, but may return more or fewer requests from the service desk application.

Property Name	Description
	Note: To determine the **number-of-tickets**, consult with the people responsible for the service desk applications within your organization.

polling-schedules	The schedule according to which the service desk application is polled for change requests. This schedule is determined by a cron expression. By default, there is one cron expression that defines the polling interval at 30 seconds. You can modify the polling interval as required. For example, you can:
	• Increase the polling interval (the service desk application is polled less often) if:
	  ◦ You want Release Control to check the service desk application for new tickets less frequently.
	  ◦ Are likely to perform a mass update of tickets. This will prevent a situation in which Release Control receives more tickets per time interval than it can process.
	• Decrease the interval (the service desk application is polled more often) if you want Release Control to be updated more frequently with change request modifications.
	
	You can edit the Cron expression or add multiple expressions, separated by the new line character. For example:
	`<polling-schedules>`
	`0/30 * * * * ?`
	`0/50 * * * * ?`
	`</polling-schedules>`
	
	For more information about cron expressions, see http://www.quartz-scheduler.org/documentation

initial-load-state	**Note:** This property is not relevant when configuring Service Manager or database adapters. For information about how to configure the adapter to collect change requests from a specific date from Service Manager and database applications, see "Retrieve all change requests from a specified date (from Service Manager and database service desk applications only)". If you specify a string date, the adapter collects all requests from the specified creation date through the current date, at one time and does not continue to collect new or updated requests. By default, this property is disabled and has no value. When enabled, this property overrides the polling-schedule.

Property Name	Description
	If you enable this property, you need to delete the SDI persistency using the **SDI Persistency Cleanup** utility (see SDI Persistency Cleanup). After Release Control completes the process of collection the requests, you need to disable this property by commenting out the line. **Format**: `MM/dd/yy HH:mm:ss z`
request-types (mandatory)	Lists all request types that the adapter collects, including all request type levels. By default, level 1 is used for changes and level 2 is used for tasks. For an explanation of the request type properties and operation properties to be included as part of the **<request-type>** element, see Request Type Properties.

Request Type Properties

(The **<request-type>** element includes the following properties:

Property Name	Description
connection-properties	Lists the properties for polling and operation connectors for each request level.

The **<operation>** element (under **<operations>** within **<request-type>**) includes the following operation properties:

Property Name	Description
name (mandatory)	The operation name to be used in locating the operation. The following operations are currently supported: approve, canApprove, retract, canRetract, deny, canDeny, reviewUpdate, canUpdateReview, updatePlannedtimes, canUpdatePlannedTimes, updateStatus, canUpdateStatus, close, canClose, updateAnalysisData. Some of the operations are only supported by specific service desks.
operation-type (mandatory)	Defines the type of operation to be performed. It is recommend not to change this property.
connector (under operation)	Defines the operation connector to be used for the execution of the operation.

Property Name	Description
(mandatory)	It is recommend not to change this property.
sender-properties	>Overrides the default properties that are used when initializing a sender for the operation.

BMC Remedy Action Request System Connector Settings

The following connector attributes can be configured in the BMC Remedy Action Request System adapter configuration file:

Property Name	Description
serverName (mandatory)	The name of the BMC Remedy Action Request System server. **Note:**This property is configured by the service desk configuration utility **(SdiConfigurer.bat)**.
userName (mandatory)	The user name with which Release Control connects to the BMC Remedy Action Request System server. **Note:** This property is configured by the service desk configuration utility **(SdiConfigurer.bat)**.
userPassword (mandatory)	The password with which Release Control connects to the BMC Remedy Action Request System server. Note that the password should be encrypted. For details, see Password Encryption. **Note:** This property is configured by the service desk configuration utility **(SdiConfigurer.bat)**.
schemaName (mandatory)	The name of the schema containing the required change requests.
field-names (mandatory)	A comma-separated list of request fields to retrieve. Use * to collect all request fields.
associationSchemaName	The schema that associates the CIs to the tickets in the BMC Remedy ARS server. **Note:** Only applicable to BMC Remedy 7.0
idFieldNameInTicket	The name of the column that contains the ticket ID to be used in the association schema. **Note:** Only applicable to BMC Remedy 7.0

Property Name	Description
associationForeignIdFieldName	The name of the column that contains the foreign ID of the CIs in the association schema. **Note:** Only applicable to BMC Remedy 7.0
associationResultFieldName	The field name of the ticket (in the Raw Ticket) to contain the array of associated CIs from the association schema. **Note:** Only applicable to BMC Remedy 7.0

XML Connector Settings

The following connector attributes can be configured in the XML adapter configuration file:

Property Name	Description
idPropertyName (mandatory)	The property name of the request's ID in each XML file to which service desk application requests are sent.

creationDatePropertyName
(mandatory)
	The property name of the request's **creation-date** value in the XML file.
	If the **creation-date**is an XML element, use the element's name. For example, you would use the property name **creation-date** for the following:
	`<change-request>`
	`<creation-date>01/01/01</creation-date>`
	`</change-request>`
	If the **creation-date** is an attribute of the request's XML element, use **@<element name>**. For example, you would use the property name **@creation-date** for the following:
	`<change-request creation-date="01/01/01">`
	`</change-request>`

dateFormat (mandatory)	The format of the **creation-date** value in the XML file.
directoryName (mandatory)	The path of the shared directory in which the service desk application requests are placed in XML file format. **Note:** This property is configured by the service desk configuration utility **(SdiConfigurer.bat)**.
pattern	The file name pattern as a regular expression.

Property Name	Description
	For more details, see http://java.sun.com/j2se/1.4.2/docs/api/java/util/regex/Pattern.html.

Service Manager Connector Settings

The following connector attributes can be configured in the Service Manager adapter configuration file:

Property Name	Description
idProperty	The property name of the ID field in the instance returned from the Service Manager Web service.
lastUpdatedPropertyForQuery	The property name of the **last-update** field used to query the Service Manager Web service (the field name used in an expert search on the Service Manager client machine).
creationDatePropertyForQuery	The property name of the **creation-date** field used to query the Service Manager Web service.
lastUpdatedPropertyForResult	The property name of the **last-update** field in the instance returned from the Service Manager Web service (usually the field name exposed as API).
creationDatePropertyForResult	The property name of the **creation-date** field in the instance returned from the Service Manager Web service.
keyMethodName	The name of the method for request keys (usually the ID field name).
startFrom (mandatory)	Indicates the past time and date from which to start fetching tickets. For example, `13/01/2000 00:00:00 EST`.
upperLimitDelta (optional)	Defines the interval that indicates how often Release Control fetches tickets. The value is defined in milliseconds. **Note:** By default, the **upperLimitDelta** property does not appear in the **<adapter name>-adapter.settings** file. If you want to define a value for it, you must add the property manually to the file in the **<connection-properties>** section.
timeZone	The Service Manager server time zone, used for converting the last updated time of a request from Service Manager. After setting the time zone, you need to ensure that the **queryDateFormatPattern** property described below, matches the time zone definition.

Property Name	Description
	Notes: • Enter the time zone as it appears in the Java database. • To handle Daylight Savings Time, use an area time zone instead of specifying a time relative to GMT.
wsDateFormatPattern	The date format used in the Service Manager Web service answer. For available formats, see: http://java.sun.com/j2se/1.4.2/docs/api/java/text/SimpleDateFormat.html
queryDateFormatPattern	The date format used for querying the Service Manager system (as used in the UI expert search). For available formats, see: http://java.sun.com/j2se/1.4.2/docs/api/java/text/SimpleDateFormat.htm
serviceUrl	The Web service URL. **Note:** This property is configured by the service desk configuration utility (**SdiConfigurer.bat**).
userName	The user name with which Release Control connects to the Service Manager system. **Note:** This property is configured by the service desk configuration utility (**SdiConfigurer.bat**).
password	The password with which Release Control connects to the Service Manager system. **Notes:** • The password can be encrypted. For details, see Password Encryption. • This property is configured by the service desk configuration utility (**SdiConfigurer.bat**).
additionalConstraintsForPolling (optional)	An additional filter criteria to allow more flexibility in what changes are fetched in the polling mode. The syntax for this constraint is the same as the one used by Service Manager's Expert Search. **Note:** This is implemented by appending an **and (<constraint>)** to the Service Manager query.

Service Desk Connector Settings

The following connector attributes can be configured in the Service Desk adapter configuration file:

Property Name	Description
connector-type (mandatory)	For top-level requests, this must be set to: `hpsdChange` For second-level requests, this must be set to: `hpsdWorkOrder`
idProperty (mandatory)	The property name of the ID field in the instance returned from Service Desk.
lastUpdatedProperty (mandatory)	The property name of the **last-update** field.
createdProperty (mandatory)	The property name of the **creation-date** field.
serviceUrl (mandatory)	The URL of the Web service. Format: `[<Service Desk server IP address>:<Service Desk server port>]` **Note:** The server port is generally 30999. This property is configured by the service desk configuration utility **(SdiConfigurer.bat)**.
userName (mandatory)	The user name with which Release Control connects to Service Desk. **Note:** This property is configured by the service desk configuration utility **(SdiConfigurer.bat)**.
password (mandatory)	The password with which Release Control connects to Service Desk. **Note:** The password can be encrypted. For details, see Password Encryption. This property is configured by the service desk configuration utility **(SdiConfigurer.bat)**.

Project and Portfolio Management / IT Governance Center Web Services Connector Settings

The following connector attributes can be configured in the Project and Portfolio Management / IT Governance Center adapter configuration file:

Property Name	Description
requestTypeName (mandatory)	The name of the Project and Portfolio Management/IT Governance Center request type to be retrieved. Note that this field is case-sensitive.
parentRequestTypeName (mandatory, if the request is a second-level request with a parent request)	The name of the Project and Portfolio Management/IT Governance Center parent request type to be retrieved, if the request is a second-level request (meaning it has a parent request associated with it).
username (mandatory)	The user name with which Release Control connects to Project and Portfolio Management/IT Governance Center. **Note:** This property is configured by the service desk configuration utility **(SdiConfigurer.bat)**.
password (mandatory)	The password with which Release Control connects to Project and Portfolio Management/IT Governance Center. Note that the password should be encrypted. For details, see Password Encryption. **Note:** This property is configured by the service desk configuration utility **(SdiConfigurer.bat)**.
serviceUrl (mandatory)	The URL of the Project and Portfolio Management/IT Governance Center Web service. **Note:** This property is configured by the service desk configuration utility **(SdiConfigurer.bat)**.
sourceStepSequence	If you are configuring your environment so that users can approve steps in Project and Portfolio Management from Release Control, define the step in Project and Portfolio Management in which the approval will be effective. **Note:** This property may be configured by the service desk configuration utility **(SdiConfigurer.bat)**.
dbURL	Include a valid Oracle DB SID (System ID), server name, and port. **Note:** This property may be configured by the service desk configuration utility **(SdiConfigurer.bat)**.
userName	Oracle DB user name. **Note:** This property may be configured by the service desk configuration utility **(SdiConfigurer.bat)**.

Property Name	Description
password	Oracle DB password. **Note:**This property may be configured by the service desk configuration utility **(SdiConfigurer.bat)**.

Server Automation Connector Settings

The following connector attributes can be configured in the Server Automation adapter configuration file:

Property Name	Description
saServerUrl (mandatory)	The URL of the Server Automation server. **Note:** This property is configured by the service desk configuration utility **(SdiConfigurer.bat)**.
saUsername (mandatory)	A valid user name to access the Server Automation server. **Note:** This property is configured by the service desk configuration utility **(SdiConfigurer.bat)**.
saPassword (mandatory)	A valid password to access the Server Automation server. **Note:** This property is configured by the service desk configuration utility **(SdiConfigurer.bat)**.
trustCertFile (mandatory)	The location of Server Automation's security certificate file. This file may be located at **var/opt/optsware/crypto/coglib/opsware-ca.crt**
filterRelevantJobs	A list of the types of jobs that are imported to Release Control. For more details, refer to the Opsware Automation Platform Developers Guide for search filter syntax. **Default:** All jobs of status **Pending** or **Recurring**.

Network Automation Connector Settings

The following connector attributes can be configured in the Network Automation adapter configuration file:

Property Name	Description
naServerURL (mandatory)	The URL of the Network Automation server. **Note:** This property is configured by the service desk configuration utility **(SdiConfigurer.bat)**.

Property Name	Description
naUsername (mandatory)	A valid user name to access the Network Automation server. **Note:** This property is configured by the service desk configuration utility **(SdiConfigurer.bat)**.
naPassword (mandatory)	A valid password to access the Network Automation server. **Note:** This property is configured by the service desk configuration utility **(SdiConfigurer.bat)**.
timeZoneString	The format for determining the time zone when converting requests located in a different time zone. To change this to a specific time zone, use the Java naming conventions for time zones. **Default**: UTC
dateFormatString	The date and time format.
queryStatus	Tasks are imported only if they have one of the statuses listed in this tag.
daysBefore	This number determines how many days before the current date tasks are imported from Network Automation (for example, 14 means import all tasks scheduled up to 14 days before today).
daysAfter	This number determines how many days after the current date tasks are imported from Network Automation (for example, 7 means import all tasks scheduled up to 7 days after today).
excludeTaskTypes	A list of task types which are NOT imported from Network Automation.

Database Connector Settings

The following connector attributes can be configured in the database configuration file:

Property Name	Description
dbUrl (mandatory)	The URL of the database. **Note:** This property is configured by the service desk configuration utility **(SdiConfigurer.bat)**.
userName (mandatory)	The user name with which Release Control connects to the database. **Note:** This property is configured by the service desk configuration utility **(SdiConfigurer.bat)**.

Property Name	Description
password (mandatory)	The password with which Release Control connects to the database. Note that the password should be encrypted. For details, see Password Encryption. > **Note:** This property is configured by the service desk configuration utility **(SdiConfigurer.bat)**.
driverClassName (mandatory)	The name of the JDBC driver. Ensures that the driver exists in the **<Release Control installation directory>\tomcat\lib** directory.
idSelectQuery (mandatory)	The SQL query that returns the set of change request IDs according to the requests' **last-updated** field value. **Important:** The query must not include the date of the last change request that was retrieved to avoid getting an infinite loop in which the same change requests are retrieved each time. To avoid this, you must NOT use a greater than and equal to sign (>=). You must use only a greater than (>) sign. Example of a correct query: A correct query includes a date which is greater than the date on which the last change request was retrieved. For example, if the last change request was retrieved on February 1, 2010, set the date as follows: `select change_id from changes where last_updated > 2/1/2010`
startFrom (mandatory)	Indicates the past time and date from which to start fetching tickets. For example, `13/01/2000 00:00:00 EST`.
upperLimitDelta (optional)	Defines the interval that indicates how often Release Control fetches tickets. The value is defined in milliseconds. > **Note:** By default, the **upperLimitDelta** property does not appear in the **<adapter name>-adapter.settings** file. If you want to define a value for it, you must add the property manually to the file in the **<connection-properties>** section.
ticketFetchQuery (mandatory)	The SQL query that returns a set of change request according to the requests' ID. For example: `select * from changes where ID = ?`
lastUpdatedFieldName (mandatory)	The name of the column in the result set that contains the **last-update** field value.

Property Name	Description
lastUpdatedFieldType (mandatory)	One of the following values: **time**, **timestamp**, **date**, **milliseconds**, or **seconds**.
idFieldName (mandatory)	The name of the column in the result set that contains the ID field value.

connectionProperties	The database properties, in java.util.Properties format.
	For example:
	`key1=value1`
	`key2=value2`

connectionPoolProperties	The database pool connection properties, in java.util.Properties format. For possible values, see: http://www.mchange.com/projects/c3p0/index.html

Rules and Syntax for Creating Links to Release Control

The following list contains various rules, tips, and syntax requirements regarding the URLs used when creating links to Release Control.

- 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 returns an exception.

URL Parameters for Customized Links

You can create links to Release Control from your service desk (see Linking to Release Control Interfaces from the Service Desk.)

The following table describes the available parameters for the URL:

Parameter	Description
filterName	Filters the requests displayed in 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 Release Control Analysis or Director module.
field-<field name>	Filters the requests displayed in Release Control according to the field values defined in this parameter. For example, **field-status=APPROVED,CLOSED.** For information about where to find allowed values for the fields used in this parameter, see Field Parameter Values Used in Links to Release Control. **Notes:** • All field names must start with the **field-** prefix. • Fields used in this parameter must be defined as filterable in Release Control. • Field names should be written as they appear in the **Administrator module fields** pane (Select **Module** > **Administrator** > **Configuration** tab > **Integrations** > **Fields**.) For details, see Fields Pane. • 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 overwrites the value in the filter. • You can specify multiple **field-<field name>** parameters.
timestamp	The date on which you want the calendar to open. The date is represented as a timestamp in milliseconds. **Note**: If no timestamp is defined, the default date is the current date.
perspective	**Note:** This parameter is only relevant when creating a link to the full Release Control application. The view in which the Analysis module opens. You can set the

Parameter	Description
	following values: • **RFCViewer.** Opens the List view. • **calendar.** Opens the Calendar view (default).

Field Parameter Values Used in Links to Release Control

When you create a link to Release Control from a service desk, you can use a field name parameter as part of the URL. This section describes where to find the allowed values for fields used in the **field-<field name>** parameter. Values are defined in:

- The service desk application
- The Universal CMDB
- The Enumerations pane (select **Module** > **Administrator** > **Configuration** > **Integrations** > **Enumerations**)
  In the Enumerations pane, you can view the allowed values for each field in the Enumeration Entries table. For details, see Enumerations Pane.

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 Universal CMDB)
category	Values as defined in the service desk ticket
change-type	• REGULAR • LATENT • SURROGATE • AUTOMATED
collision-severity	• NONE • VERY_LOW • LOW • MEDIUM

Field Name	Corresponding Enumeration Value
	• 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	Enumerations pane
implementation-outcome	Enumerations pane
implementors	Values as defined in the service desk ticket
lastImpact-cis-label	System CI labels (as defined in Universal CMDB)
lastImpact-cis-refId	System CI IDs (as defined in Universal CMDB)
opinion-type	Enumerations pane
priority	Enumerations pane
review-customer-satisfaction	Enumerations pane
review-planning-satisfaction	Enumerations pane
status	Enumerations pane
subcategory	Values as defined in the service desk ticket
ticket-level	Enumerations pane

Troubleshooting and Limitations

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

Problems Saving Post Implementation Review Comments to Service Manager

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

1. In the 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 click the **New Field/Key** button.
4. Type **closure.comments** in the **name** box, and type **array** in the **type** box.
5. Click the **Add Field** button.
6. A similar window opens. Enter **character** in the **type** box.
7. Click the **Add Field** button.

Label and Term Configuration

This chapter includes:

Concepts

- Configuring Default Display Labels and Terms Overview

Reference

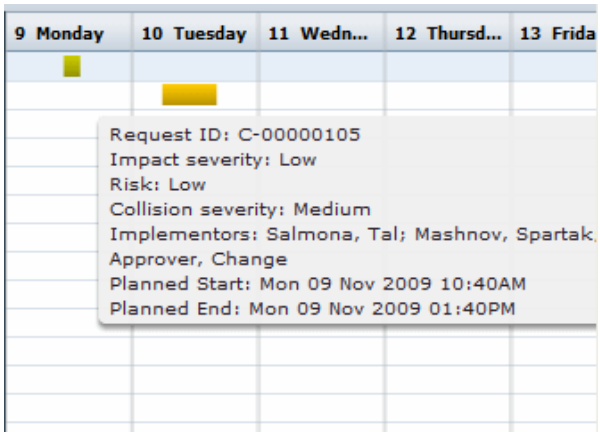
- Labels and Terms Pane

Concepts

Configuring Default Display Labels and Terms Overview

You can change the way in which the labels and terms for the user interface elements are displayed in Release Control by modifying their default display values in the scripts in the **Labels and Terms** pane in the Administrator module.

For example, in the **enumeration-labels.properties** script, you can define the colors that indicate the impact severity level of the change request in the Change Requests — Calendar View.



The default language in which the labels and terms in the Release Control user interface are displayed is English (United States). Currently, Release Control supports English only. If required, you can translate the labels and terms into other supported languages.

> **Notes:**
>
> - After translating the required strings, be sure that you change the language Release Control uses for its user interface display (select the required language in the Auto detect language settings box in the User Workspace Pane).
> - The changes you made in label properties will take effect after you restart the Release Control Server services. An example of a label properties update would be changing enumerations from **PriorityEnum.IMMEDIATE=Immediate** to **PriorityEnum.IMMEDIATE=Critical**.

For more information, see Labels and Terms Pane.

Reference

Labels and Terms Pane

This pane enables you to change the way in which the terms and labels for the user interface elements are displayed in Release Control.

To access	Select **Module** > **Administrator** > **Configuration** > **Labels and Terms**.
Important Information	The default language in which the labels and terms in the Release Control user interface are displayed is English (United States). If required, you can translate the labels and terms into other supported languages. After translating the required strings, be sure that you change the language Release Control uses for its user interface display (select the required language in the Auto detect language settings box in the User Workspace Pane).
See also	Configure Files in the Configuration Tab

User interface elements are described below:

UI Elements (A-Z)	Description
Locale	The default language in which the labels and terms in the Release Control user interface are displayed.

The Label and Term panes are described below:

UI Elements (A-Z)	Description
customizable-labels.properties	Maps the business terms used in Release Control to their default display values. You can modify the way in which Release Control displays each of the business terms listed in this file. For example, you may want to rename the term for the time period **Neutral to Changes** as **Neutral**. To do so, change the line: **timeperiod.type.neutraltochanges.label=**`Neutral to Changes` to: **timeperiod.type.neutraltochanges.label=**`Neutral`
enumeration-labels.properties	Maps the configured enumeration fields in Release Control to their default display values. You can modify the way in which Release Control 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, 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**, 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 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:

UI Elements (A-Z)	Description
	LevelEnum.1=`Change` **LevelEnum.2=**`Task` **LevelEnum.Level.UNKNOWN=**`Unknown` > **Note:** Do not change the default keys to the left of the equal sign (=). You can only modify the values to the right of the equal sign (=).
fields-labels.properties	Maps the fields in Release Control to their default display values. You can modify the way in which Release Control displays each of the fields listed in this file. For example, you may want to rename the **Planned Start** field as **Planned Start Time**. To do so, you would change the line: **fields.planned-start-time.label=**`Planned Start` to: **fields.planned-start-time.label=**`Planned Start Time` > **Note:** Do not change the default keys to the left of the equal sign (=). You can only modify the values to the right of the equal sign (=).
override-labels.properties	The resource files that map the labels in Release Control to their default values are located in: **<Release Control installation directory>\RC920\apps\ccm\WEB-INF\lib\<ccm-l10n-*.jar files>**. The **override-labels.properties** script enables you to override the default label values located in the **ccm-l10n-*.jar files**. > **Note:** The **override-labels.properties** script is empty by default. To override a default label value: • Edit the required string in the relevant **<ccm-l10n-*.jar>** file. For example, to rename the **Time Periods** field as **Change Windows**, change the line: **admin.main.timePeriodsSettings.title=**`Time Periods` to: **admin.main.timePeriodsSettings.title=**`Change Window`. • Search the text for any instances of `Time Periods` and change them to `Change Windows`. • Copy the modified string to the **override-labels.propreties** file.

Module Configuration

This chapter includes:

Concepts

- Configuring Notifications Overview
- Configuring Reports Overview

Tasks

- Configure Dashboard Settings

Reference

- Value Expressions
- Notification Rule Configuration
- Modules Configuration User Interface

Concepts

Configuring Notifications Overview

By default, only automatic email notifications and non-customized notifications are sent by Release Control. It is recommended, however, that you configure notifications to be sent to users who do not regularly work with 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 **change-flow.js** script, located in the Change Flow Script pane in the Administrator module, using the **getUsersToNotify** function. For details, see Change Flow Script Pane.

For details about how to configure a notification rule using the **getUsersToNotify** function, see Notification Rule Configuration.

For details on how to configure notification properties, and the format of the emails that Release Control sends in the **ftl** files, see Notifications Pane.

Configuring Reports Overview

You can customize the reports generated by Release Control in the Analysis module. Release Control uses JasperReports as the report engine.

The report template files are located in the Reports pane in the Administrator module. For a description of these reports, see Reports Panes. You can download the latest version of the iReport tool from http://sourceforge.net/projects/ireport/ and use the iReport tool to edit these report templates.

You can use value expressions to customize your reports. For details, see Value Expressions.

> **Note:**
>
> 1. After editing the reports, there is no need to restart the Release Control server.
> 2. To verify your editing changes, you can generate the report in the Analysis module.

Tasks

Configure Dashboard Settings

The **<Release Control installation directory>\conf\Dashboard_Objects_Export.xml** file contains definitions for the Release Control Default Page in the Dashboard. If you changed the **Pending Approval** or **Closed** status in the **Module** > **Administrator** > **Configuration** > **Integrations** > **Enumerations** pane, you must update the **Dashboard_Objects_Export.xml** file with the alternative status or statuses that you are using.

This task describes how to update the **Closed** and **Pending Approval** statuses.

This section includes:

Step 1: 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 **Module** > **Administrator** > **Configuration** > **Integrations** > **Enumerations**. For details, see Enumerations Pane.

3. Replace **[Closed]** with the label you assigned to the above status in **Module** > **Administrator** > **Configuration** > **Labels and Terms**. For details, see Labels and Terms Pane.

Step 2: 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 **Module** > **Administrator** > **Configuration** > **Integrations** > **Enumerations**. For details, see Enumerations Pane.

3. Replace **[Pending_Approval]** with the label you assigned to the above status in **Module** > **Administrator** > **Configuration** > **Labels and Terms**. For details, see Labels and Terms Pane.

Reference

Value Expressions

You can define value expressions using report parameters, variables, and fields, and you can use Java expressions to customize your report.

For details about the report templates used for the reports generated in the Analysis module's List and Calendar views, see Reports Panes.

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 Release Control API. For information on the **GenericRFC** class, refer to the **API_Reference.chm** file. (To access the API Reference, select **Start** > **Programs** > **Release Control 9.60** > **Documentation** and open the **pdfs** directory).

Java Expressions

You can use Java expressions to customize your reports. For example, if the user interface 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.

Notification Rule Configuration

You use the **getUsersToNotify** function in the **change-flow.js** script located in **Modules** > **Administrator** > **Configuration** tab > **Change Process** > **Change flow 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 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) {

     return false;

/*
```

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


    var message = "";
    var riskStatusStr = "is ";


    var riskIncreased = true; // start by assuming risk increased (relevant to
when the change first arrives)


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


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

> **Note:** For details on risk calculations, see Risk Analysis.

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

```
if (statusIsPendingApproval && riskIncreased && riskAboveThreshold) {
    var 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 (notificationContext.hasUsers()) {// if there are users affected by this
request, then notify them to check it out

message = "This request potentially affects one or more applications for which
you are registered " +

"to receive notifications.\n" + message;
```

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

```
} else {

    notificationContext.addUsersByRole("Administrator");

    message = "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 a 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. (To access the API

Reference, select **Start** > **Programs** > **Release Control 9.60** > **Documentation** and open the **pdfs** directory).

Modules Configuration User Interface

This section includes:

- Analysis Pane
- Analysis Info Pane
- Calendar Pane
- Charts Pane
- Filter Pane
- General Info Pane
- Notifications Pane
- Reports Panes
- Dashboard Pane
- Director Pane
- Alerts Pane

Analysis Pane

This pane defines default properties for some of the tabs in the Analysis module.

To access	Select **Modules** > **Administrator** > **Configuration** tab > **Modules** > **Analysis**.

User interface elements are described below:

UI Elements (A-Z)	Description
Change refresh frequency	Enables you to set the refresh interval in the Change Planner dialog box and the Change Approval pane in the **Collaborate** > **Resolution** tab. **Default:** 5000 (in milliseconds)
Maximum impact search result size	Enables you to define the maximum number of impact CIs that Release Control can display per change request. When this limit is

UI Elements (A-Z)	Description
	reached, Release Control displays the following message: `Impact CIs (Too many CIs to display. Please refine the search criteria.)` **Default:** 2000
Name	The name of the tab in the Analysis module.
Tab Visibility	Hide or display the tab in Release Control.
Use Eager Loading	• If selected, the data is retrieved automatically. • If not selected, the data is retrieved only on demand.

Analysis Info Pane

This pane defines default properties for some of the fields in the Analysis module.

To access	Select **Modules** > **Administrator** > **Configuration** tab > **Modules** > **Analysis** > **Analysis Info**.

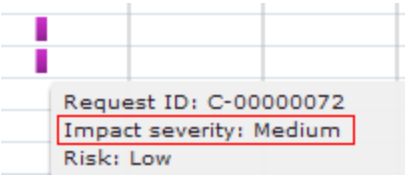
User interface elements are described below:

UI Elements (A-Z)	Description
Field	The name of the field in the Analysis module.
Visibility	Hide or display the field in Release Control.

Calendar Pane

In this pane you can define a color mapping scheme that enables you to associate a color with an existing field value in the Change Requests — Calendar View and the <Change Request Summary Chart Pane>.

For example, if you map **Medium** for impact severity to purple, a change request whose impact severity is **Medium**, appears purple in **Day** or **Week** mode in the Calendar view. When viewing the field in graphic format (in the <Change Request Summary Chart Pane>), the pie slice or column representing that field appears purple.



You can also define the first day of your business week as well as the number of working days in your week.

To access	Select **Modules** > **Administrator** > **Configuration** tab > **Modules** > **Analysis** > **Calendar**.
See also	Change Requests — Calendar View

User interface elements are described below:

UI Elements (A-Z)	Description
Color by field	The field whose values you are mapping to a color.
Default color	The color to which a field value is mapped if no color is defined for that value. **Default:** Gray
First day of week	Sets the selected day as the first day of your business week. **Default:** Monday
Number of working days	Determines the number of working days in the week.
Jump to start date of selected change	Controls whether the date jumps to the planned start date of the selected change or not when switching to the Day view.

Calendar Color Mapping Pane

This pane enables you to map an existing field value to a color in the Change Requests — Calendar View and the <Change Request Summary Chart Pane>.

User interface elements are described below:

UI Elements (A-Z)	Description
	Add configuration to configuration set. Enables you to add an existing field value to the field selected in the **Color by Field** box.
	Remove configuration from configuration set. Enables you to delete the selected field value and its associated color.
Color	Defines the color you want to associate with the field value. Click

UI Elements (A-Z)	Description
	the color box to select the required color. If a color is not defined, it is mapped to the default color defined in the **Default color** box in the Calendar pane.
Field value	An existing field value that is defined for the field you selected from the **Color by field** list. **Note:** Ensure that the field values you define are valid for the field you selected from the **Color by field** list. For example, let us assume that you defined the values Critical, High, Medium, and Low for the **Impact Severity** field. If you then select the **Contact Person** field from the **Color by field** list, Release Control no longer displays the values Critical, High, Medium, and Low since they are not valid values for the **Contact Person** field.

Charts Pane

The monthly Change Requests — Calendar view in the Analysis module displays:

- The change requests that have been processed by Release Control for each calendar day of the selected month.
- Graphs that represent the data of a specific field for the change requests that are included in the currently active filter.

This pane enables you to select the fields whose data you want to appear in the monthly Calendar view, as well as determine the default graphic format in which the data is displayed.

For more information on the Calendar view, see Change Requests — Calendar View.

To access	Select **Modules** > **Administrator** > **Configuration** tab > **Modules** > **Analysis** > **Charts**.

User interface elements are described below:

UI Elements (A-Z)	Description
	Add configuration to configuration set. Enables you to add a field.
	Remove configuration from configuration set. Enables you to delete the selected field.

UI Elements (A-Z)	Description
	Note: If you delete all the fields in this pane, no graphs appear in the monthly Calendar view.
Enabled	Select the fields you want to appear in graphic format in the monthly Calendar view. **Notes:** • You can enable a maximum of four fields. • If you do not enable any of the fields, no graphs appear in the monthly Calendar view.
Field	Select the fields whose data you want to appear in graphic format in the **<Change Request Summary Chart pane>** in the Calendar view. **Note:** Only those fields that are defined as **Enabled** appear in the monthly Calendar view.
Type	Select the format in which you want the data displayed. The options are: • Pie chart • Column graph

Filter Pane

This pane defines default properties for some of the filter items in the Analysis module.

To access	Select **Modules** > **Administrator** > **Configuration** tab > **Modules** > **Analysis** > **Filter**.

User interface elements are described below:

UI Elements (A-Z)	Description
Item	The name of the filter item in the Analysis module.
Visibility	Hide or display the filter item in Release Control.

Filter Tabs Pane

This pane defines default properties for some of the filter tabs in the Analysis module.

To access	Select **Modules** > **Administrator** > **Configuration** tab > **Modules** > **Analysis** > **Filter Tabs**.

User interface elements are described below:

UI Elements (A-Z)	Description
Tab	The name of the filter tab in the Analysis module.
Visibility	Hide or display the filter tab in Release Control.

General Info Pane

This pane defines default properties for some of the general information fields in the Analysis module.

To access	Select **Modules** > **Administrator** > **Configuration** tab > **Modules** > **Analysis** > **General Info**.

User interface elements are described below:

UI Elements (A-Z)	Description
Field	The name of the field in the Analysis module.
Visibility	Hide or display the field in Release Control.

Notifications Pane

This pane enables you to configure notification properties.

To access	Select **Modules** > **Administrator** > **Configuration** tab > **Modules** > **Analysis** > **Notifications.**
See also	• Configuring Notifications Overview • Notification Rule Configuration

User interface elements are described below:

UI Elements (A-Z)	Description
Email notification enabled	Enables you to enable/disable the notification feature. When you disable this feature, no notifications are sent by Release Control.

UI Elements (A-Z)	Description
Notification aging factor	The time interval (measured in seconds) that indicates how long a rejected email (for example, an email with an unknown or invalid email address) is held in the queue.
Notification job frequency	The time interval (measured in seconds) between each successive email notification that is sent.
Sender email address	The email address of the default notification sender.

<Notification Template Panes>

The Notifications panes enable you to configure the format of the emails that Release Control sends in the **ftl** files.

To access	Select **Modules** > **Administrator** > **Configuration** tab > **Modules** > **Analysis** > **Notifications** > **<Notification template panes>**. **Note:** For details about editing the files in these panes, see Configure Files in the Configuration Tab.
Important Information	• 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. (To access the API Reference, select **Start** > **Programs** > **Release Control 9.60** > **Documentation** and open the **pdfs** directory). • The Release Control fields that can be used in the FTL files are those that are defined in the Fields pane of the Administrator module. For details, see Fields Pane.
See also	• Configuring Notifications Overview • Notification Rule Configuration

User interface elements are described below:

UI Elements (A-Z)	Description
Action item HTML template	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.
Action item mail body HTML template	Includes the action item (in HTML format) that a user sends by clicking the **Forward by Email(FYI)** button in the Action Items pane.

UI Elements (A-Z)	Description
Action Item mail body text template	Includes the action item (in text format) that a user sends by clicking the **Forward by Email(FYI)** button in the Action Items pane.
Action Item mail subject template	Defines the subject line of an email. By default, Release Control displays **<request-id> – <request summary>** (for example, **C-10020 – Upgrade database server**) as the subject line of the notification.
Action Item text template	Defines the content of the email that a user sends by clicking the **Forward by Email(FYI)** button in the Action Items pane.
CAB invitation HTML template	Includes a list of the participants (in HTML format) of the CAB meeting by clicking the **Send Email > Send CAB invitation** button in the Change Request pane.
CAB invitation text template	Includes a list of the participants (in text format) of the CAB meeting by clicking the **Send Email > Send CAB invitation** button in the Change Request pane.
CAB minutes HTML template	Includes the minutes of the CAB meeting (in HTML format) by clicking the **Send Email > Send CAB minutes** button in the Change Request pane.
CAB minutes text template	Includes the minutes of the CAB meeting (in text format) by clicking the **Send Email > Send CAB minutes** button in the Change Request pane.
Change request mail body HTML template	Defines the content of the email (in HTML format) sent to a user who subscribed to receive notification of updates to a change request.
Change request mail body text template	Defines the content of the email sent to a user who subscribed to receive notification of updates to a change request.
Change request mail subject template	Defines the subject line of the email sent to a user who subscribed to receive notification of updates to a change request.
Free text only HTML template	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.
Free text only text template	Defines the content of the email that a user sends by clicking the **Send Email** button in the Collaboration tab's Discussion view.
Mail body HTML template	Defines the content of a notification sent in HTML format.
Mail body text template	Defines the content of a notification sent in text format.
Mail Subject template	Defines the subject line of the email sent to a user after a change request enters the system.

UI Elements (A-Z)	Description
PIR invitation HTML template	Includes a list of the participants (in HTML format) of the PIR meeting by clicking the **Send Email > Send PIR invitation** button in the Change Request pane.
PIR invitation text template	Includes a list of the participants (in text format) of the PIR meeting by clicking the **Send Email > Send PIR invitation** button in the Change Request pane.
PIR minutes HTML template	Includes the minutes of the PIR meeting (in HTML format) by clicking the **Send Email > Send PIR minutes** button in the Change Request pane.
PIR minutes text template	Includes the minutes of the PIR meeting (in text format) by clicking the **Send Email > Send PIR minutes** button in the Change Request pane.
User mail body HTML template	Defines the content of the email (in HTML format) that a user sends by clicking the **Send Email** button in the Change Requests pane.
User mail body text template	Defines the content of the email that a user sends by clicking the **Send Email** button in the Change Requests pane.

Release Control Objects

By default, the above files make use of the following 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 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. (To access the API Reference, select **Start** > **Programs** > **Release Control 9.60** > **Documentation** and open the **pdfs** directory).
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. (To access the API Reference, select **Start** > **Programs** > **Release Control 9.60** > **Documentation** and open the **pdfs** directory).

Object	Description
affectedCIs	Returns a list of the CIs that are impacted by a change request.
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. (To access the API Reference, select **Start** > **Programs** > **Release Control 9.60** > **Documentation** and open the **pdfs** directory).
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. (To access the API Reference, select **Start** > **Programs** > **Release Control 9.60** > **Documentation** and open the **pdfs** directory).

Reports Panes

These panes describe the report templates used for the reports generated in the Analysis module's List and Calendar views.

To access	Select **Modules** > **Administrator** > **Configuration** tab > **Modules** > **Analysis** > **Reports**.
Important Information	You can define value expressions using report parameters, variables, and fields, and you can use Java expressions to customize your report. For details, see Value Expressions.
See also	• Working with the Configuration Tab • Report Details Dialog Box

User interface elements are described below:

UI Elements (A-Z)	Description
Reports fuse	The maximum number of change requests that can be included when generating a report. For details, see Report Details Dialog Box.

The Reports panes are described below:

UI Elements (A-Z)	Description
One page report template	Template for generating a one page PDF or HTML report.
Changes report - PDF and HTML template	Template for generating first level changes in a PDF or HTML list report.
Tasks sub report template	Template for generating second level changes in a PDF or HTML list report.
Changes report - Excel template	Template for generating a list report in Excel format.

Dashboard Pane

This pane contains the **dashboard.settings** file, which maps the two types of roles in 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.

To access	Select **Modules** > **Administrator** > **Configuration** tab > **Modules** > **Dashboard**.
Important Information	The definitions in this file should not be modified.
See also	Working with the Configuration Tab

Director Pane

This pane enables you to determine whether the Director module is displayed.

To access	Select **Modules** > **Administrator** > **Configuration** tab > **Modules** > **Director**.
See also	• Working with the Configuration Tab • Director Module

User interface elements are described below:

UI Elements (A-Z)	Description
Director module shown	Enables you to hide/display the Director module.

Alerts Pane

This pane enables you to configure the settings for alerts in the Alerts pane of the Director module.

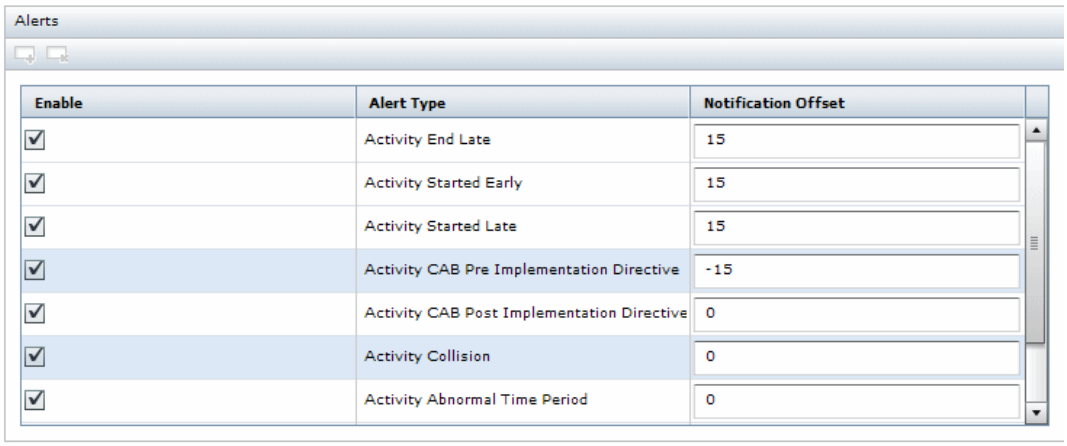
To access	Select **Modules** > **Administrator** > **Configuration** tab > **Modules** > **Director** > **Alerts**.
Important information	You must restart the Release Control service for these configuration changes to take effect.
See also	Alerts Pane

User interface elements are described below:

UI Elements (A-Z)	Description
Alert calculation period	The first run of the alert engine is very heavy on the system, calculating alerts, by default, over a 2 day time period retroactively. This option enables you to modify the time interval during which the alert engine calculates alerts. **Default:** 2 days (2880 minutes), measured in minutes.
Alert engine Cron expression	Release Control refreshes alerts in the Director module using an alert engine. This option enables you to specify the interval that indicates how often the alert engine runs. **Default:** 1 (measured in minutes), as displayed by the cron expression, **0 0/1 * * * ?**. **Examples:** • To run the engine every 5 minutes, change the value to **0 0/5 * * * ?** • To run the engine every 30 minutes, change the value to **0 0/30 * * * ?** For more information about cron expressions, see http://quartz.sourceforge.net/javadoc/org/quartz/CronTrigger.html.
Alert engine enabled	Enable or disable the alert engine. **Default:** Enabled
Change-modify min/max time window	Emergency Activity alerts and Activity Modification alerts are generated for all activities whose schedules intersect with the **Change-modify min/max time window**. More specifically:

UI Elements (A-Z)	Description
	• 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 min/max window** is the window of time surrounding or close to the current time. • The **Change-modify min time window** defines the time behind the current time. It is the number of minutes before (negative value) or after (positive value) the current time, representing the beginning of the time window. **Default:** 12 hours (720 min). Measured in minutes. • The **Change-modify max time window** defines the time ahead of the current time. The number of minutes before (negative value) or after (positive value) the current time, representing the end of the time window. **Default:** 24 hours (1440 min). Measured in minutes. For an example that illustrates minimum and maximum values for the time window, and where alerts are or are not generated, see Examples Showing Instances Where Alerts Are or Are Not Generated.
Change statuses for collision alerts	Calculates collision-related alerts only on activities with the selected statuses.

Alert Type Pane



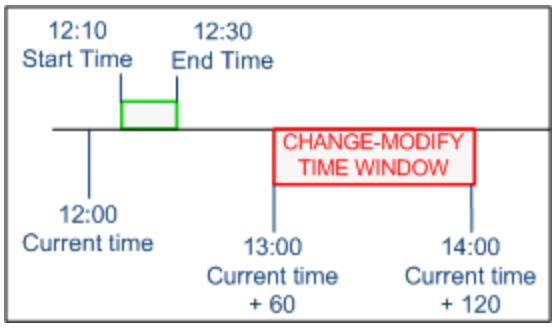
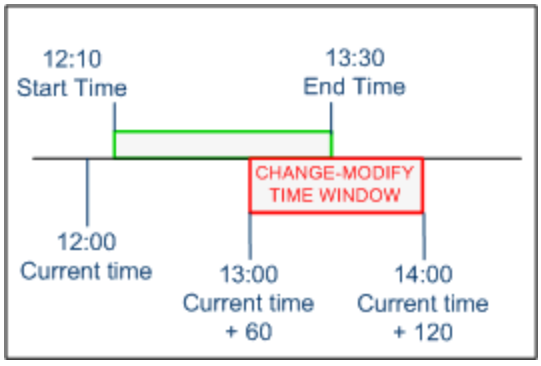
This pane enables you to enable or disable alerts, and define the number of minutes before or after events that you want alerts to be generated.

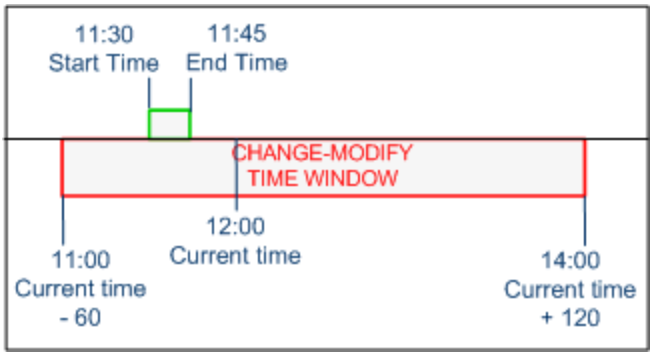
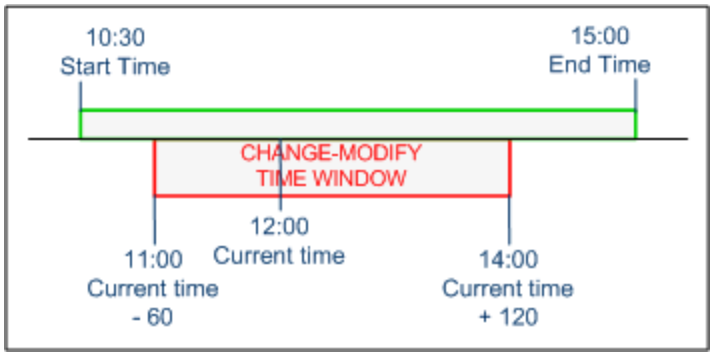
User interface elements are described below:

UI Elements (A-Z)	Description
Alert Type	The type of alert.
Enable	Enables or disables the alert.
Notification Offset	Specify the number of minutes before or after the event that the alert is to be generated.

Examples Showing Instances Where Alerts Are or Are Not Generated

The following examples illustrate minimum and maximum values for the time window, and where alerts are or are not generated.

Scenario 1- No alert generated • Emergency Activity inserted 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 inserted: 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	

Security Configuration

This chapter includes:

Concepts

- Lightweight Single Sign-On Authentication Overview
- Release Control User Authentication Overview
- Using Identity Management
- Release Control's Identity Manager Mode Architecture
- Using LDAP Authentication
- Release Control's LDAP Authentication Architecture

Tasks

- Use Identity Management Mode
- Work in Database Authentication Mode
- Configure the LDAP Connection Properties
- Set the Connection Between Release Control and the LDAP Server

Reference

- LW-SSO Limitations
- LW-SSO Security Warnings
- LW-SSO Important Information
- Security Configuration User Interface

Concepts

Lightweight Single Sign-On Authentication Overview

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 Release Control is Lightweight Single Sign-On (LW-SSO). LW-SSO is embedded in Release Control and does not require an external machine for authentication.

For details on how to enable LW-SSO in Release Control, see Lightweight SSO (LWSSO) Pane.

Release Control User Authentication Overview

You can configure Release Control to work in one of the following user authentication modes:

- **Identity Manager.** Release Control can work with identity management systems that manage authentication, for example, Lightweight Directory Access Protocol (LDAP). For details on how to use identity management, see Using Identity Management.
- **LDAP.** 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. For details, see Using LDAP Authentication.
- **Database.** Release Control does not work with an identity management system or LDAP, and Release Control authenticates all users. For details, see Work in Database Authentication Mode.

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.

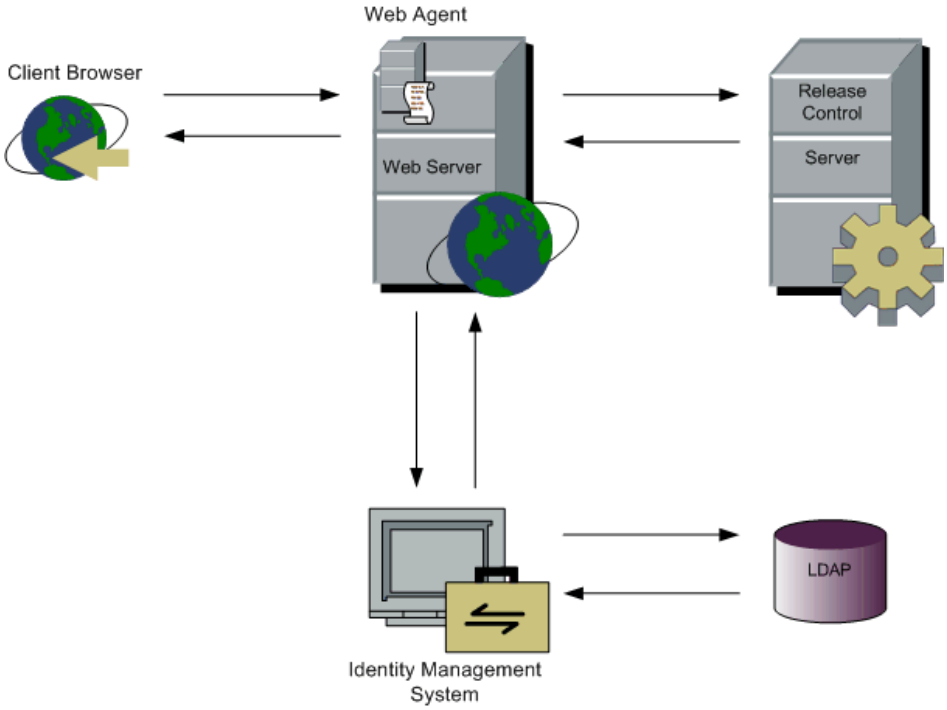
Release Control supports a variety of identity management systems. The configuration samples in this document use the CA SiteMinder 6.0 identity management system.

For details on identity manager mode architecture, see Release Control's Identity Manager Mode Architecture.

For details on how to use identity management mode, see Use Identity Management Mode.

Release Control Identity Manager Mode Architecture

The following diagram illustrates Release Control Identity Manager mode architecture.



To work with identity management in conjunction with Release Control, you must deploy Release Control to work with a Web server (Microsoft Internet Information Services (IIS) or Apache HTTP Server). For details, see *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 Release Control.

Using LDAP Authentication

You can configure Release Control to use LDAP for user authentication. Release Control automatically takes the user login information from the LDAP server. Since Release Control and LDAP are synchronized, any user information that changes in LDAP is reflected in Release Control the next time a user logs in. When you configure LDAP authentication, you map the LDAP user groups to Release Control user roles.

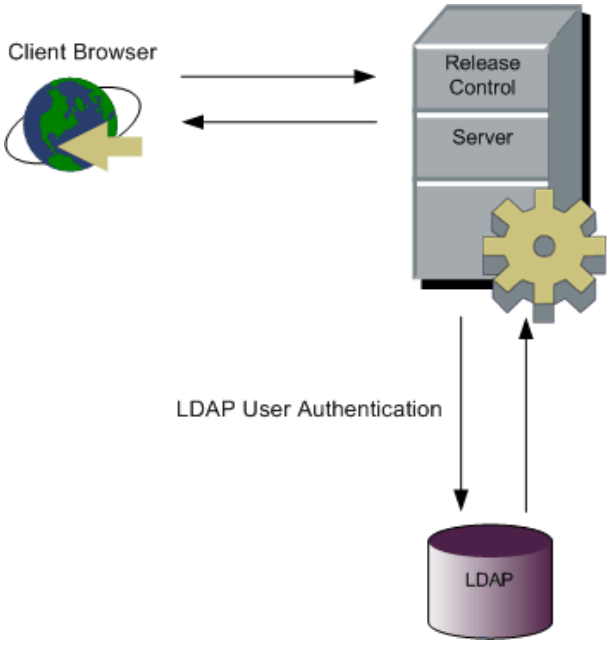
For details on LDAP authentication architecture, see Release Control's LDAP Authentication Architecture.

For details on how to use LDAP authentication, see Configure the LDAP Connection Properties.

> **Note:** If the LDAP server allows anonymous binding, Release Control allows you to log in using an empty password.

Release Control LDAP Authentication Architecture

The following diagram illustrates Release Control LDAP authentication mode architecture.



Tasks

Use Identity Management Mode

To work with Release Control in conjunction with an identity management system such as CA SiteMinder, you must configure both 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.

> **Caution:** Before you change your security settings, it is recommended that you back up your current Release Control configuration set using the export configuration set utility. For details, see Export Configuration Set.

The Release Control identity management mode configuration process includes the following steps:

Step 1: Configure Release Control to work with Identity Manager

Step 2: Configure an Identity Manager to work with Release Control

Step 3: Add your organization's administrator to Release Control

Step 4: Work in Identity Management mode

Step 5: Use the Identity Manager mode command line option when running a utility

Step 6: (Optional) Redeploy the ccm_package.zip file in Universal CMDB (only when upgrading Release Control and working with the Change Configuration adapter)

Step 7: Configure Release Control to work with a federation adapter in Identity Manager mode

Step 1: Configure Release Control to work with Identity Manager

To work with Release Control in conjunction with CA SiteMinder, the Release Control administrator must do the following:

1. Set the authentication mode. Select **Module** > **Administrator** > **Configuration** tab > **Security** > **Authentication**. In the Authentication pane, select **Identity Manager** from the **Authentication mode** list. Specify the user login information required to connect to the LDAP server.
2. Select **Module** > **Administrator** > **Configuration** tab > **Security** > **Authentication > Identity Manager Mode**. In the Identity Manager Mode pane, define the following user login information:
   - **First name header**
   - **Last name header**
   - **Email header**
   - **Request encoding**

   For details, see Identity Manager Mode Pane.
3. If your organization has a logout page, ask the CA SiteMinder administrator to provide you with an Release Control logout URL. In **Module** > **Administrator** > **Configuration** tab > **Security**, enter the value provided in the **Logout URL** field. For details, see Security Pane.
4. After you save and apply your configuration settings, restart the Release Control service.

Step 2: Configure an Identity Manager to work with Release Control

To work with CA SiteMinder in conjunction with Release Control, the CA SiteMinder administrator must do the following:

1. Install and configuring the Web agent.
   Install the Web agent on the Release Control server machine and configure the agent to protect the Release Control resource. Only users who are authorized to work with Release Control should be allowed access to the 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 SiteMinder.

2. Configure CA SiteMinder to add the following headers to the HTTP header request that is returned following a successful authentication:
   - Login name header
   - First name header
   - Last name header
   - Email header

3. In order to work with the Universal CMDB change federation adapter and with command line utilities, ensure that logon to CA SiteMinder supports basic authentication.
   In the CA SiteMinder **Authentication Scheme** dialog box, select the **Support non-browser clients** check box.

4. Configuring the logout page. If your organization does not have a logout page, CA SiteMinder should be configured to use the Release Control logout page, defined in the **Logout URL**box in **Module** > **Administrator** > **Configuration** > **Security** pane.

Step 3: Add your organization's administrator to Release Control

By default, Release Control includes one user, **admin**, with administrative privileges. This user, however, does not exist in the LDAP information directory. Your organization's real Release Control administrator, whose properties are stored in the LDAP directory, does not initially exist in Release Control and must be added using the following bootstrap procedure. To add your organization's administrator to Release Control, do the following:

1. By default, the role assigned to a user in Identity Management mode in the **Default Roles** box is **System Administrator**. This way, the first login is assigned the user with System Administrator privileges.
   Log in to Release Control (http://<server name>/ccm) using the user whose credentials you want to become the administrator in Release Control.

2. Ensure that users who log on to Release Control in the future will be assigned regular user privileges.
   To do this, go to **Module** > **Administrator** > **Configuration** tab > **Security** > **Authentication** > **Identity Manager** and change the role assigned in the **Default Roles** box to **User**.

3. (Optional) Change the **admin** user's password.
4. After you save and apply your configuration settings, restart the Release Control service.

> **Notes:**
>
> - Once you have performed the above procedure, you can close the Tomcat server port (by default, 8080) by a firewall for inbound traffic (ensure that the Tomcat server is still open for traffic from localhost).
> - It is recommended that you do not remove the **admin** user from Release Control.

Step 4: Work in Identity Management mode

When you work in Identity Manager 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 address user properties in the HTTP header request. Release Control checks whether this user already exists in Release Control. If so, the user's first name, last name, and address are updated, if necessary. If not, the user is added to Release Control as a regular user (**User** role), with the properties returned from the identity management system.

> **Notes:**
>
> - The created user is unable to log in to Release Control using the Database authentication mode until the Release Control administrator provides the user with an Release Control password. For details, see Work in Database Authentication Mode.
> - 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 Release Control, you can add the user to Release Control using the user importer utility. For details on this utility, see Import Users.
> When working in identity management mode, the following user and Release Control administrator restrictions exist:
> - Users are unable to modify their user names, passwords, first names, last names, or email addresses.
> - The Release Control administrator is unable to add users to Release Control using the Administrator module.
> - The Release Control administrator is unable to update the user name, password, first name, last name, or email address of any user within Release Control.

Step 5: Use the Identity Manager mode command line option when running a utility

When running any of the utilities, you must use the **--im-mode** command line option in the command line to specify that Release Control is working in Identity Manager mode. For details, see Release

Control Utilities.

Step 6: (Optional) Redeploy the ccm_package.zip file in Universal CMDB (only when upgrading Release Control and working with the Change Configuration adapter)

If you have upgraded your Release Control version, you must redeploy the **ccm_package.zip** file in Universal CMDB. For details, see *Configuring Universal CMDB* in the *Release Control Deployment Guide*.

Step 7: Configure Release Control to work with a federation adapter in Identity Manager mode

When configuring a federation adapter in Universal CMDB, you must enter `{IMMODE}` before your user name when entering your credentials.

For example: `{IMMODE}<username>`

For details about configuring federation adapters, see the *Universal CMDB Developer Reference Guide*.

Work in Database Authentication Mode

As an alternative to using the Release Control's identity management or LDAP user authentication solutions, you can use Release Control's Database authentication mode.

To work in Database authentication mode:

1. If you previously closed the Tomcat server port (by default, 8080), reopen it.
2. Set the Release Control authentication mode to **Database** in the **Authentication mode** list in **Module** > **Administrator** > **Configuration** tab > **Security** > **Authentication** pane and restart the Release Control service.
3. Log in to 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 are able to log in to Release Control using Release Control's regular authentication mode. For details, see User Preferences.

Configure the LDAP Connection Properties

This task describes how to set the LDAP parameters to be able to work with LDAP authentication in Release Control.

1. Set up the LDAP server.
2. Set the authentication mode:
   a. Select **Module** > **Administrator** > **Configuration** tab > **Security** > **Authentication**.
   b. In the Authentication pane, select **LDAP** from the **Authentication mode** list.
   c. Specify the user login information required to connect to the LDAP server.
3. Select **Module** > **Administrator** > **Configuration** tab > **Security** > **Authentication** > **LDAP Mode**. In the LDAP Mode pane, define the following user login information:
   - First name header
   - Last name header
   - Email header

   For details, see LDAP Mode Pane.
4. Map the LDAP user groups to roles in Release Control in the LDAP Groups to Release Control Roles Mapping pane. Select **Module** > **Administrator** > **Configuration** tab > **Security** > **Authentication** > **LDAP Mode.**
   Specify the **LDAP Group Name** of the LDAP user group and then select one or more corresponding **Release Control Roles**.
5. Indicate whether to synchronize the group mapping if a definition changes. Select **Module** > **Administrator** > **Configuration** tab > **Security** > **Authentication** > **LDAP Mode**. In the **Roles synchronized** check box, do one of the following:
   - Select the **Roles synchronized** check box to specify that if a user changes to a different LDAP group, they are automatically mapped to new corresponding Release Control roles.
   - Clear the **Roles synchronized** check box 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 Release Control client.
6. Specify which roles to map to a user if they do not belong to any of the groups defined in the **groups** section. Select **Module** > **Administrator** > **Configuration** tab > **Security** > **Authentication** > **LDAP Mode** and select the required default role from the **Default Roles**list. If you select a default role from the **Default Roles** list, the LDAP authentication allows users that do not belong to any of the LDAP groups to access Release Control and is assigned the default role.

> **Note:** At least one of the default roles or the mapped roles should have the editConfiguration permission assigned to it. By default, the role System Administrator is assigned the editConfiguration permission.

Set the Connection Between Release Control and the LDAP Server

The **ldap.properties** file enables you to set the connection between Release Control and the LDAP server.

The Release Control installation provides two sample **ldap.properties** files. Both of these files contain detailed instructions for setting the connection between Release Control and the LDAP server.

This task describes how to set the connection between Release Control and the LDAP server using the **ldap.properties** file.

1. Select **Module** > **Administrator** > **Configuration** tab > **Security** > **Authentication** > **LDAP Mode** > **LDAP Server Properties**. You can add LDAP information in the right pane.
2. Browse to the **<Release Control installation directory>\examples\ldap-examples** directory and do one of the following:
   - If you are working with LDAP Active Directory, then copy the **ldap.properties.AD** file located in **<Release Control installation directory>\examples\ldap-examples** to your local directory.
   - If you are working with LDAP SUN One, then copy the **ldap.properties.SO** file located in **<Release Control installation directory>\examples\ldap-examples** to your local directory.

     > **Note:** If you are working with another LDAP server, you can use either one of the examples as a template.
3. Set the necessary LDAP information and save the file.

   > **Note:** If the LDAP server is configured to work over SSL, make sure to set `enableSSL = true` in the ldap.properties file and that you have a security certificate installed in the Release Control Java Virtual Machine (JVM).

Reference

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.
- **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.
  - 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.
  - 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 Internet Explorer, 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 *.mydomain.com) to the "Intranet"/"Trusted" zone on your computer (on Microsoft Internet Explorer, select **Tools** > **Internet Options** > **Security** > **Local Intrane**t > **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.
- **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 than three 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, it is recommended, if possible, to 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:

Confidential InitString parameter in LW-SSO:

LW-SSO uses Symmetric Encryption to validate and create an 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.

> **Notes:**
>
> 1. It is not possible to use LW-SSO without setting the initString parameter.
> 2. The initString parameter is confidential information and should be treated as such in terms of publishing, transporting, and persistency.
> 3. The initString parameter should be shared only between applications integrating with each other using LW-SSO.
> 4. The minimum length of the initString parameter is 12 characters.

LW-SSO Important Information

This section contains important information regarding LW-SSO.

- **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 **Protected Domains** settings (located in **Module** > **Administrator** > **Configuration** tab > **Security** > **Lightweight SSO (LWSSO)** pane), if they are required to integrate with applications in different DNS domains.

>

Security Configuration User Interface

This section includes:

- Security Pane
- Authentication Pane
- Database Mode Pane
- Identity Manager Mode Pane
- Identity Manager Mode Pane
- LDAP Server Properties Pane
- Lightweight SSO (LWSSO) Pane

Security Pane

This pane enables you to define the URL to which the application is redirected after logging out, as well as configure your computer to log in without having to enter a user name and password.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Security**.
Relevant tasks	Use Identity Management Mode
See also	Using Identity Management

User interface elements are described below:

UI Elements (A-Z)	Description
Logout URL	The URL to which the application is redirected after logging out. **Default:** /ccm/imresources/ccmLogout.html
Remember me enabled	When you log in to Release Control from the opening page, you can select **Remember me** on this computer so that the next time you log in from the same computer, you do not need to enter a user name and password.

Authentication Pane

This pane enables you to define the authentication mode in which you want Release Control to work.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Security** > **Authentication**.
Relevant tasks	• Use Identity Management Mode • Work in Database Authentication Mode • Configure the LDAP Connection Properties
See also	Release Control User Authentication Overview

User interface elements are described below:

UI Elements (A-Z)	Description
Authentication mode	Enables you to configure Release Control to work in one of the following user authentication modes: • Database • LDAP • Identity Manager

Database Mode Pane

This pane enables you to configure the Release Control security requirements if you are working in database authentication mode.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Security** > **Authentication** > **Database Mode**.
Relevant tasks	Work in Database Authentication Mode
See also	Release Control User Authentication Overview

User interface elements are described below:

UI Elements (A-Z)	Description
Password minimum length	Determines the minimum number of characters that a password can contain. By default, a password must contain at least one character.
Password maximum length	Determines the maximum number of characters the password can contain. This number must be greater than 25. **Default:** 50
Password validation pattern	Using regular expressions, specify the characters that each user password can contain. For example, use the following expression to indicate that a password can be any upper-case or lower-case letter,

UI Elements (A-Z)	Description
	as well as any digit: `^[A-Z,a-z,0-9]$`.
Password validation pattern error message	The type of error message to be displayed if the password contains a character that is not allowed.
Username maximum length	Determines the maximum number of characters that a user name can contain. This number must be greater than 25. **Default:** 50
Username minimum length	Determines the minimum number of characters that a user name can contain. **Default:** 1
Username validation pattern	Using regular expressions, specify the characters that each user name can contain. For example, use the following expression to indicate that a user name can be any upper-case or lower-case letter, as well as any digit: `^[A-Z,a-z,0-9]$`.
Username validation pattern error message	The type of error message to be displayed if the user name contains a character that is not allowed.

Identity Manager Mode Pane

When configuring an identity manager system to work with Release Control, you must configure the identity manager to add the headers in this pane to the HTTP header request that is returned following a successful authentication.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Security** > **Authentication** > **Identity Manager Mode**.
Relevant tasks	Use Identity Management Mode
See also	Using Identity Management

User interface elements are described below:

UI Elements (A-Z)	Description
Email header	Contains the user's email address.
First name header	Contains the user's first name.
Last name header	Contains the user's last name.
Login name header	Contains the user name with which the user logs on to Release Control.

UI Elements (A-Z)	Description
Request encoding	The encoding value with which identity management works. **Default:** ISO-88591

LDAP Mode Pane

This pane enables you to configure Release Control to work in LDAP mode.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Security** > **Authentication** > **LDAP Mode**.
Relevant tasks	Configure the LDAP Connection Properties
See also	Using LDAP Authentication

User interface elements are described below:

UI Elements (A-Z)	Description
Default roles	A default Release Control user role that is assigned to a user who is not mapped to any of the LDAP user groups. • If you select a default role from the **Default Roles** list, the LDAP authentication allows users who do not belong to any of the LDAP groups to access Release Control and is assigned the default role. • If you do not select a default role, the LDAP authentication does not allow a user who does not belong to any of the LDAP groups to log on to Release Control.
Email header	The name of the LDAP attribute that stores the user's email address.
First name header	The name of the LDAP attribute that stores the user's first name.
Last name header	The name of the LDAP attribute that stores the user's last name.
Role synchronized	Indicates whether to synchronize the group mapping if a definition changes. • Select this check box to specify that if a user changes to a different LDAP group, they are automatically mapped to new corresponding Release Control roles. • Clear this check box 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 Release Control client.

UI Elements (A-Z)	Description
	Default: Not selected.

LDAP Groups to Release Control Roles Mapping Pane

This pane enables you to map the LDAP user groups to Release Control user roles.

User interface elements are described below:

UI Elements (A-Z)	Description
	Add configuration to configuration set. Enables you to map another LDAP user group to an Release Control user role.
	Remove configuration from configuration set. Enables you to delete the selected row.
LDAP Group Name	The name of the LDAP user group.
Release Control Roles	Select the Release Control user role to map to the corresponding LDAP user group.

LDAP Server Properties Pane

This pane contains the **ldap.properties** file, which enables you to set the connection between Release Control and the LDAP server.

The Release Control installation provides two sample **ldap.properties** files. Both of these files contain detailed instructions for setting the connection between Release Control and the LDAP server.

- If you are working with LDAP Active Directory, then copy the **ldap.properties.AD** file located in **<Release Control installation directory>\examples\ldap-examples** to your local directory.
- If you are working with LDAP SUN One, then copy the **ldap.properties.SO** file located in **<Release Control installation directory>\examples\ldap-examples** to your local directory.

For details on how to modify these files, see Configure Files in the Configuration Tab.

For a description of the connection properties included in the **ldap.properties file**, see Connection Properties in the ldap.properties File.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Security** > **Authentication** > **LDAP Mode** > **LDAP Server Properties**.
Relevant tasks	Set the Connection Between Release Control and the LDAP Server
See also	• Using LDAP Authentication

	• Release Control's LDAP Authentication Architecture • Working with the Configuration Tab

Connection Properties in the ldap.properties File

The following describes the connection properties included in the **ldap.properties** file:

Connection property	Description
Administrator's password	Administrator's password used for creating the initial LDAP connection. > **Note:** This parameter is not required if the **useAdministrator** option is set to `false`.
Administrator's username	Administrator's user name used for creating the initial LDAP connection. > **Note:** This parameter is not required if the **useAdministrator** option is set to `false`.
BATCHSIZE	Indicates the minimum chunk size that must be received before the results are returned. > **Note:** This parameter influences only the LDAP response time.
dynamicGroupsClass	Object class used for storing the dynamic group's information.
dynamicGroups DescriptionAttribute	Attribute used to store the dynamic group's description.
dynamicGroups DisplayNameAttribute	Attribute used to store the dynamic group's display name.
dynamicGroups MemberAttribute	Attribute used to store the search URL that defines the members of the dynamic group.
dynamicGroups MemberAttribute	Attribute used to store the dynamic group name.
enableDynamic Groups	Release Control is instructed to search for users in dynamic groups as well as in static groups.
enableNestedGroups	Release Control is instructed to search recursively for all users in subgroups. > **Note:** Instances are returned by the group's search filter.

Connection property	Description
enableSSL	If this parameter is selected, SSL is used to connect to the LDAP server.
groupsBase	The distinguished name (DN) used to search for groups in the LDAP directory.
groupsDescription Attribute	Used to store the group's description.
groupsDisplayNameAttribute	Used to store the group's display name.
groupsFilter	Indicates what instances should be returned from the LDAP group search.
groupsMembers Attribute	Used to store the group's member information.
groupsNameAttribute	Used to store the group name.
groupsObjectClass	Object class used for storing the static group's information.
groupsScope	The scope for the group search is as follows: • **SCOPE_SUB**. Searches the subtree under the group's base. • **SCOPE_ONE**. Searches only the first level of the subtree under the group's base. • **SCOPE_BASE.** Searches only the root of the subtree. **Note:** The group's base is defined in the **groupsBase** attribute.
ldapHost	Host name of the machine running the LDAP server.
maximalAllowed GroupsHierarchyDepth	Defines the maximum allowed depth for the groups hierarchy. A negative value means that an unlimited depth is allowed. **Note:** This parameter is relevant only if the **enableNestedGroups** parameter is set to `true`.
MAXBACKLOG	Indicates the size of queue waiting for batch results if **BATCHSIZE** is not **0**. **Note:** This parameter influences only the LDAP response time.
ldapPort	Port number of the LDAP server. If **enableSSL** is set to `true`, then this port is used for the SSL connection.
REFERRALS	Some objects in LDAP may just be referrals to another

Connection property	Description
	LDAP, containing the required information. If selected, the search follows references automatically, until it reaches the number indicated by the **REFERRALS_HOP_LIMIT** parameter. Otherwise, if the number of HOPs is exceeded, the search may not return all required results.
REFERRALS_HOP_LIMIT	Indicates the number of times the referrals are followed, until an exception occurs terminating the search.
rootGroupsBase	The distinguished name (DN) used to search for root groups in the LDAP directory.
rootGroupsFilter	Indicates what instances should be returned from the LDAP search.
rootGroupsSearch Scope	The scope for the rootgroup search is as follows: • **SCOPE_SUB**. Searches the subtree under the group's base. • **SCOPE_ONE**. Searches only the first level of the subtree under the group's base. • **SCOPE_BASE.** Searches only the root of the subtree. **Note:** The group's base is defined in the **rootGroupsBase** attribute.
SIZELIMIT	Enables you to limit the total number of results returned from LDAP by one search.
TIMELIMIT	Enables you to limit the amount of time spent by LDAP on one search.
usersBase	The distinguished name (DN) used to search for users in the LDAP directory.
usersDisplayName Attribute	The attribute used to store the user's display name.
usersFilter	Indicates what instances should be returned from the LDAP user search.
useAdministrator	If set to `true`, the LDAP connection is created with the Administrator's user name and password provided in the **Administrator username** and **password** parameters. Otherwise the LDAP connection is created without a user name or password. **Note:** The v2 guest user is not supported by the library.

Connection property	Description
usersObjectClass	Object class used for storing the user information.
usersScope	The scope for the users search is as follows: • **SCOPE_SUB**. Searches the subtree under the group's base. • **SCOPE_ONE**. Searches only the first level of the subtree under the group's base. • **SCOPE_BASE.** Searches only the root of the subtree. **Note:** The user search base is defined in the **usersBase** attribute.
usersUniqueIDAttribute	Stores the actual login name of the user. **Note:** The DN search and authentication functions suppose that this attribute is unique.

Lightweight SSO (LWSSO) Pane

In this pane, you can enable LW-SSO in Release Control.

To access	Select **Module** > **Administrator** > **Configuration** tab > **Security** > **Lightweight SSO (LWSSO)**.
See also	Lightweight Single Sign-On Authentication Overview

User interface elements are described below:

UI Elements (A-Z)	Description
Domain	(Optional) Should contain the Release Control server domain. If left undefined, Release Control automatically assigns a value to this element.
Initialization string	Must contain a shared string that is used by all trusted applications integrating with LW-SSO.
Protected domains	(Optional) Should contain at least one Release Control server domain. In cases where trusted applications are located in other domains, all those domains should be defined here.

Server Configuration

This chapter includes:

Concepts

- Multi-Tenancy Configuration Overview
- Cluster Deployment Overview

Tasks

- Configure the Release Control Server for Multi-Tenancy (SaaS Only)
- Set Up a Cluster Deployment of Release Control

Reference

- Server Configuration User Interface

Concepts

Multi-Tenancy Configuration Overview

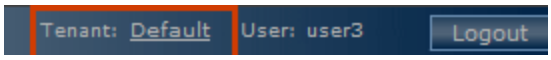
> **Note:** This configuration option is specifically relevant to SaaS providers.

You can configure your Release Control server to serve multiple client organizations (tenants).

In such an environment, each Release Control tenant is mapped to a Universal CMDB Customer ID. Change request tickets from the service desks are allocated to tenants in Release Control based on the value of a specified tenant allocation field.

When logging in to Release Control, a user who is associated with more than one tenant, is prompted to select the tenant name to which the required change request tickets are allocated.

If you want to work with a different tenant once inside the system, it is not necessary to log out. Select the required tenant from the tenant selection option that appears to the left of the **Logout** button in the top right-hand corner of the screen (see the illustration below). Release Control logs you in to the system again without having to enter your credentials.



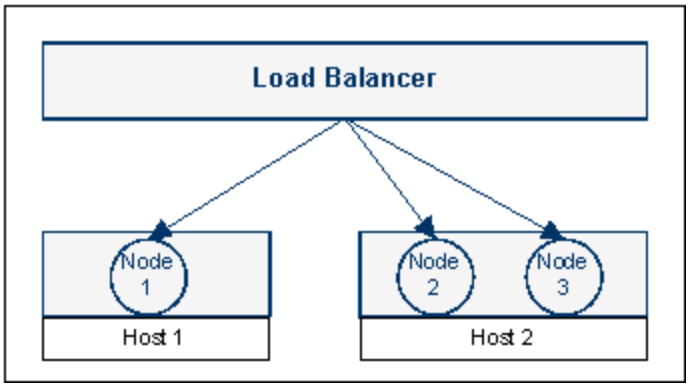
> **Notes:**
>
> 1. The tenant selection option does not appear if the user is associated with only one tenant.
> 2. You can modify the display value of the term **tenant** in Release Control in the **customizable-labels.properties** file in **Modules** > **Administrator** > **Configuration** tab > **Labels and Terms**. For details, see Label and Term Configuration.

In a multi-tenant environment, the basic configuration of Release Control is the same for all of the tenants.

For details on configuring your server for multi-tenancy, see Configure the Release Control Server for Multi-Tenancy (SaaS Only).

Cluster Deployment Overview

The Release Control server can be deployed on multiple nodes. You can deploy a cluster of nodes over multiple instances of the same physical machine or over separate machines.



> **Note:** For details about how to deploy a cluster, see Set Up a Cluster Deployment of Release Control.

Load Balancer

Client requests are distributed across the nodes using a **load balancer**. In a cluster deployment, the load balancer is the point of entry into the system and you enter Release Control through the URL of the load balancer.

Release Control includes a reference implementation of a software load balancer. This load balancer is made up of a Web server component (Apache or IIS) and a **mod_jk** component. However, it is

recommended to use a hardware load balancer. Release Control supports any load balancer that includes a **sticky session** feature.

Clustering Advantages - User Capacity and Server Availability

Whether you deploy the cluster on the same machine or over separate machines, the **concurrent user capacity** of Release Control is increased. However, if you also want to increase **server availability**, you need to deploy the cluster over separate machines.

Notes and Limitations

- Certain configuration changes require you to restart the Release Control service. In a cluster deployment, you need to restart all the nodes in the cluster.
- If you made changes to the field settings (**Module** > **Administrator** > **Configuration** tab > **Integrations** > **Fields**) in a cluster deployment, you need to bring down all the nodes in the cluster, except for one. This does not result in any system downtime, because one node is still up during this short procedure.
  The reason you need to bring down the nodes is that this configuration may result in schematic changes in the database. To avoid having to synchronize the reconfiguration of the database model in each of the nodes, this configuration change is handled by a single node.

  To activate changes to the field settings:

  a. Save a draft of your changes.

  b. Bring down all the nodes in the cluster, except for one.

  c. Activate the configuration on that one node.

  d. Start the other nodes up again.
- If you configure a service desk adapter on one of the nodes and the other nodes are installed on separate machines, do the following:
  a. If Release Control is running on any of the nodes, stop the Release Control service.

  b. Copy the **<serviceDeskName>-adapter-log4j.properties** file from the first node's **conf** directory into the other node's **conf** directory.

  c. Copy the **SDI-<serviceDeskName>** directory from the first node's **apps** directory into the other node's **apps** directory.

Tasks

Configure the Release Control Server for Multi-Tenancy (SaaS Only)

> **Note:** The task is specifically relevant to SaaS providers.

This task describes how to configure your Release Control server to serve multiple client organizations (tenants). For background information about this configuration option, see Multi-Tenancy Configuration Overview.

This task includes the following steps:

Step 1: Define a custom field for tenant allocation

Step 2: Add tenants and assign allocation field values

Step 3: Map tenants to UCMDB Customer IDs

Step 4: Associate users with tenants

Step 1: Define a custom field for tenant allocation

1. In your service desk, decide on a field which will be used as the tenant allocation field. Change request tickets from the service desk will be allocated to tenants in Release Control based on the value of this field. In addition, consider which values are used for each tenant.

   > **Note:** If you are integrating with Service Manager, select the Company field to enable you to work with multiple tenants.

2. Map the service desk tenant allocation field, which you selected above, to a corresponding field in Release Control. The Release Control field should be of type **Short Text**.
   - For details about creating fields in Release Control, see Field and Enumeration Setting Configuration.
   - For details about mapping service desk fields to Release Control fields, see Writing Conversion Scripts.

Step 2: Add tenants and assign allocation field values

In the Multi-Tenancy pane (**Module** > **Administrator** > **Configuration** > **Server** > **Multi-Tenancy**),

you add new tenants and you map each tenant to a tenant allocation field value. Based on this value, change request tickets are allocated to the relevant tenant.

For user interface details, see Multi-Tenancy Pane.

Step 3: Map tenants to UCMDB Customer IDs

In the UCMDB Custom ID to Tenant Mapping area of the Available Connections pane (**Module** > **Administrator** > **Configuration** > **Integrations** > **Universal CMDB** > **Available Connections** > **<Universal CMDB server name>**), you associate the tenants with Universal CMDB Customer IDs.

> **Note:** You can associate multiple tenants with multiple Customer IDs of one Universal CMDB configuration, or you can associate different tenants with different Universal CMDB configurations.
> If there are multiple Universal CMDB configurations, each configuration needs to be of the same version.

For user interface details, see <Available Connections Panes>.

Step 4: Associate users with tenants

To associate Release Control users with different tenants, you use the user importer utility. This utility enables you to import a list of defined users and user properties from a CSV file to Release Control.

In the **TENANT** property of the CSV file, specify the tenant name associated with the user. Users can be associated with more than one tenant. The tenant names should be separated by a semicolon. In the following example of a CSV file entry, John Doe is associated with two tenants, **customer1** and **customer2**.

```
USERNAME,PASSWORD,FIRST_NAME,LAST_NAME,EMAIL,BUSINESS_ID,TENANT,ROLE
jdoe,1234,John,Doe,jon.doe@hpe.com,jdoe,customer1;customer2,NOC
```

For details about the user importer utility, see Import Users.

Set Up a Cluster Deployment of Release Control

This task describes how to deploy Release Control on multiple nodes.

This task includes the following steps:

Step 1: Install and configure Release Control on the first node

Step 2: Configure the Release Control server with the load balancer details

Step 3: Configure network transport options on the first node

Step 4: Install and configure Release Control on additional nodes

Step 5: Configure a load balancer

Step 1: Install and configure Release Control on the first node

On the first node, you install Release Control and perform the initial configuration as you would in a regular deployment. For details about installing and performing initial configuration of Release Control, see the *Release Control Deployment Guide*.

You must at least install the product and configure the database. However, it is recommended that you perform all the basic configuration steps, including configuring the Universal CMDB connectivity, the service desk integration settings, custom fields, and custom enumeration settings.

> **Note:** Certain configuration changes require you to restart the Release Control service. At this point, you would only need to restart a single node. If you make these configuration changes after you deploy the cluster, you will need to restart the whole cluster.

Step 2: Configure the Release Control server with the load balancer details

1. Select **Module** > **Administrator** > **Configuration** > **Server** and define the following settings in the Server pane:
   - **Server name** Enter the host name (full domain) or IP address of the load balancer.
   - **Server address** Specify the URL of the load balancer.
2. Save and apply your configuration changes (see Save and Apply Configuration Changes).

Step 3: Configure network transport options on the first node

You can configure your cluster to use multicast or unicast transport.

1. Select the type of transport.
   Select **Module** > **Administrator** > **Configuration** > **Server** > **Cluster** and in the Cluster transport box, select either multicast or unicast.
2. Configure the transport settings.
   - **If you selected Multicast transport**, configure the transport settings in the Multicast Cluster pane (**Module** > **Administrator** > **Configuration** > **Server** > **Cluster** > **Multicast Cluster**). For user interface details, see Multicast Cluster Pane.
   - **If you selected Unicast transport**, configure the transport settings in the Unicast Cluster pane (**Module** > **Administrator** > **Configuration** > **Server** > **Cluster** > **Unicast Cluster**). For user interface details, see Unicast Cluster Pane.
3. Save and apply your configuration changes (see Save and Apply Configuration Changes).
4. Restart the Release Control service.

Step 4: Install and configure Release Control on additional nodes

You can deploy a cluster of nodes over multiple instances of the same physical machine or over separate machines.

- **To deploy a cluster of nodes over multiple instances of the same physical machine:**
  Run the create node utility. For details, see Deploy Multiple Instances of Release Control on the Same Machine.
- **To install additional nodes on separate machines:**
  a. Install Release Control on the new machine.
  b. Copy the **database.properties** file from the first node's **conf** directory into the new node's **conf** directory.
  c. If you configured a service desk adapter on the first node, do the following:
     i. If Release Control is running on any of the nodes, stop the Release Control service.
     ii. Copy the **<serviceDeskName>-adapter-log4j.properties** file from the first node's **conf** directory into the new node's **conf** directory.
     iii. Copy the **SDI-<serviceDeskName>** directory from the first node's **apps** directory into the new node's **apps** directory.

Step 5: Configure a load balancer

You can configure either a hardware or software load balancer. It is recommended to use a hardware load balancer.

- **To configure a hardware load balancer:**
  Configure the third party load balancer to use **sticky session** and route requests through all nodes.
- **To configure a software load balancer:**
  Release Control includes a reference implementation of a software load balancer. This load balancer is made up of a Web server component (Apache or IIS) and a **mod_jk** component.

For an example of configuring a software load balancer with an Apache Web server, see Configure a Software Load Balancer.

Deploy Multiple Instances of Release Control on the Same Machine

The following steps describes how to use the create node utility to deploy Release Control over multiple nodes on the same physical machine.

> **Note:** When you create a node, you also create a Windows service for that node. You can choose to skip this step, and create the service at a later stage.

- Create a new node
- Remove an existing node
- Create a Windows service for an existing node
- Remove a Windows service for an existing node

Create a new node

From the **<Release Control installation directory>\bin** directory, run the following command:

```
createNode create -<node parameters>
```

Use the following parameters to define the node:

- **-DnodeName.** The name of the new node. This name is used as a directory name under the **servers** directory and as a jvmRoute in Tomcat.

  > **Note:** The default convention for the node names is server-<n>. For example, the first node is referred to as server-0.

- **-DtomcatPort.** The Tomcat control port. In server-0 this is set to 8005.
- **-DhttpPort.** The Tomcat http port. In server-0 this is set to 8080.
- **-DhttpsPort.** The Tomcat https port. In server-0 this is set to 8443.
- **-DajpPort.** The Apach Java Protocol port. In server-0 this is set to 8009.
- **-DjmxHttpPort.** The JMX http port. In server-0 this is set to 39900.
- **-DjmxRemotePort.** The JMX remote port. In server-0 this is set to 39600.
- **-DnodeDebugPort.** The debug port. In server-0 this is set to 7878.
- **-DservicePrefix.** In Windows, a service for the node will be created named **ReleaseControl <node-name>**. Use this parameter to change the prefix from **ReleaseControl** to something else.
- **-Dskip.service.** Set this to any value to skip the creation of a Windows service.

  > **Note:** You can create a Windows service for the node at a later stage, using a separate command. For details, see Create a Windows service for an existing node.
  >
  > If you did not create a Windows service, you can use the <Release Control installation directory>\StartCcm-<server-name>.bat script to start the Tomcat server.

Example:

```
createNode create -DnodeName=server-1 -DtomcatPort=9005 \

-DhttpPort=9090 -DhttpsPort=9443 \

-DajpPort=9009 -DjmxHttpPort=29900 \

-DjmxRemotePort=29600 -DnodeDebugPort=7878
```

Remove an existing node

From the **Release Control installation directory>\bin** directory, run the following command:

```
createNode remove-node -DnodeName=<nodeName>
```

where **<nodeName>** is the name of an existing node that you want to remove.

Example:

```
createNode remove-node -DnodeName=server-1
```

Create a Windows service for an existing node

If you chose to skip the creation of a Windows service when you created a new node, you can create the Windows service in a separate command.

From the **Release Control installation directory>\bin** directory, run the following command:

```
createNode create-service <node details>
```

Use the following parameters to define the node:

- **-DnodeName.** The name of the existing node for which to create the service.
- **-DjmxHttpPort.** The JMX http port. In server-0 this is set to 39900.
- **-DjmxRemotePort.** The JMX remote port. In server-0 this is set to 39600.
- **-DnodeDebugPort.** The debug port. In server-0 this is set to 7878.
- **-DservicePrefix.** The prefix of the Windows service name. By default, the prefix is **ReleaseControl**.

Example:

```
createNode create-service -DnodeName=server-1 \

-DjmxHttpPort=29900 \

-DjmxRemotePort=29600
```

Remove a Windows service for an existing node

1. From the **<Release Control installation directory>\bin** directory, run the following command:

   ```
   createNode remove-service -DnodeName=<nodeName>
   ```

   where **<nodeName>** is the name the existing node for which to remove the service.

2. Delete the relevant node files from the **<Release Control installation directory>\servers** directory.

Example:

```
createNode remove-service -DnodeName=server-1
```

Configure a Software Load Balancer

The Release Control includes a reference implementation of a software load balancer. This load balancer is made up of a Web server component (Apache or IIS) and a **mod_jk** component.

This task describes how to configure a software load balancer using an Apache Web server.

This task includes the following steps:

Step 1: Change the server.xml file on each node

> **Note:** This step should be carried out for each node in the cluster.

1. Open the **<Release Control installation directory>\tomcat\conf\server.xml** file.
2. Locate the text **<Engine** and add the following attribute:

   ```
   jvmRoute="<nodeName>"
   ```

   where **<nodeName>** is the name of the node.

   For example, on server-0, add:

```
jvmRoute="server-0"
```

Step 2: Decide which node to use as the load balancer

You can use one of the nodes on which you installed Release Control or a separate node that does not contain an installation of Release Control.

Step 3: Install Apache and mod_jk.so on the designated machine

1. We recommend to download the Apache 2.4 VC14 HTTP server and the corresponding mod_jk.so files from the following links:
   - httpd-2.4.23-win64-VC14.zip
   - mod_jk-1.2.41-win64-VC14.zip
   - httpd-2.4.23-win32-VC14.zip
   - mod_jk-1.2.41-win32-VC14.zip
2. Copy the mod_jk.so file and paste it to the **<Apache installation directory>\modules** directory.
3. Open a command window, navigate to the ..\Apache24\bin directory, and then run the **httpd –k install** command to install an Apache service.
4. Run the following command:

   <Release Control installation directory>\bin\WebServerConfigurer.bat config apache "C:\Program Files\Apache Software Foundation\Apache24"
5. After success, start the Apache server and the Release Control server.

Step 4: Configure the load balancer

1. (Windows only) add the following line to the end of the **httpd.conf** file:

   ```
   Include conf.d/*.conf
   ```
2. Create a directory called **conf.d** under the Apache installation.
3. Create a file called **rc-cluster.conf** in this directory and configure the file according to the following example (replace the host names and node names accordingly):

   ```
   LoadModule jk_module modules/mod_jk.so



   LoadModule jk_module modules/mod_jk.so
   ```

```
JkLogLevel info
JkLogStampFormat "[%a %b %d %H:%M:%S %Y] "
JkLogFile logs/mod_jk.log

JkWorkerProperty worker.list=balancer,jkstatus,server-0

JkWorkerProperty worker.jkstatus.type=status

JkWorkerProperty worker.balancer.type=lb
JkWorkerProperty worker.balancer.balance_workers=server-0,server-1
JkWorkerProperty worker.balancer.sticky_session=true

JkWorkerProperty worker.server-0.type=ajp13
JkWorkerProperty worker.server-0.host=host1.example.com
JkWorkerProperty worker.server-0.port=8009
JkWorkerProperty worker.server-0.lbfactor=1

JkWorkerProperty worker.server-1.type=ajp13
JkWorkerProperty worker.server-1.host=host2.example.com
JkWorkerProperty worker.server-1.port=9009
JkWorkerProperty worker.server-1.lbfactor=1

JkMount /ccm/messagebroker/amfpolling server-0
JkMount /ccm/messagebroker/amfpolling/* server-0
JkMount /ccm/* balancer
```

```
JkUnMount /ccm/messagebroker/amfpolling balancer

JkUnMount /ccm/messagebroker/amfpolling/* balancer

JkMount /dashboard/* balancer

JkMount /rcdocs/* balancer

JkMount /jkmanager/* jkstatus


Redirect /rc /ccm/
```

> **Note:** The chat feature in the Director module will only work if the domain of the LW-SSO is configured correctly and the access to the client is done using a fully qualified domain name.

4. Restart Apache.

Step 5: Results

You should now have a working load balancer. To verify this, you can access the balancer management URL at http://balancer-host/jkmanager/.

Reference

Server Configuration User Interface

This section includes:

- Server Pane
- Cluster Pane
- Multicast Cluster Pane
- Unicast Cluster Pane
- Multi-Tenancy Pane

Server Pane

This pane enables you to configure:

- Connection properties for the SMTP mail server responsible for sending Release Control email notifications.
- The Release Control application server name and address. Release Control uses these settings to create links to requests in the Release Control application from email notifications.
- Other general settings.

To access	Select **Module** > **Administrator** > **Configuration** > **Server**.
See also	Working with the Configuration Tab

User interface elements are described below:

UI Elements (A-Z)	Description
Client time zone	This option is relevant only when the **Force Client time zone** option is selected. The **Force Client time zone** option forces all users to see the time and date in the time zone selected here.
Default filter name	The default filter that is used in the Filters pane in **Module** > **Analysis** > **Change Requests** and in the **Activities** box in **Module** > **Director** > **Control** when logging on to the system.
Force client time zone	All Release Control users see the time and date in the same time zone, that is, the time zone selected in the **Client time zone** box. **Default:** Not selected
Server address	Specify the Release Control server address as follows: • If you install one Release Control server, specify the URL of this machine. > **Note:** If you are using a Web server, use the port of the web server. • If you cluster two or more Release Control servers behind a load balancer, specify the URL of the load balancer.
Server name	Enter the server's Fully Qualified Domain Name (FQDN). > **Note:** > • Do not use the default value **localhost** or the IP address. > • If you cluster two or more Release Control servers behind a load balancer, specify the domain name of the load balancer.
SMTP host	Enter the host name of the SMTP mail server machine.
SMTP password	Enter the password required to connect to the SMTP mail server. If

UI Elements (A-Z)	Description
	the password must be encrypted, see Password Encryption for details on encrypting passwords.
SMTP port	Specify the port to be used to connect to the SMTP mail server.
SMTP username	Specify the user name required to connect to the SMTP mail server, if one is required.
System language	The default language used by Release Control. **Default:** English
Time zone displayed	Includes the time zone in the date when the date is formatted as long date format. **Default:** Not selected

Cluster Pane

This pane enables you to select the type of transport to be used in a cluster deployment.

To access	Select **Module** > **Administrator** > **Configuration** > **Server** > **Cluster**.
Relevant tasks	Set Up a Cluster Deployment of Release Control
See also	• Working with the Configuration Tab • Cluster Deployment Overview

User interface elements are described below:

UI Elements (A-Z)	Description
Cluster transport	Select the type of transport to be used in a cluster deployment: • **Disable cluster transport.** Select this option if you are not deploying Release Control in a cluster. This is selected by default. • **Mulitcast transport.** If you select this option, configure the multicast transport details in the Multicast Cluster pane. (See Multicast Cluster Pane.) • **Unicast transport.** If you select this option, configure the unicast transport details in the Unicast Cluster pane. (See Unicast Cluster Pane.)

Multicast Cluster Pane

This pane enables you to configure the multicast transport details in a cluster deployment.

To access	Select **Module** > **Administrator** > **Configuration** > **Server** > **Cluster** > **Multicast Cluster**.
Important Information	This pane is only relevant if you select the **Multicast transport** option in the Cluster pane (**Module** > **Administrator** > **Configuration** > **Server** > **Cluster**).
Relevant tasks	Set Up a Cluster Deployment of Release Control
See also	• Working with the Configuration Tab • Cluster Deployment Overview

User interface elements are described below:

UI Elements (A-Z)	Description
Multicast address	Enter the multicast IP address. If you do not have an IP address you can create one. Valid IP addresses for a multicast address are in the class D range. It is recommended to use an address in the range 239.0.0.0/8, for example, 239.0.0.1. **Note:** Ensure that you do not use an existing cluster IP address.
Multicast port	Choose a port at random between 1025-65000. **Example:** 45566

Unicast Cluster Pane

This pane enables you to configure the unicast transport details in a cluster deployment.

To access	Select **Module** > **Administrator** > **Configuration** > **Server** > **Cluster** > **Unicast Cluster**.
Important Information	This pane is only relevant if you selected the **Unicast transport** option in the Cluster pane (**Module** > **Administrator** > **Configuration** > **Server** > **Cluster**).
Relevant tasks	Set Up a Cluster Deployment of Release Control

See also	• Working with the Configuration Tab • Cluster Deployment Overview

User interface elements are described below:

UI Elements (A-Z)	Description
Port range	If you deploy multiple nodes on the same machine, when the nodes start up, they search for the first available port. Define the number of ports which the node will search through for availability. The node starts searching from the port number defined in the **Start port** box.
Start port	>Define the port number from which the node starts searching for availability when it starts up.
Static addresses	Enter the static IP addresses of all nodes in the cluster. **Example:** If node 1 is on 10.0.0.1 and node 2 is on 10.0.0.2 and they are both on port 7800, enter the following string: `10.0.0.1[7800],10.0.0.2[7800]`.
Timeout	The time that one node waits for a message to be received by another node before there is a time-out. **Default:** 3000 milliseconds (recommended)

Multi-Tenancy Pane

This pane enables you to configure your Release Control server to serve multiple client organizations (tenants).

To access	Select **Module** > **Administrator** > **Configuration** tab > **Server** > **Multi-Tenancy.**
Important Information	This pane is specifically relevant to SaaS providers only.
Relevant tasks	Configure the Release Control Server for Multi-Tenancy (SaaS Only)
See also	• Working with the Configuration Tab • Multi-Tenancy Configuration Overview

User interface elements are described below:

UI Elements (A-Z)	Description
	Add configuration to configuration set. Enables you to add a new tenant.
	Remove configuration from configuration set. Enables you to delete the selected tenant.
Tenant allocation field	Select the change request field that is used as a basis for allocating change request tickets to the relevant tenants. **Note:** If you are integrating with Service Manager, select the **Company** field to enable you to work with multiple tenants.
Tenant Allocation Field Value	Specify a value for the Tenant allocation field. Based on this value, change request tickets are allocated to the corresponding tenant in the Tenant Name column.
Tenant Name	Specify a name for the tenant.

Time Period Configuration

This chapter includes:

Concepts

- Time Period Configuration Overview

Tasks

- Define Time Periods

Reference

- Time Periods Tab

Concepts

Time Period Configuration Overview

You configure different types of time periods and group these periods into categories. Release Control assigns processed change requests to the defined categories based on criteria that you define for each time category.

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

- **Change Window.** A period of time during which change requests may be implemented.
- **Blackout.** A period of time during which change requests may not be implemented.
- **Neutral to Changes.** A period of time indicating an external event, such as a holiday, which has no direct bearing on request implementation.

For more information about time periods, see Time Periods.

For details describing the recommended procedure for defining time periods in your organization, see Define Time Periods.

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

Change requests whose implementation is not planned within the configured **Change Window** periods are marked as **Time Period Conflict** in the Analysis module. Likewise, change requests whose implementation is planned within the configured **Blackout** periods are marked as **Time Period Conflicts**. In the Analysis List view, these requests are marked by an icon in the Abnormal column. In the Calendar view, these requests are marked with a black frame.

You can view the time period conflicts in which a selected change request is scheduled to take place either outside of a **Change Window** or within a **Blackout** period. For details, see Assess > Time Period Conflicts Tab.

> **Note:** If you defined time period-related risk factors and then updated the time period settings, you can manually run the recalculation process to calculate risk based on the new time period settings. For details, see Launch Manual Change Process Dialog Box.

Tasks

Define Time Periods

This task describes the recommended procedure for defining time periods.

This section includes:

Step 1: Identify the Change Window and Blackout periods

Step 2: Define a filter

Step 3: Define a Time Period category

Step 1: Identify the Change Window and Blackout periods

Time periods define when changes may and may not be implemented.

When defining time periods, it is recommended to first identify the Change Windows and the Blackout periods in your organization.

- A Change Window is a period of time during which requests are designated to be implemented. For example, you may define a Change Window that allows you to make changes to your company's Web site only from Saturday at 5:00 PM to Sunday at 11:00 PM.
- A Blackout period is a period of time during which requests may not be implemented. For example, you might need to define a Blackout period that restricts you from making any changes to

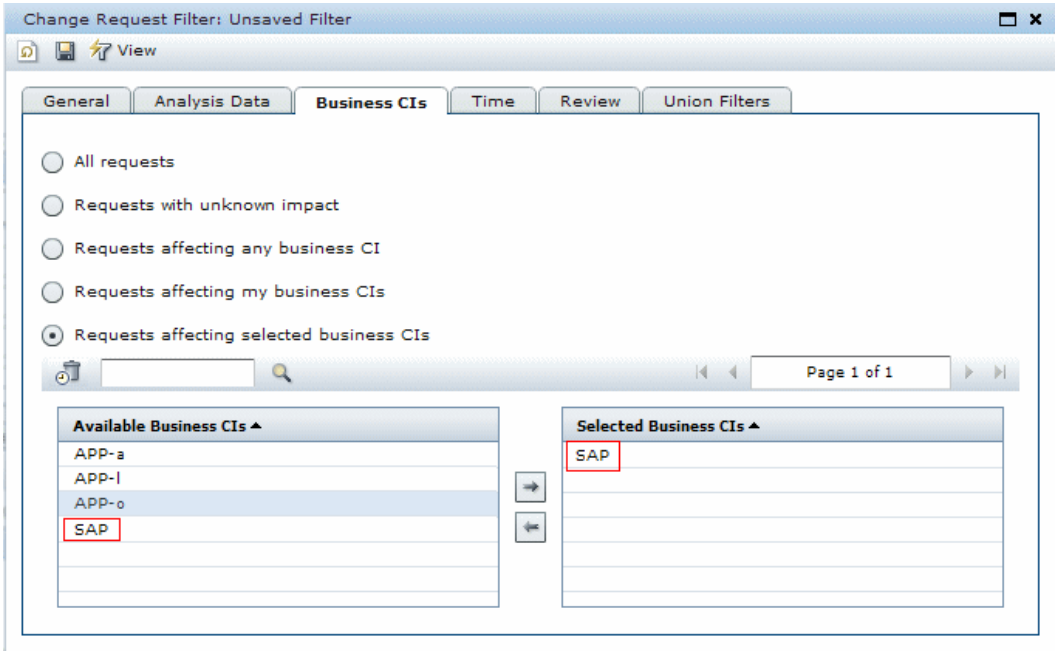
your company's Web site during periods that extend from the first day after the end of each fiscal quarter, to the day after your company issues a press release regarding the company's performance in that quarter.

Step 2: Define a filter

Define a filter that is relevant to the Change Window or Blackout period you identified in your organization.

For example, if your organization needs to make changes to your SAP application, you can create a filter that displays change requests whose impact analysis results affect certain business CIs. You define the filter to include the business CIs that are associated with the SAP application.

In the Business CIs tab of the Change Request Filter dialog box, you select the Business CIs you want to include in the filter.



For details on how to create a filter, see Activity/Change Request Filter Dialog Box.

When you save the filter, give it an appropriate name, for example, `sap_application`, and then select the **Time Period Filter** check box. The filter then appears in the **Matching Changes: Filter** box in the Administrator module's Time Periods tab and you can select this filter when defining a time period category.

> **Note:** In certain cases, the **Time Period Filter** check box cannot be selected. For details about when you can save a filter as a time period filter, see Time Period Filter.

For details on defining time periods, see Time Period Configuration Overview.

Step 3: Define a Time Period category

After you create the relevant filters, you configure a time period category for each Change Window and Blackout period. If there is more than one type of Change Window and Blackout period, you must define a different category for each one.

For example, you have to define a Change Window for both your SAP and Siebel applications. You may define a Change Window in which changes to the SAP application may only take place every Friday from 10:00 PM to 11:30 PM and another Change Window in which changes to the Siebel application may take place every Saturday night from 9:00 PM to 11:00 PM. In this case, you would define a different time period category for each Change Window.

The Time Periods tab in the Administrator module enables you to define new time period categories. When you define a new time period category relating to the SAP application, you can select the `sap_application` filter from the **Matching Changes: Filter** box to instruct Release Control to include the change request in the current category. You then define the required recurrence rule you want to apply to the time period category.

For details on defining time periods, see Time Period Configuration Overview.

Reference

Time Periods Tab

This tab enables you to configure different types of time periods and group these periods into categories.

To access	Select **Module** > **Administrator** > **Time Periods** tab.
Relevant tasks	Define Time Periods
See also	• Time Period Configuration Overview • Time Periods • Assess > Time Period Conflicts Tab

Time Periods Pane

User interface elements are described below:

UI Elements (A-Z)	Description
	Add Time Period Category. Enables you to configure time period categories. A new time period category appears in the Time Periods pane. Define the properties of the new category in the right pane. For details see Time Period Category Pane. **Note:** If you created time period categories in earlier versions of 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.
	Delete Time Period Category. Delete the selected time period category.
	Add Time Period Recurrence Rule. Enables you to configure time period recurrence rules for the selected category in the Time Periods pane. A new time period recurrence rule appears in the Time Periods pane. Define the properties of the new rule in the right pane. For details, see Time Period Recurrence Rule Pane.
	Delete Time Period Recurrence Rule. Deletes the selected time period recurrence rule.
	Refresh and Undo Modifications. Enables you to undo your general setting, category, and rule configurations (before you save these settings). The Time Periods tab is restored to its most recent saved settings.
	Save Settings. Saves your configuration settings. **Note:** The save process can take a few minutes. If users log in to Release Control during this process, they need to refresh their Analysis views in order to view the updated time period settings.
	Click to: • View general time period settings • Display time period category details **Note:** If you selected a time period category, you can click the **Expand** button to the left of the item to display the category's recurrence rules. • denotes a Change Window • denotes a Blackout period

UI Elements (A-Z)	Description
	• denotes a Neutral to Changes period
General Settings	Enables you to configure general time period settings in the right pane. For details, see the General Settings pane below.

General Settings Pane

To access	Select **General Settings** in the Time Periods pane.

User interface elements are described below:

UI Elements (A-Z)	Description
<Background pattern>	The available background patterns from which you can choose when configuring patterns for Change Windows, Blackout, and Neutral to Changes periods: • **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 Release Control's Analysis module should use to display a defined **Blackout** period in the Change Requests — Calendar View. Select one of the available background patterns.
Pattern for 'Change Window' period	The background pattern that Release Contro's Analysis module should use to display a defined Change Window period in the Change Requests — Calendar View. Select one of the available background patterns.
Pattern for 'Neutral to Changes' period	The background pattern that Release Control's Analysis module should use to display a defined Neutral to Changes period in the Change Requests — Calendar View. Select one of the available background patterns.
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 Release Control so that the duration is always applied from the current date.

UI Elements (A-Z)	Description
	For example, if you define a time period duration of 200 days, each day you log in to Release Control you can view the defined time periods for the following 200 days in the Analysis module's Change Requests — Calendar View. Incoming requests are analyzed based on these time periods.

Time Period Category Pane

To access	Click **Add Time Period Category** in the Time Periods pane.
See also	Filtering Change Requests and Activities

User interface elements are described below:

UI Elements (A-Z)	Description
Color	The color to be assigned to the new time period category. This is the color that Release Control uses to display the category in the Analysis module.
Matching changes	The criteria by which 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 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. **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** is included in the newly defined category. • **Filter.** Instructs Release Control to include a change request in the current category if the request meets the criteria of the selected filter. Select the required filter from the **Filter** drop-down list. The filters in this list were defined as a time period filter in the Save Filter dialog box (meaning the **Time period filter** check box was selected by the administrator who created the filter). For details, see Save Filter Dialog Box. For details on how to create a new filter, see Activity/Change Request Filter Dialog Box.
Name	A descriptive name for the new time period category.

UI Elements (A-Z)	Description
	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 is displayed in the Filters Selection list (see Filters Selection List).
Type	The type of time period — **Change Window**, **Blackout**, or **Neutral to Changes**. All rules in this category are of this type. For explanations of each of these time period types, see Time Period Configuration Overview.

Time Period Recurrence Rule Pane

To access	Click **Add Time Period Recurrence Rule** in the Time periods pane.

User interface elements are described below:

UI Elements (A-Z)	Description
Name	A descriptive name for the new time period recurrence rule. **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. **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 recurs every 3 days.
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.

UI Elements (A-Z)	Description
	• 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 **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.** The time of day at which you want the time period to end. • **After X days at X.** 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.

Business CI Configuration

This chapterincludes:

Concepts

- Business CI Configuration Overview

Reference

- Business CI Configuration User Interface

Concepts

Business CI Configuration Overview

Release Control enables you to view details of the business CIs affected by the change requests processed by Release Control.

In addition, you can also assign importance levels to these business CIs, and associate specific users with them. For details on how to configure business CIs, see Business CI Configuration User Interface.

Reference

Business CI Configuration User Interface

This section includes:

- Business CIs Tab
- Edit Business CIs – <Business CI Name> Dialog Box

Business CIs Tab

This tab displays the details of the business CIs included in the Universal CMDB view that you defined for Release Control.

To access	Select **Module** > **Administrator** > **Business CIs** tab.

User interface elements are described below:

UI Elements (A-Z)	Description
	Edit. Opens the Edit Business CIs – <Business CI Name> dialog box. Enables you to: • View the description of the business CI as well as other Universal CMDB-related details of the selected business CI. • Associate specific Release Control users with each business CI. For more information, see Edit Business CIs – <Business CI Name> Dialog Box.
	Show/Hide Obsolete. Toggle between hiding and displaying the obsolete CIs.
	Find. Search for a specific business CI by entering the name or part of a name in the search box. The search returns all business CIs that contain the entered string somewhere in the name. Click the **Find** button to run the search.
<View other pages>	To view other pages, use the left and right arrows. The number between the left and right arrows indicates which page is currently being displayed. For example, 1 of 9 means that the 1st page out of 9 is being displayed. Page 1 of 9

Edit Business CIs - <Business CI Name> Dialog Box

This dialog box displays Universal CMDB-related details of the business CI, and enables you to associate specific Release Control users with each business CI.

To access	Select **Module** > **Administrator** > **Business CIs** tab > **Edit**.

Business CIs Details Tab

This pane tab enables you to view details of the Business CIs.

Important Information	As part of the 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 are marked by Release Control as having a higher risk. If you are configuring the Business CI importance property using Universal CMDB 10.20 or later, you configure the importance property from within Universal CMDB. The property is referred to as **business_criticality_level** in Universal CMDB. To export old data from the importance property which was assigned within Release Control to Universal CMDB, see Upgrade the Universal CMDB Version.

User interface elements are described below:

UI Elements (A-Z)	Description
Business CI importance	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 Risk Factors Pane.

Business CI Users Tab

This tab enables you to associate specific Release Control users with the selected business CI.

User interface elements are described below:

UI Elements (A-Z)	Description
	Enforce Business CI. Enables you to ensure that the user is not able to remove the association with a specific business CI.
	Stop Enforcing Business CI. Enables the user to remove the association with a specific business CI.
	Find. Search for a specific user by entering the name or part of a name in the search box. The search returns all users that contain the entered string somewhere in the name. Click the **Find** button to run the search.

UI Elements (A-Z)	Description
	Move the selected user from the left pane to the **Selected Users** pane. The user is associated with the business CI. **Note:** You can select multiple users using the CTRL key.
	Move the selected user from the **Selected Users** pane to the left pane. The user is not associated with the business CI. **Notes:** • You can remove the association of a business CI with the current user only if the administrator did not require the user to view data for the business CI by enforcing the business CI for the user. • You can select multiple users using the CTRL key.
<Left pane>	Contains a list of the Release Control users previously defined by the administrator.
<View other pages>	To view other pages, use the left and right arrows. The number between the left and right arrows indicates which page is currently being displayed. For example, 1 of 9 means that the 1st page out of 9 is being displayed. Page 1 of 9
Selected Users pane	Users that are associated with the selected business CI.

User Configuration

This chapter includes:

Concepts

- User Configuration Overview

Reference

- User Configuration User Interface

Concepts

User Configuration Overview

Release Control enables you to configure user settings for new users, and associate business CIs with the user you are defining. In addition, you can modify the settings of an existing Release Control user. For details on how to configure user settings, see User Configuration User Interface.

For information on configuring user properties for the current Release Control user, see User Preferences.

Reference

User Configuration User Interface

This section includes:

- User Settings Dialog Box
- Users Tab

User Settings Dialog Box

This dialog box enables you to define a new user by configuring settings, including basic user details and associated business CIs, or modify the settings of an existing Release Control user.

To access	Select **Module** > **Administrator** > **Users** tab. • If you are defining a new user, click **New User** . • If you are modifying the settings of an existing user, click **Edit User** .
Important Information	If you are working in identity management mode or LDAP mode, you cannot add users in the Administrator module. For details on working in identity management mode, see Using Identity Management.
See also	• Security Configuration • User Preferences

User Details Tab

This tab enables you to configure the settings of a new user, or modify the settings of an existing one.

User interface elements are described below:

UI Elements (A-Z)	Description
Email address	The email address of the user you are defining. This is the email address to which notifications are sent for this user.
First name	The first name of the user you are defining.
Last name	The last name of the user you are defining.
Password	The password by which the user is able to log in to Release Control.
Retype password	Confirms the password entered in the **Password** box.
User ID	The user's login ID, where applicable.
User login name	The user name by which the user is able to log in to Release Control.
User role	Contains a list of the predefined roles you can assign to the user. **Notes:** • For a description of the permissions assigned to each

UI Elements (A-Z)	Description
	predefined role, see Role Manager. • You can create custom roles and define which roles appear in this list. For details, see Role Manager.

User Business CIs Tab

This pane enables you to associate business CIs with the user you are defining. If a user is associated with a CI, then the user gets notification every time the CI changes. For details on how to associate or remove business CI associations from the current user, see Business CIs Pane.

User interface elements are described below:

UI Elements (A-Z)	Description
	Enforce Business CI. Enables you to ensure that the user is not able to remove the association with a specific business CI.
	Stop Enforcing Business CI. Enables the user to remove the association with a specific business CI.
	Find. Search for a specific business CI by entering the name or part of a name in the search box. The search returns all business CIs that contain the entered string somewhere in the name. Click the **Find** button to run the search.
	Move the selected business CIs from the **Available Business CIs** list to the **Selected Business CIs** list. The business CI is associated with the current user.
	Move the selected business CIs from the **Selected Business CIs** list to the **Available Business CIs** list. The business CI is not associated with the current user.
	Show Obsolete. Toggle between hiding and displaying the obsolete CIs.
<View other pages>	To view other pages, use the left and right arrows. The number between the left and right arrows indicates which page is currently being displayed. For example, 1 of 9 means that the 1st page out of 9 is being displayed. Page 1 of 9
Available Business CIs	The business CIs in this list are not associated with the current user.

UI Elements (A-Z)	Description
My Business CIs	The business CIs in this list are associated with the current user.

Users Tab

This tab enables you to configure user settings for new Release Control users and associate business CIs with the user you are defining, edit the settings of existing users, and delete users.

To access	Select **Module** > **Administrator** > **Users** tab.
Important Information	If you are working in identity management mode or LDAP mode, you cannot add users in the Administrator module. For details on working in identity management mode, see Using Identity Management.
See also	User Preferences

User interface elements are described below:

UI Elements (A-Z)	Description
	New User. Enables you to configure user settings for new users, and associate business CIs with the user you are defining. Opens the User Settings dialog box. For details, see User Settings Dialog Box.
	Edit User. Enables you to modify the settings of an existing Release Control user. Opens the User Settings dialog box. For details, see User Settings Dialog Box.
	Delete User. Enables you to delete any previously defined Release Control users from the database.
	Find. Search for a specific user name by entering the name or part of a name in the search box. The search returns all users that contain the entered string somewhere in the name. Click the **Find** button to run the search.
<View other pages>	To view other pages, use the left and right arrows. The number between the left and right arrows indicates which page is currently being displayed. For example, 3 of 5 means that the 3rd page out of 5 is being displayed. Page 3 of 5
Email address	The email address of the user you are defining. This is the email

UI Elements (A-Z)	Description
	address to which notifications is sent for this user.
First name	The first name of the user you are defining.
ID	The user's login ID, where applicable.
Last name	The last name of the user you are defining.
Role	The role to which the user is assigned.
User name	The user name by which the user is able to log in to Release Control.

Part VII: Appendices

Utilities

> **Notes:**
>
> - **For all utilities:**
> If you have upgraded 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.
> - **For the Export Application Importance, Queue Manager, Change Cleaner, Role Manager, and Import Users utilities:**
> - If you are working in Identity Manager mode, you must use the **--im-mode** option when running a utility.
> - The **<username>** and **<password>** options are necessary to run the utility commands. If you do not specify them in the command line, the utility prompts you for them.
> - If you want to connect to the Release Control server using the non-default values for port number and server name, you must specify the values you want to use for the connection.

This chapter includes:

Reference

- Release Control Utilities

Reference

Release Control Utilities

This section provides information on the following utilities:

- Change Cleaner
- Change Context Path
- Dump
- Export Configuration Set

- Export Application Importance
- Import Configuration Set
- Import Users
- Password Encryption
- Populate
- Queue Manager
- Role Manager
- SDI Persistency Cleanup
- Web Server Configuration

Change Cleaner

The change cleaner utility enables you to count and remove Release Control database change requests. You can count and remove all available change requests, change requests before a specified date, or change requests that meet the criteria of a specified filter.

> **Caution:** The change cleaner utility submits a request to a running Release Control server, which means that after you run the change cleaner command, you cannot stop the change removal operation. Closing the command line does not stop the operation.

To count or remove requests in the database:

Run the following command:

```
<Release Control installation directory>\bin\ChangeCleaner.bat <options>
```

Following are the command line <options>:

Option	Description
-c **--count**	Count the number of changes.
-cb <yyyy-MM-dd> **--count-before <yyyy-MM-dd>**	Count the number of changes before the specified date.
--encrypted-password-file <file>	Use the encrypted password specified in <file>.
-cf <filter-name>	Count number of changes that are included in the specified filter. See

Option	Description
--count-filter <filter-name>	Specifying a Filter: Notes and Limitations.
-h **--help**	Print all command line <options>.
--im-mode	Release Control is working in Identity Manager mode.
-p <password> **--password <password>**	Encrypt a single plain-text password.
---port	Specify the port used by the Release Control server. **Default value:** 8080
--server <server>	Specify the name or IP address of the Release Control server. **Default value:** localhost
-u <username> **--username <username>**	Specify the user name required to connect to the Release Control server.
-ra **--remove-all**	Remove all changes from the database.
-rb <yyyy-MM-dd> **--remove-before <yyyy-MM-dd>**	Remove changes before the specified date.
-rf <filter-name> **--remove-filter <filter-name>**	Remove the changes and dependent tasks that are included in the specified filter. See Specifying a Filter: Notes and Limitations.

For example, to remove the changes planned or implemented before the 20th of September 2008 when working in Identity Manager mode, run the following command:

```
<Release Control installation directory>\bin\ChangeCleaner.bat --im-mode -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 Release Control Analysis or Director module.
- You can only specify filters created by users with the administrator role.

- You can only specify filters that return top level changes. (In the filter definition, the **Hierarchy level** should be defined as **Change.**)
- If the same filter name has been used for more than one filter, you cannot specify that filter name. You can define filters with the same name, for example one as a private filter of a certain user, and the other as an administrator filter.
- Filters that depend on the context of the user are not supported. (For example, **Requests affecting my business CIs**).

Change Context Path

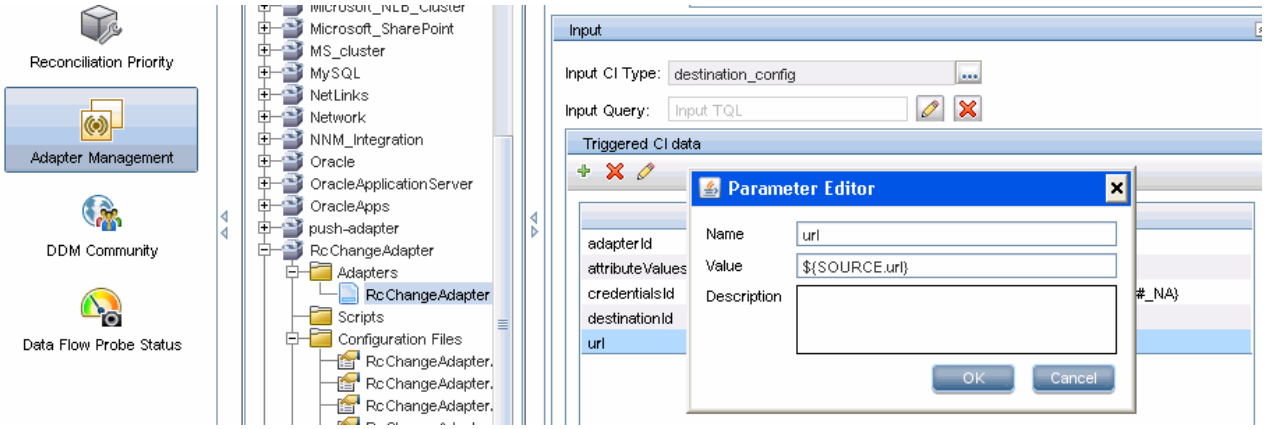
The change context path utility enables you to change the default context path of **/ccm** to a different context path in Release Control.

To change the context path:

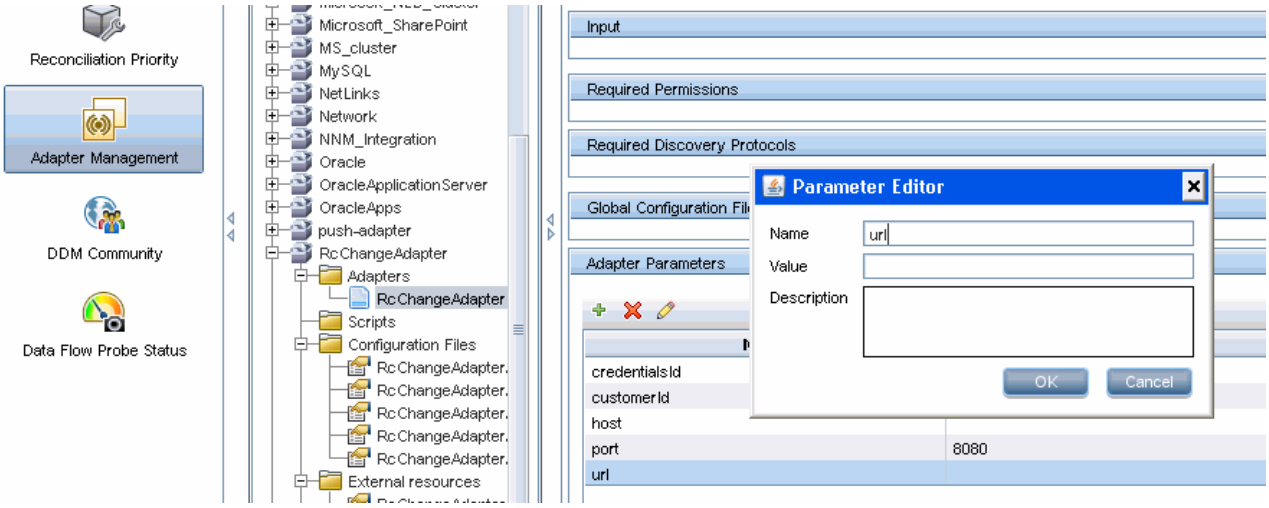
1. Stop the Release Control service.
2. For Release Control 9.13 and earlier, run the `ChangeContextPath.bat` command on Windows. For Release Control 9.20 and later, either run the `ChangeContextPath.bat` command on Windows or run the `ChangeContextPath.sh` command on Linux.
3. Type a new context path at the prompt. Note that the path should neither start nor end with a slash (/). For example, the path of **/abc/** is invalid, whereas both **abc** and **a/b/c** are correct.
4. Verify the server address. In Release Control, select **Module** > **Administrator** > **Server**. Update the server address if needed.

   > **Note:** It is not necessary to change the server address if a proxy server is being used for Release Control.

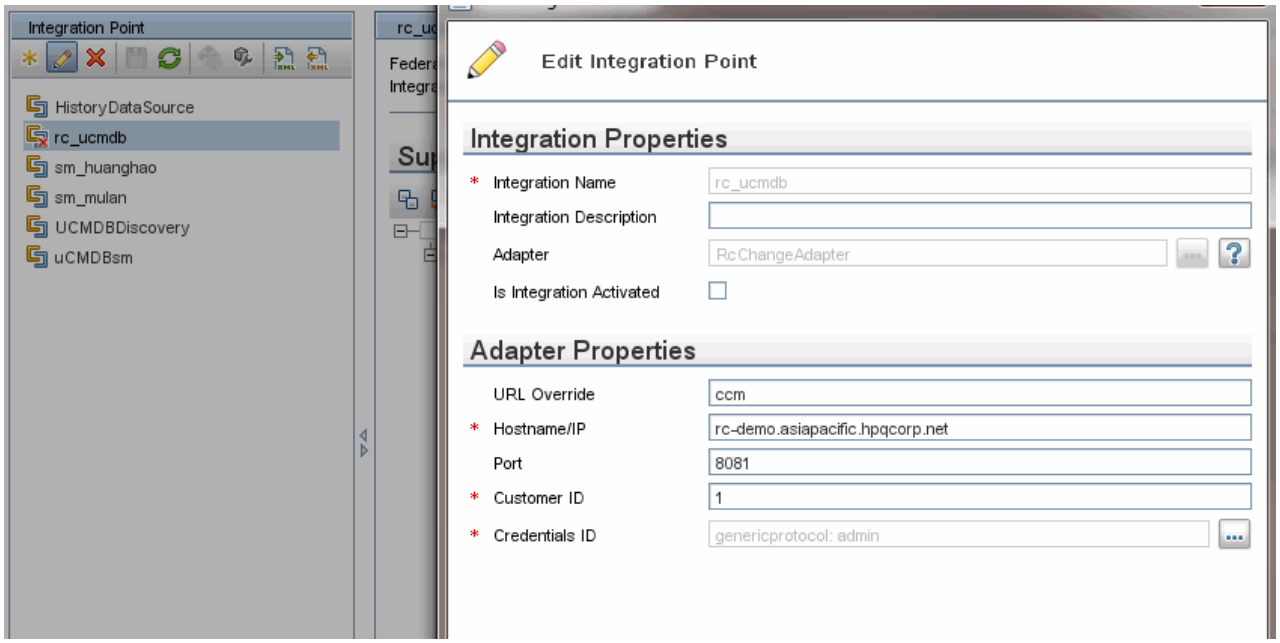
5. Change the adapter parameter in Universal CMDB. This step can be skipped if you do not use Release Control Change Adapter in uCMDB.
   a. Add the new parameter for the url.
   Go to **Adapter Management** and select **RcChangeAdapter** from the list. Click the Expand button(+), select **Adapters** > **RcChangeAdapter**. In Input section, click the Add button to add a new parameter with the name of **url** and the value of **${SOURCE.url}**.



In Adapter Parameters section, click the Add button to add a new parameter with the name of **url**.



b. Set the parameter to the new context path.
Go to **Integration Studio** and select **rc_ucmdb** from the **Integration Point** list. Click the **Edit** button to open this parameter. In the **URL Override** field, specify the new context path value.



As displayed in the screenshot above, **rc_ucmdb** is the Release Control adapter name and it may be different in your environment. You need to create a new one if it does not exist.

6. Restart the Release Control service.

> **Note:** The context path of Release Control documentation is updated automatically when the context path of **/ccm** application is changed. For example, if the context path is changed to **/CCM/CustomerA**, the context path of Release Control documentation is updated to **/CCM/CustomerA/rcdocs**.

Dump

The purpose of the Dump utility is to provide Software Support with information about the running environment in case of problems that require a service request.

The Dump utility makes a copy of all log files and active configuration sets (but not draft configuration sets), and places them into a zip file called **dump.zip**. The **dump.zip** is created by default in the directory in which the utility has been invoked.

To use the Dump utility:

Run the following command:

```
<Release Control installation directory>\bin\Dump.bat
```

Export Configuration Set

The export configuration set utility enables you to export a configuration set to a configuration dump file. Configuration dump files can later be imported to the same or different instance of Release Control. This is useful, for example, when you have a staging/test environment and would like to migrate the configuration set to a production environment.

> **Notes:**
>
> - This functionality is also available within the Release Control UI. Use this utility only in situations where for some reason the UI is locked, for example, when you started Release Control with an invalid configuration and the server cannot start.
> - This utility does not require the Release Control server to be up.
> - Before importing an SDI adapter from another Release Control server, create an SDI adapter of the same type and with the same name of the SDI adapter to be imported.

To export a configuration set:

Run the following command:

```
<Release Control installation directory>\bin\ExportCs.bat <database properties>
<configuration set ID><dump file name>
```

where **<database properties>** can be specified by pointing to the location of the **database.properties** file or by specifying each database property.

To locate the configuration set ID, run the ExportCS utility using the **--history** or **--drafts** options to list all historic and draft configuration sets. Historic configuration sets include all configuration sets that were ever activated, including the current configuration set.

Following are the command line <options>:

Option	Description
--connection-url	Database connection URL. **Note**: Use this only if **-p** is not used. Use it with --dialect, --driver, --username and --password.
--dialect	Database dialect. **Supported dialects:** H2Dialct, SQLServerDialect, Oracle9iDialect, Oracle10gDialect

Option	Description
	Note: Use this only if **-p** is not used. Use it with **--connection-url**, **--driver**, **--username** and **--password**.
--driver	Database driver class name. For example: org.h2.Driver, net.sourceforge.jtds.jdbc.Driver, oracle.jdbc.OracleDriver. **Note:** Use this only if **-p** is not used. Use it with --connection-url, --dialect, --username and --password.
--drafts	Display the configuration set drafts - all non-activated configuration sets
-f <filename> **--file <filename>**	Dump file name. **Note:** This option is required.
-h **--help**	Usage message.
--history	Display the configuration set history - all activated configuration sets.
-i <id> **--Id <id>**	ID of the configuration set to export.
-p <file> **--database-properties <file>**	Location of the **database.properties** file. **Note:** This option is required unless you use --connection-url, --driver, --username and --password to specify the database properties.
--password	Database password. **Note:** Use this only if **-p** is not used. Use it with --connection-url, --dialect, --driver and --username.
--username	Database username. **Note:** Use this only if **-p** is not used. Use it with --connection-url, --dialect, --driver and -password.
--verbose	Verbose mode.

For example:

- To export a configuration set with an id 1 to the dump.zip:

```
cd <RC installation home>\bin

ExportCs.bat -p ..\conf\database.properties -i 1 -f dump.zip
```

- To list historic configuration sets:

```
cd <RC installation home>\bin

ExportCs.bat -p ..\conf\database.properties --history
```

Export Application Importance

The Export Application Importance utility enables you to export the importance level of Business CIs from Release Control to Universal CMDB. For information about assigning importance levels to Business CIs, see Edit Business CIs – <Business CI Name> Dialog Box.

When using Universal CMDB 10.20 or later, the Business Criticality attribute is defined in Universal CMDB. If you defined the importance level in Release Control working with Universal CMDB 7.x and upgraded to 10.20 or later, you can use the **ApplicationImportanceExporter.bat** utility to export the Business Criticality attribute from Release Control to Universal CMDB.

To export the importance level using this utility:

Run the following command:

```
<Release Control installation directory>\bin\ApplicationImportanceExporter.bat

<options>
```

Following are the command line <options>:

Option	Description
--encrypted-password-file <file>	Use the encrypted password specified in <file>.
-h **--help**	Print all command line <options>.
--im-mode	Release Control is working in Identity Manager mode.
-p <password> **--password <password>**	Encrypt a single plain-text password.

Option	Description
---port	Specify the port used by the Release Control server. **Default value:** 8080
--server <server>	Specify the name or IP address of the Release Control server. **Default value:** localhost
-u <username> **--username <username>**	Specify the user name required to connect to the Release Control server.

Import Configuration Set

The import configuration set utility enables you to import a configuration set dump file into an instance of Release Control. Importing a configuration set is useful, for example, when migrating to a different environment, for example, from staging/test to production.

> **Notes:**
>
> 1. This functionality is also available within the Release Control UI. and it is recommended to use the UI option which also performs validations on the imported configuration set.
> 2. The imported configuration set is given the name of the dump file. The configuration set name is unique which means that it is not possible to import the same dump file name twice.

To import a configuration set:

1. Although the server may be up when using this utility, it is recommended that you first stop all running instances of Release Control, since some of the configurations may require a system-wide restart.
2. Run the following command:

   ```
   <Release Control installation directory>\bin\ImportCs.bat <database
   properties> <dump file name>
   ```

   where **<database properties>** can be specified by pointing to the location of the **database.properties** file or by specifying each database property.

Following are the command line <options>:

Option	Description
--activate	Activate the imported configuration.

Option	Description
--connection-url	Database connection URL. > **Note**: Use this only if **-p** is not used. Use it with --dialect, --driver, --username and --password.
--dialect	Database dialect. **Supported dialects:** H2Dialct, SQLServerDialect, Oracle9iDialect, Oracle10gDialect. > **Note:** Use this only if **-p** is not used. Use it with --connection-url, --driver, --username and --password.
--driver	Database driver class name. For example: org.h2.Driver, net.sourceforge.jtds.jdbc.Driver, oracle.jdbc.OracleDriver. > **Note:** Use this only if **-p** is not used. Use it with --connection-url, --dialect, --username and --password.
-f <filename> **--file <filename>**	Dump file name. > **Note:**This option is required.
-h **--help**	Usage message.
-p <file> **--database-properties <file>**	Location of the **database.properties** file. > **Note:** This option is required unless you use --connection-url, --driver, --username and --password to specify the database properties.
--password	Database password. > **Note:** Use this only if **-p** is not used. Use it with --connection-url, --dialect, --driver and --username.
--username	Database username. > **Note:** Use this only if **-p** is not used. Use it with --connection-url, --dialect, --driver and -password
--verbose	Verbose mode.

For example, to import a configuration set dump file called mydump.zip:

```
cd <RC installation home>\bin
```

```
ImportCs.bat -p ..\conf\database.properties -f mydump.zip
```

Import Users

The Import Users utility enables you to import a list of defined users and user properties from a CSV file to Release Control.

To import users using this utility:

Run the following command:

```
<Release Control installation directory>\bin\ImportUsers.bat <options>
```

Following are the command line <options>:

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 example, for Asian languages). If this option is not specified, the default file character set is UTF-8.
--encrypted-password-file <file>	Use the encrypted password specified in <file>.
-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. (This option may be very verbose) If this option is not specified, the default level is 1 - report errors.
-h **--help**	Print all command line <options>.

Option	Description
--im-mode	Release Control is working in Identity Manager mode.
-p <password> **--password <password>**	Encrypt a single plain-text password.
---port	Specify the port used by the Release Control server. **Default value:** 8080
--server <server>	Specify the name or IP address of the Release Control server. **Default value:** localhost
-u <username> **--username <username>**	Specify the user name required to connect to the Release Control server.

The following is an example of a CSV file with one user:

```
USERNAME,PASSWORD,FIRST_NAME,LAST_NAME,EMAIL,BUSINESS_ID,ROLE
jdoe,1234,John,Doe,jon.doe@hpe.com,jdoe,NOC
```

Updating User Details

The **business ID** and **username** fields are unique identifiers. There cannot be two different users in 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 is now updated to **johnd**. However, if the username, **johnd**, already exists in Release Control, the user is not updated.

Password Encryption

To encrypt a password:

1. Ensure that your Release Control installation directory contains a **security** directory that includes the key.txt file.

This file is created during the installation process. However if these files do not exist, then run either of the following commands in the **<Release Control installation directory>\bin** directory:

```
GenerateKey.bat [128]
```

```
GenerateKey.bat [256]
```

The GenerateKey utility generates key for ASE. The value 256 is for more cryptographic strength. However, due to import control restrictions, the version of JCE policy files that are bundled in the JDK(TM) 7 environment allow "strong" but limited cryptography to be used. To apply the value of 256 with no restrictions on cryptographic strengths:

a. Download the UnlimitedJCEPolicyJDK7.zip file at http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html.

b. Unzip this file and replace local_policy.jar and US_export_policy.jar in <Release Control installation directory>\java\lib\security directory.

2. In the **<Release Control installation directory>\bin** directory, run the following command:

```
EncryptPassword <options>
```

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.
--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**, which is where the GenerateKeys utility creates the private and public key.
-h **--help**	Print this message.

For example, to encrypt a single password, run the following command:

```
EncryptPassword.bat -p <password to encrypt>
```

3. Copy and paste the generated encrypted password (**{ENCRYPTED} <encrypted password>**) into the appropriate 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 **<Release Control installation directory>\bin** directory, run the following command:

```
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 Release Control configuration file.

Populate

The Populate utility enables you to create tables in the Release Control database.

> **Note:** This utility deletes any data that was previously stored in the database.

To use the Populate utility:

Run the following command:

```
<Release Control installation directory>\bin\Populate.bat i
```

Queue Manager

The queue manager utility enables you to manage the change requests that are waiting to enter Release Control from the service desk application.

To use the queue manager utility:

Run the following command:

```
<Release Control installation directory>\bin\QueueManager.bat <options>
```

Following are the command line <options>:

Option	Description
--encrypted-password-file <file>	Use the encrypted password specified in <file>.
-l sd **--list sd**	List all the change requests in the queue that originated from a service desk.
-l mcp **--list mcp**	List all the change requests in the queue that originated from a manual change process.
--remove sd	Delete all change requests in the queue that originated from a service desk.
--remove mcp	Delete all change requests in the queue that originated from the manual change process.
-h **--help**	Print all command line <options>.
--im-mode	Release Control is working in Identity Manager mode.
-p <password> **--password <password>**	Specify the password required to connect to Release Control.
---port	Specify the port used by the Release Control server. **Default value:** 8080
--server <server>	Specify the fully qualified server name of the Release Control server. **Default value:** localhost
-u <username> **--username <username>**	Specify the user name required to connect to the Release Control server.

For example, to delete all the change requests that originated from a service desk in the queue, run:

```
<Release Control installation directory>\bin\QueueManager.bat --remove sd
```

Role Manager

Release Control comes with a set of predefined roles you can assign to users. For a description of the predefined roles, see Predefined Roles below.

Each predefined role is assigned a set of one or more predefined permissions. For a description of the predefined permissions that come with Release Control, see Available Permissions below.

The Role Manager utility enables you to create new roles, update existing roles and delete roles using the predefined set of permissions.

To use the Role Manager utility:

Run the following command:

```
<Release Control installation directory>\bin\ManageRoles.bat <options>
```

Following are the command line <options>:

Option	Description
-a--permissions	Display a list of the predefined permissions provided by Release Control. For details, see Available Permissions.
-c **--create**	Create a new role.
--delete	Delete a role.
--description	(Optional) Enter a description for the role.
--encrypted-password-file <file>	Use the encrypted password specified in <file>.
-h **--help**	Print all command line <options>.
--im-mode	Release Control is working in Identity Manager mode.
-l **--list-all**	Display a list of the available roles.
--list-permissions	Display a list of the available permissions,
-p <password> **--password <password>**	Specify the password required to connect to Release Control.
---port	Specify the port used by the Release Control server. **Default value:** 8080
-r <role> **--role-name <role>**	Specify the name of the role.
--rename <new name>	Specify a new name for an existing role.
--server <server>	Specify the name or IP address of the Release Control server.

Option	Description
	Default value: localhost
-u <username> --username <username>	Specify the user name required to connect to the Release Control server.
--update	Modify the permissions for an existing role.

Examples:

- To create a role called `NewRole`, run:

```
<Release Control installation directory>\bin\ManageRoles.bat -c -r NewRole -a
<permission name1> <permission name 2>...
```

- To rename a role called `ExistingRole` to `NewRole`, run:

```
<Release Control installation directory>\bin\ManageRoles.bat -r NewRole --
rename ExistingRole
```

- To replace the permissions of an existing role called `NewRole`, run:

```
<Release Control installation directory>\bin\ManageRoles.bat --update -r
NewRole -a <permission name1> <permission name2>...
```

- To delete a role called `NewRole`, run:

```
<Release Control installation directory>\bin\ManageRoles.bat --delete -r
NewRole
```

Predefined Roles

The following table contains the predefined roles that come with Release Control and the permissions assigned to each one.

Role	Permissions
Business Administrator	• abortAnyManualChangeProcess • collaborate • dashboardAdministrator • editBusinessCis • editFilterCategory • editPublicFilter • editTimePeriod

Role	Permissions
	• login • planChange • teachSimilarity • triggerManualChangeProcess • viewAdminsitratorModule • viewAnalysisModule • viewDashboardModule • viewDirectorModule • viewImplementorModule
Change Manager	• abortAnyManualChangeProcess • approveChange • collaborate • editCabMinutes • login • planChange • reviewChange • sendCabInvitation • sendCabMinutes • triggerManualChangeProcess • viewAnalysisModule
Implementor	• editActivityStatus • login • viewAnalysisModule • viewImplementorModule
NOC	• editActivityStatus • editEventLog • chatAdministrator • login • rescheduleActivity • resolveAlert • viewAnalysisModule • viewDirectorModule

Role	Permissions
Restricted User	• login • viewAnalysisModule • viewDirectorModule • viewImplementorModule
System Administrator	All permissions
User	• collaborate • login • viewAnalysisModule • viewDirectorModule • viewImplementorModule

Available Permissions

The following table contains the predefined set of permissions that come with Release Control. You can assign one or more of these permissions to any role.

Permission	Description
abortAnyManualChangeProcess	Abort any manual change process (triggered by you or anyone else). For details, see Launch Manual Change Process Dialog Box.
approveChange	Approve or deny a change request, or retract the approval. For details, see Collaborate > Resolution Tab.
chatAdministrator	Add and delete chat rooms. For details, see User Communication.
collaborate	• Add, update, or delete action items. For details, see Add/Edit Action Item Dialog Box. • Add a discussion thread and vote on any change request. For details see New Discussion Thread Dialog Box.
dashboardAdministrator	Export or import Dashboard portlets.
editBusinessCIs	Edit the list of users you want to associate with a business CI.
editCabMinutes	Edit the CAB minutes of the selected change. For details, see Change Requests Toolbar Options.
editActivityStatus	Change the start and end time, and the status of an

Permission	Description
	activity in the Director module. For details, see Reschedule Activity Dialog Box.
editConfiguration	Edit, save, import, export, or activate a configuration set. For details, see Configuration Tab.
editEventLog	Add an event log message. For details, see the Event Log tab in the Activity Information Dialog Box. **Note:**Enables you to add an event log message in the Director module only.
editFilterCategory	Add, edit, or delete a filter category. For details, see General Tab.
editPublicFilter	Add, update, or delete a public filter. For details, see Filters Selection List.
editTimePeriods	Add, update, or delete time periods. For details, see Time Periods Tab.
editUser	Add, update, or delete users. For details, see Users Tab.
login	Log in to Release Control.
planChange	Save changes to a change from the Change Planner. For details, see Change Planner Dialog Box.
purgeChange	Delete changes using the ChangeCleaner utility. For details, see Change Cleaner.
rescheduleActivity	Reschedule an activity in the Director module. For details, see Reschedule Activity Dialog Box.
resolveAlert	Resolve and dismiss alert. For details, see Alerts Pane.
reviewChange	Add review notes to any change request with an Evaluation and Closure status. For details, see Review > Conclusions Tab.
sendCabInvitation	Send an invitation to the CAB meeting. For details, see Change Requests Toolbar Options.
sendCabMinutes	Send the CAB minutes of the selected change. For details, see Change Requests Toolbar Options.
teachSimilarity	Add, delete, or confirm similar changes. For details, see Similar Changes.
triggerManualChangeProcess	Run the change process again on the selected changes

Permission	Description
	and abort your own manual processes. For details, see Launch Manual Change Process Dialog Box.
viewAdministratorModule	View the Administrator module.
viewAnalysisModule	View the Analysis module.
viewDashboardModule	View the Dashboard module.
viewDirectorModule	View the Director module.
viewImplementorModule	View the Implementor module.

SDI Persistency Cleanup

By default, your service desk adapter is configured to retrieve change requests at predefined intervals.

Alternatively, you can retrieve all the change requests from your service desk starting from a point in time which is earlier than the last time the service desk application was polled. To enable this, you must delete the database persistency by running the **SDI Persistency Cleanup** utility.

> **Note:** This utility should be activated only after configuring the service desk adapter. For details, see Service Desk Adapter Properties.

To delete the database persistency:

1. Stop all running instances of Release Control.
2. From the **<Release Control Installation directory>\bin** directory, run the following command:

   ```
   SdiPersistencyCleanup.bat
   ```

3. The utility displays a list of the currently active adapters in Release Control. Select the adapter for which you want to delete persistency.
4. Start the Release Control service again.

Web Server Configuration

You can deploy Release Control to work with a Web server. You can install one of the following Web servers on the same machine as Release Control:

- Microsoft Internet Information Services (IIS) 5.x or 6.x
- Apache HTTP Server 2.2x
  The Apache installation is available in the **<Release Control installation directory>\utilities\webServerConfigurer\apache** directory.

> **Note:** Release Control cannot be configured with an Apache server if a Microsoft IIS Web server is already installed and activated on the server because the default port of both web servers is 80. The Microsoft IIS Web server must be stopped first. After the installation you can configure the apache web server to work with a different port (e.g. 90) and restart your IIS.

You may need to configure a Web server in the following cases:

- You are working with a third party identity management solution such as CA SiteMinder.
- You are deploying a software load balancer that cannot use the AJP protocol to communicate with Tomcat in a cluster deployment.

To configure the Web server, use the **WebServerConfigurer** utility.

> **Note:** After you install the Web server, ensure that the port of the Web server is specified inside the **Server address** box in the **Module** > **Administrator** > **Configuration** tab > **Server** pane. If the server address is not configured correctly, emails and reports may not work properly. For details see Server Pane.

To use the Web server configure utility:

Run the following command:

```
<Release Control installation directory>\bin\WebServerConfigurer.bat <options>
```

Following are the command line <options>:

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.

Option	Description
	• **<RC Website>.** The Web site defined for Release Control. In a new IIS installation, the Release Control default site is called **Default Web Site**.
--encrypted-password-file <file>	Use the encrypted password specified in <file>.
remove-config	Configures Release Control to work without a Web server. This command does not uninstall the Web server. **Note:** In the **<Release Control installation directory>\conf\server.settings** file, the Release Control port number in the **server-address** property is reset to the Tomcat default port (8080). Ensure that the Release Control and Tomcat port number are the same.

For example:

- To install an Apache server, run:

```
<Release Control installation directory>\bin\WebServerConfigurer.bat install
apache "C:\Apache Software Foundation\Apache 2.2"
```

- To configure an IIS server version 6 for the default Web site, run:

```
<Release Control installation directory>\bin\WebServerConfigurer.bat config
IIS 6 "Default Web Site"
```

> **Caution:**
>
> - After configuring an IIS Web server with the webServerConfigurer utility, the ISAPI filter that is responsible for the redirection from IIS to the Release Control Tomcat server, may have a status of **Unknown**. After the first user logs on to Release Control, the ISAPI filter status should be updated to **Ready**.
> - It is not possible to configure an IIS Web server that has an existing ISAPI filter running in it already. To do this you must first remove the previous installation of the mod_jk ISAPI filter, then use the webServerConfigurer utility to configure IIS for Release Control.

- To remove the Web server configuration, run:

```
<Release Control installation directory>\bin\WebServerConfigurer.bat remove-
config
```

Log Files

This chapter includes:

Concepts

- Log File Overview

Tasks

- Configure Log File Properties

Reference

- Available Log Files in Release Control

Concepts

Log File Overview

Release Control enables the setup of clusters. The cluster may include more than one server on a single instance of the operating system. Each server may include more than one adapter. For more information about cluster deployment, see Cluster Deployment Overview.

- The Release Control logs and the Tomcat server logs are generated to separate directories according to the node (server) name. The logs are generated to **<Release Control installation directory>\servers\<server name>\logs**.
  For example, for the first server (installed by default) the logs are generated to: **<Release Control installation directory>\servers\server-0\logs**.

  The logs include the following default files:

  - Tomcat logs (**localhost**, **admin**, **manager**, **host-manager**).
  - Release Control logs (**ccm*.log**) files. For a description of each of these log files, see Available Log Files in Release Control.

- An Release Control log file is created for each adapter. The logs for each adapter are generated to **<Release Control installation directory>\servers\<server name>\logs\<adapter name>-adapter>**.
- An Release Control log file is created for each CMDB adapter. The logs for each adapter are generated to **<Release Control installation directory>\servers\<server name>\logs\cmdb-<version>.**

Tasks

Configure Log File Properties

The following steps describe how to modify log definitions for the log files in the **<Release Control installation directory>\servers\<server-name>\logs** and **<Release Control installation directory>\servers\<server-name>\logs/<adapter name>-adapter>** directories.

- You modify the log definitions in the server-specific log files in the **<Release Control installation directory>\conf\ccmlog4j.properties** file.
- You modify the log definitions in the adapter-specific log files in the **<Release Control installation directory>\conf\<adapter name>-adapter-ccmlog4j.properties** file.
- You modify the log definitions in the CMDB adapter-specific log files in the **<Release Control installation directory>\conf\cmdblog4j.properties** file.

For more information about log4j files, see http://logging.apache.org/log4j/1.2/manual.html.

- Modify the types of messages displayed
- Modify file size
- Modify file backup policy

Modify the types of messages displayed

To modify the types of messages displayed, edit the following line:

```
log4j.rootCategory=WARN, ccm_general_fileout, stdout
```

The following three types of log message commands can be used:

- **FATAL** Shows fatal error messages only.
- **ERROR** Shows error messages only.
- **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 messages and additional debug messages.

> **Caution:** Setting a log to **DEBUG** level may impact performance.

Modify file 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:

```
def.file.max.size=4000KB
```

Modify file size

By default, there are 10 backup log files at any given time. To change this setting for all log files, modify the following line:

```
def.files.backup.count=10
```

Reference

Available Log Files in Release Control

The following table describes each of the server-specific **ccm*.log** files located in the **< Release Control installation directory>\servers\<server-name>\logs** directory:

Log name	Usage
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 Universal

Log name	Usage
	CMDB.
ccm_datamodel	Log file for most of the interactions between Release Control and the database.
ccm_general	Log file for the Release Control console messages that were formerly displayed in the Tomcat console.
ccm_hibernate	Log file for the interactions with the database involving the **hibernate** object to database mapper.
ccm_services	Log file for 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 Release Control reporting module.
ccm_sdi	Log file containing the number of tickets retrieved from the service desk application, and information regarding adapter connectivity problems.
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.

The following table describes each of the adapter-specific **ccm*.log** files located in the **<Release Control installation directory>\servers\<server-name>\logs\<adapter name>-adapter>** directory.

Refer to these logs when troubleshooting adapter-related problems.

Log name	Usage
ccm_general	Log file for the Release Control console messages that were formerly displayed in the Tomcat console.
ccm_jobs	Log file containing information regarding job details in the system.
ccm_sdi	Log file containing the number of tickets retrieved from the service desk application, and information regarding adapter connectivity problems.
ccm_security	Log file for security infrastructure issues.
ccm_services	Log file for Release Control server requests.

> **Note:** 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 Release Control server

> requests (**ccm_services**), depending on which part of the change request process you want to investigate.

The following table describes each of the CMDB adapter-specific log files located in the **<Release Control installation directory>\servers\<server-name>\logs\cmdb-<version>** directory.

Refer to these logs when troubleshooting CMDB-related problems.

Log name	Usage
cmdb_general	Log file containing all CMDB-related messages.
cmdb_adapter	Log file containing all adapter-related messages.
cmdb_cmdb	Log file that displays CMDB server error messages.
cmdb_commons	Log file containing Release Control internal messages.

Ticket Processing Error Handling

This chapter includes:

Concepts

- Error Handling During Change Request Conversion
- Error Handling During Change Request Analysis

Concepts

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 details, see Converting Change Requests Overview.)

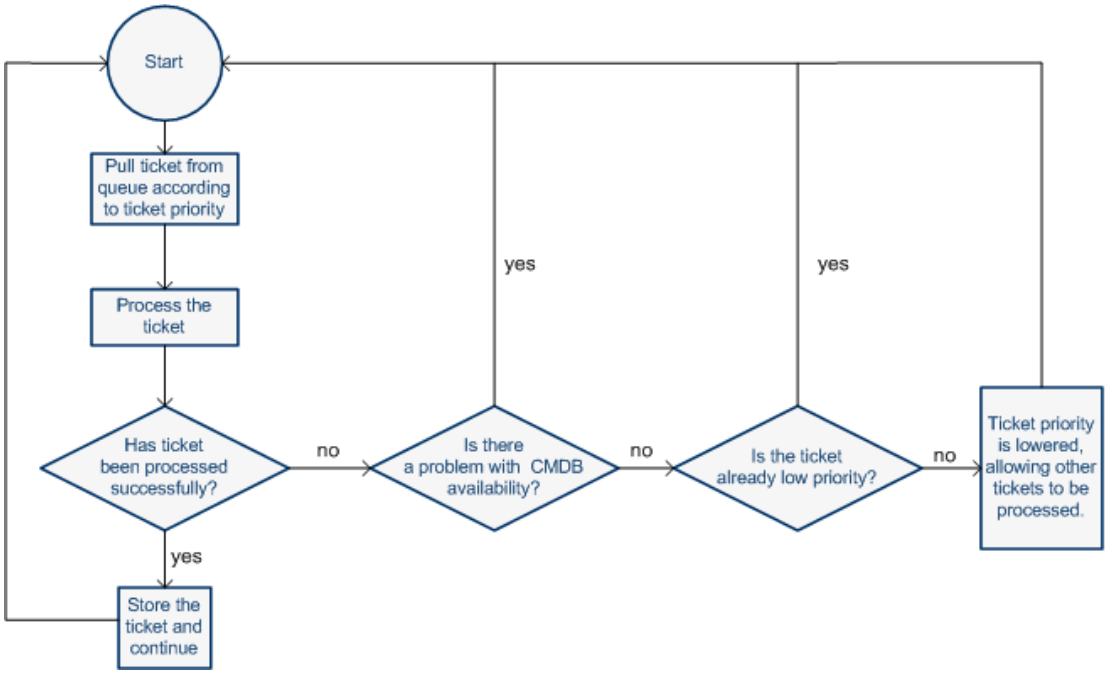
During the conversion process, Release Control may encounter errors with a ticket in the service desk. When an error is detected in one of the tickets, Release Control handles these errors as follows:

- **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),** Release Control skips over the problematic ticket and continues converting the remaining tickets. A message is written to the **ccm_general** log.

Error Handling During Change Request Analysis

Release Control analyzes change requests, performing calculations such as impact, risk, and collision analysis.

During the analysis process, 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.

Database Configuration and Maintenance

This chapter includes:

Reference

- Guidelines for Configuring and Maintaining MS SQL Server Databases
- Guidelines for Oracle Server Databases
- Working in Non-English Locales
- Database Pool Configuration Settings

Reference

Guidelines for Configuring and Maintaining 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.

This section includes:

- Recreate Data and Index Pages
- Update Statistics

Recreate Data and Index Pages

The 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.

Update 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 judgements 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.

Guidelines for Oracle Server Databases

It is recommended that you set cache attributes and collect statistics for the Oracle Server database as described below.

Set cache attributes

Set the **cache\nocache** attribute of the **CCM_CHANGES** table to **cache** by executing the following statement:

```
alter table CCM_CHANGES cache;
```

Gather statistics

It is recommended that you gather statistics once a day.

To gather statistics once a day:

1. Turn on the **MONITORING** flag to the tables in the 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.

Working in Non-English Locales

To work in a non-English language Release Control environment, you can use either an Oracle Server database or a Microsoft SQL Server database.

- **For Oracle Server**. When defining the character set, the encoding of the database can be either **UTF-8** or **AL32UTF-8**.

  > **Note:** AL32UTF-8 is the recommended.

- **For Microsoft SQL Server.** When defining the **Collation** settings, select the default option **SQL_Latin1_General_CP1_CI_AS** to support English, or select a different language if you plan to store non-English data in your database. The selected language should match the language of the Windows operating system.

  > **Note:** When using a Microsoft SQL Server database, the encoding of the database should be the same as the encoding of the specific language.

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, Release Control does not log MS SQL or Oracle Server database statements. To modify this default setting, ensure that the following line in the **<Release Control installation directory>\conf\ccmlog4j.properties** file is not commented out:

```
log4j.logger.org.hibernate.SQL=debug
```

Send documentation feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on User Guide (Release Control 9.60)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to docs.feedback@microfocus.com .

We appreciate your feedback!

MICRO FOCUS®

Java™ COMPATIBLE