OPTIMIZE

MERCURY CHANGE CONTROL MANAGEMENT™

Installation and Configuration Guide

Version 2.1

MERCURY™

BUSINESS TECHNOLOGY OPTIMIZATION

Mercury Change Control Management

Installation and Configuration Guide

Version 2.1

MERCURY™

Mercury Change Control Management Installation and Configuration Guide, Version 2.1

Mercury Interactive Corporation
379 North Whisman Road
Mountain View, CA 94043
Tel: (650) 603-5200
Fax: (650) 603-5300
http://www.mercury.com

If you have any comments or suggestions regarding this document, please send them by e-mail to documentation@mercury.com.

CCMICG2.1/01

Table of Contents

Table of Contents

Welcome to This Guide

Welcome to the *Mercury Change Control Management Configuration and Installation Guide*, which explains how to install and configure Mercury Change Control Management. Using Change Control Management, change managers and the Change Advisory Board can make more informed, and therefore more accurate, decisions regarding the approval of planned changes, thereby minimizing the business risks and costs associated with the change process.

How This Guide Is Organized

This guide contains the following parts:

Part I   Introduction

Provides an overview of Change Control Management.

Part II   Installation and Deployment

Describes the Change Control Management installation and deployment process.

Part III   Configuration

Describes how to approach Change Control Management configuration and provides detailed instructions for each part of the configuration process.

Part IV   Appendixes

Contains an appendix on password encryption and another on GMT time zones.

Who Should Read This Guide

This guide is intended for the Mercury service engineers who are responsible for installing and configuring Change Control Management. The chapter that describes how to configure various elements of the Change Control Management application is written for the application administrator. Regular users of the Change Control Management application—that is, change managers and members of the Change Advisory Board—need not read this guide.

Change Control Management Documentation

Mercury Change Control Management comes with the following documentation:

Mercury Change Control Management Installation and Configuration Guide explains how to install Change Control Management and configure the various parts of the Change Control Management system. This guide is available in PDF format on the Mercury Change Control Management CD-ROM. It can be read and printed using Adobe Reader, which can be downloaded from the Adobe Web site (http://www.adobe.com).

Mercury Change Control Management User's Guide explains how to use the Change Control Management application. This guide is available in PDF format on the Mercury Change Control Management CD-ROM.

Mercury Change Control Management Online Help includes the **Mercury Change Control Management User's Guide**. The Mercury Change Control Management Online Help is accessible from the Change Control Management application by clicking the **Help** tab.

Mercury Change Control Management API Reference explains how to work with Change Control Management's API. The API Reference is available in CHM format on the Mercury Change Control Management CD-ROM.

Mercury Change Control Management Readme provides information on last-minute known problems and limitations. The Readme is available in HTML format on the Mercury Change Control Management CD-ROM.

Additional Online Resources

Customer Support Web Site uses your default Web browser to open the Mercury Customer Support Web site. This site enables you to browse the Mercury Support Knowledge Base and add your own articles. You can also post to and search user discussion forums, submit support requests, download patches and updated documentation, and more. The URL for this Web site is http://support.mercury.com.

Mercury Home Page uses your default Web browser to access Mercury's Web site. This site provides you with the most up-to-date information on Mercury and its products. This includes new software releases, seminars and trade shows, customer support, educational services, and more. The URL for this Web site is http://www.mercury.com.

Mercury Best Practices contain guidelines for planning, creating, deploying, and managing a world-class IT environment. Mercury provides three types of best practices: Process Best Practices, Product Best Practices, and People Best Practices. Licensed customers of Mercury software can read and use the Mercury Best Practices available from the Customer Support site, http://support.mercury.com.

Documentation Updates

Mercury is continually updating its product documentation with new information. You can download the latest version of this document from the Customer Support Web site (http://support.mercury.com).

To download updated documentation:

1 In the Customer Support Web site, click the **Documentation** link.

2 Under **Please Select Product**, select Change Control Management.

Note that if the required product does not appear in the list, you must add it to your customer profile. Click **My Account** to update your profile.

3 Click **Retrieve**. The Documentation page opens and lists the documentation available for the current release and for previous releases. If a document was updated recently, **Updated** appears next to the document name.

4 Click a document link to download the documentation.

Typographical Conventions

This guide uses the following typographical conventions:

UI Elements	This style indicates the names of interface elements on which you perform actions, file names or paths, and other items that require emphasis. For example, "Click the **Save** button."
Arguments	This style indicates method, property, or function arguments and book titles. For example, "Refer to the *Mercury User's Guide*."
<**Replace Value**>	Angle brackets enclose a part of a file path or URL address that should be replaced with an actual value. For example, <**MyProduct installation folder**>**bin**.
Example	This style is used for examples and text that is to be typed literally. For example, "Type Hello in the edit box."
CTRL+C	This style indicates keyboard keys. For example, "Press ENTER."
Function_Name	This style indicates method or function names. For example, "The **wait_window** statement has the following parameters:"
[ ]	Square brackets enclose optional arguments.
{ }	Curly brackets indicate that one of the enclosed values must be assigned to the current argument.
...	In a line of syntax, an ellipsis indicates that more items of the same format may be included. In a programming example, an ellipsis is used to indicate lines of a program that were intentionally omitted.
|	A vertical bar indicates that one of the options separated by the bar should be selected.

Part I

Introduction

1

Introduction to Mercury Change Control Management

This chapter provides an overview of Mercury Change Control Management.

This chapter describes:	On page:
Working with Change Control Management	3

Working with Change Control Management

You use Change Control Management to analyze the effect of proposed software changes on the infrastructure components of your IT system. By running an impact analysis at various points in the workflow of a requested change, you can acquire a better picture of the effect the change will have and use this data to assess the business impact of the planned change on your IT environment. This enables you to make more informed decisions regarding IT changes, thereby optimizing your organization's change management process.

For example, a proposed software change might involve upgrading a database server. To perform the upgrade, you will need to stop the server. In certain cases, this could prevent users from accessing crucial services, or even cause a crash of your system. Change Control Management analyzes the potential impact of a planned change and indicates which components in your IT environment will be impacted. Based on this information, you can then evaluate the way in which you want to continue with the proposed change.

The Change Control Management work process involves the following steps:

➤ the conversion of Change Control Management-relevant Service Desk Application requests (Remedy Action Request System, Peregrine ServiceCenter, Mercury IT Governance Center, Mercury Service Desk, or other third-party application requests) to generic requests that can be processed by the Change Control Management server.

➤ the identification of configuration items (CIs) within the collected requests, based on specified analysis rules. A configuration item represents a physical or logical entity in your IT environment, such as a server, a host machine, a service, or a business process, that may be affected by a change request.

➤ an impact analysis of the identified CIs, using Mercury Application Mapping.

➤ the presentation of impact analysis calculation results—changed and affected CIs—in both the Change Control Management Web-based application and e-mail notifications.

The following diagram illustrates the way in which Change Control Management operates:
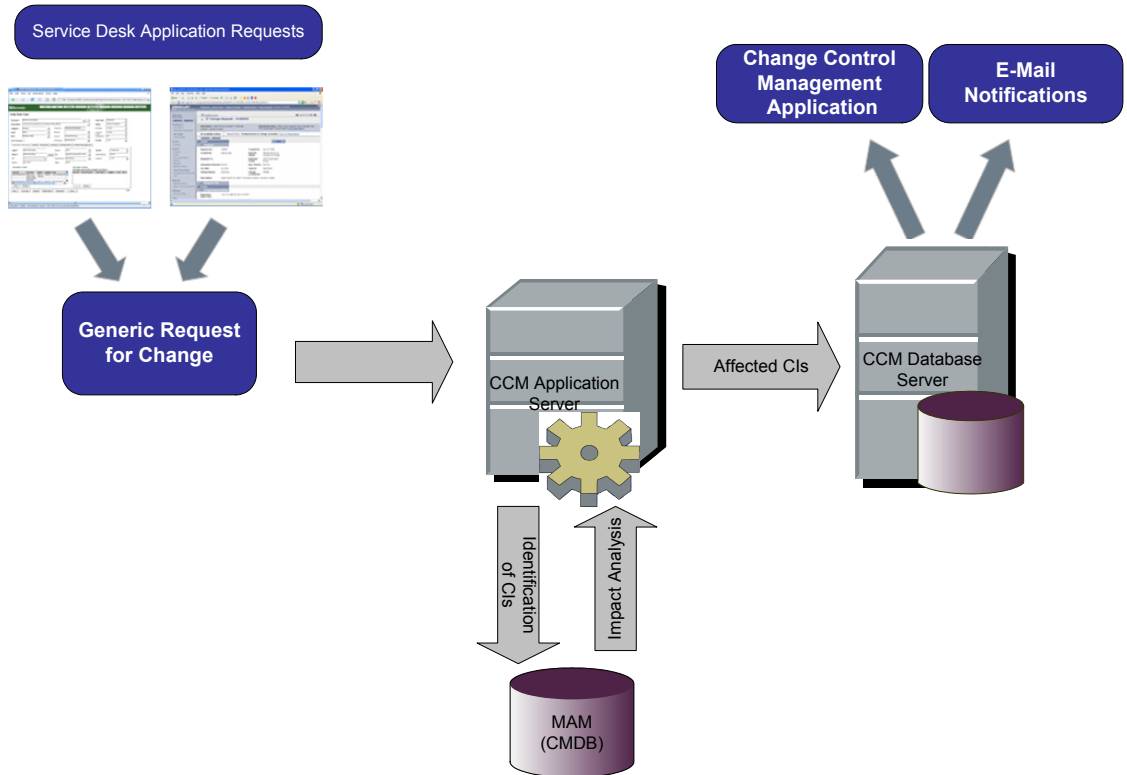
Part II

Installation and Deployment

2

Installing Mercury Change Control Management

This chapter provides an explanation of the installation and post-installation procedures you must perform in order to work with Mercury Change Control Management. It also describes the Change Control Management system requirements.

This chapter describes:	On page:
System Requirements	10
Installation Procedures	11
Post-Installation Procedures	20

System Requirements

The following table describes the system requirements for working with Change Control Management:

CPU	Windows Pentium 4
Memory (RAM)	Minimum of 2 GB
Free Disk Space	Minimum of 5 GB
Operating System	Windows 2000/2003 Server
Database	➤ Microsoft SQL Server 2000 Enterprise Edition Service Pack 4 ➤ Oracle 9i, 10
Mercury Application Mapping (MAM)	Version 3.0, 6.1, 6.2, or 6.5 For a full list of system requirements for each of these versions, refer to the Mercury Application Mapping documentation.

Note: For a list of the service desk applications supported, see "About Converting Service Desk Application-Specific Requests to Generic Requests" on page 40.

Installation Procedures

You install Mercury Change Control Management using the InstallShield Wizard for Change Control Management.

To install Change Control Management:

1 Click the **setup.exe** file located in the **disk1** folder of your Mercury Change Control Management CD-ROM. The InstallShield Wizard for Change Control Management opens.
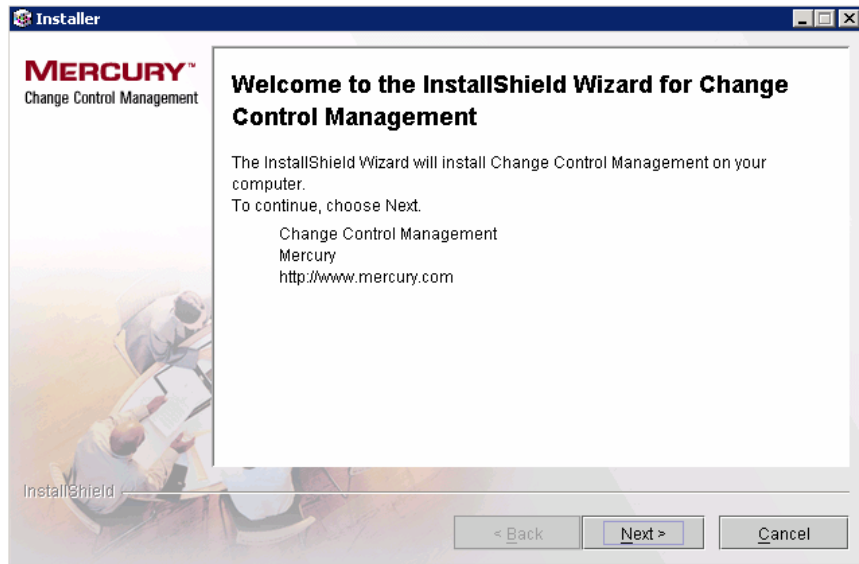
Click **Next**.

   2 Accept the terms of the software license agreement that is displayed.
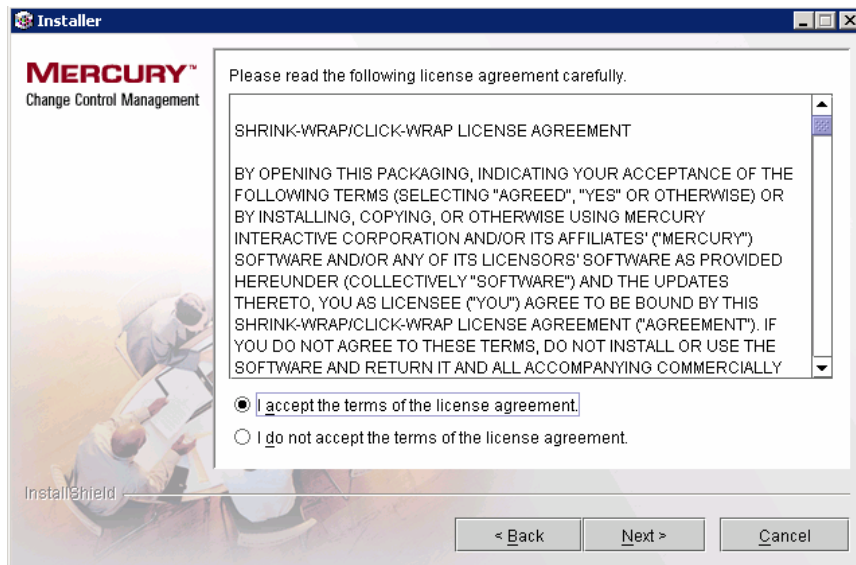
   Click **Next**.

 3 In the following screen, accept the default installation directory or click
 Browse to select a different directory. Note that the directory you select
 cannot contain spaces.
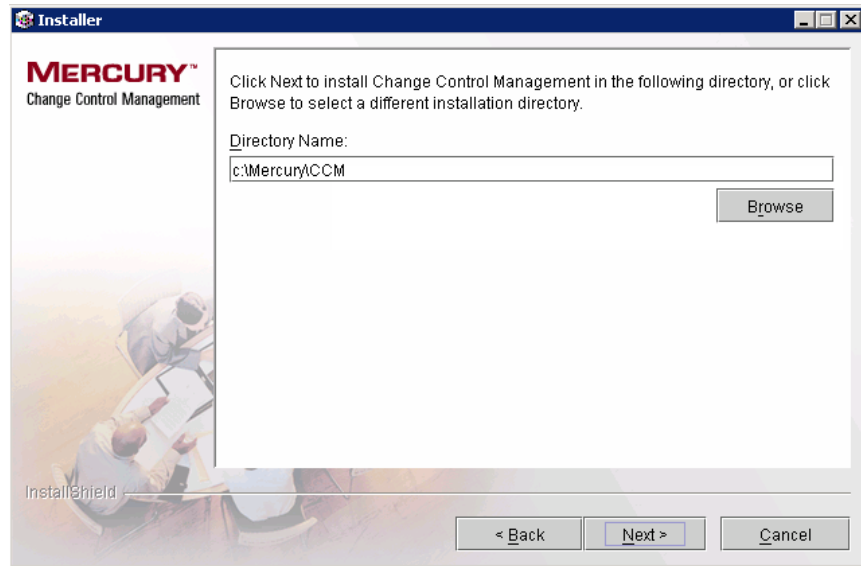
 Click **Next**.

4 In the Web Server Configuration screen, select a Web server—**Microsoft IIS** or **Apache**—to be used by Change Control Management. If you want to work with Change Control Management without a Web server, select the **Do not use a Web server** option.
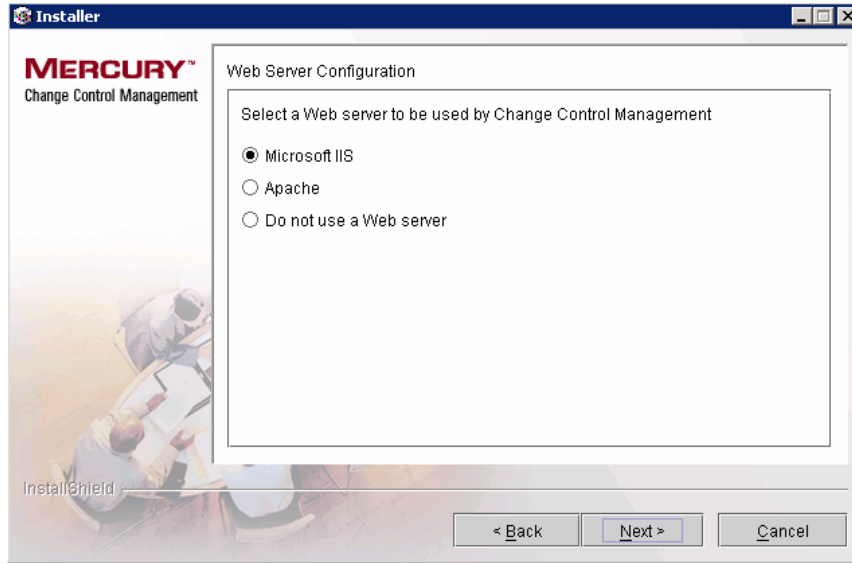
Notes:

➤ It is assumed that Microsoft IIS is already installed on the Change Control Management server machine.

➤ If you select **Apache**, the Apache Web server is installed as a Windows service (**Apache2**) on the Change Control Management server machine during Change Control Management installation.

➤ If you select **Do not use a Web server**, the Tomcat server is used, with a default port of 8080. (Note that the Tomcat server is always installed, under the name **Apache Tomcat**.)

Click **Next**. If you selected **Microsoft IIS**, proceed to step 5. If you selected **Apache**, proceed to step 6. If you selected **Do not use a Web server**, proceed to step 7.

5 If you selected Microsoft IIS in the Web Server Configuration screen, you are prompted to select the Microsoft IIS Web site under which you want to install the Microsoft IIS Web server virtual directories.
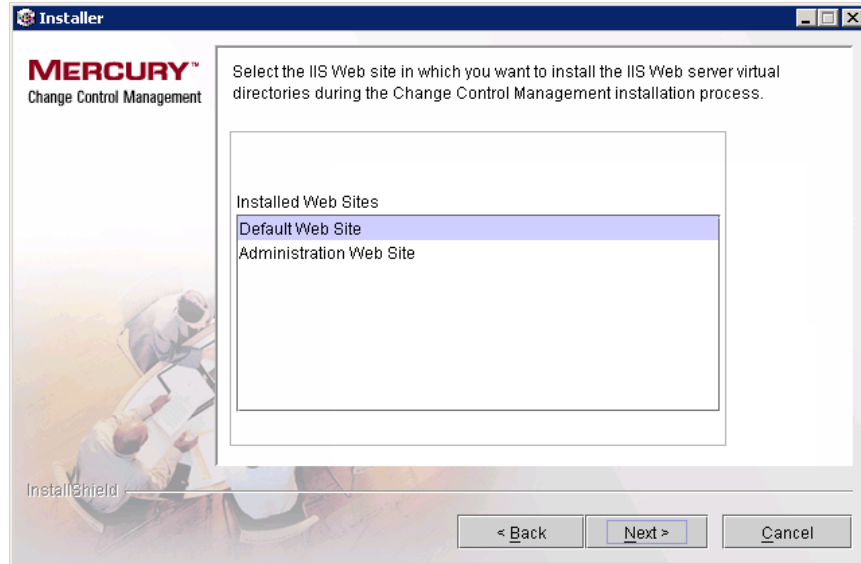
Select the required IIS Web site and click **Next**. Proceed to step 7.

6 If you selected Apache in the Web Server Configuration screen, you are prompted to enter the Apache server port through which you want the Apache Web server to communicate with the Change Control Management server, as well as the Apache Web server administrator's e-mail address.
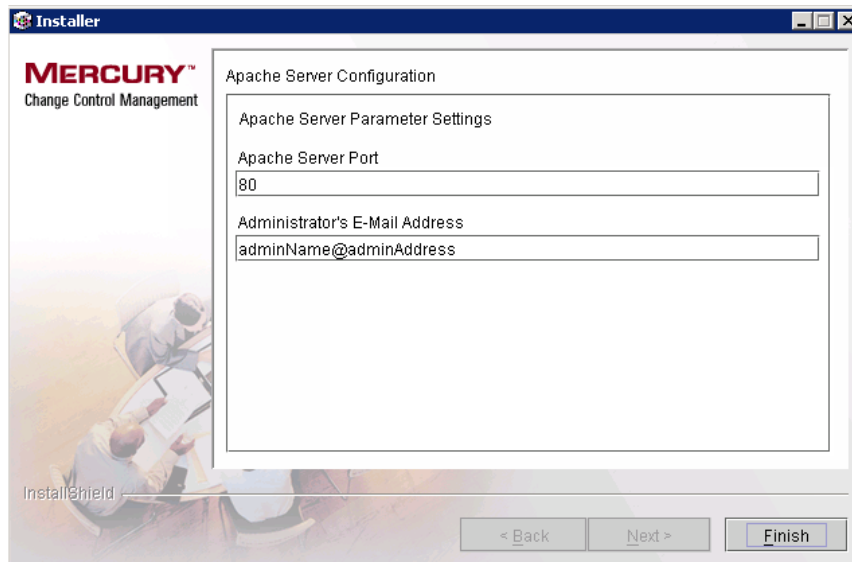
Click **Next**.

7 In the following screen, select the version of Mercury Application Management (MAM)—**3.0**, **6.1**, **6.2, or 6.5**—that you want to use with Change Control Management.
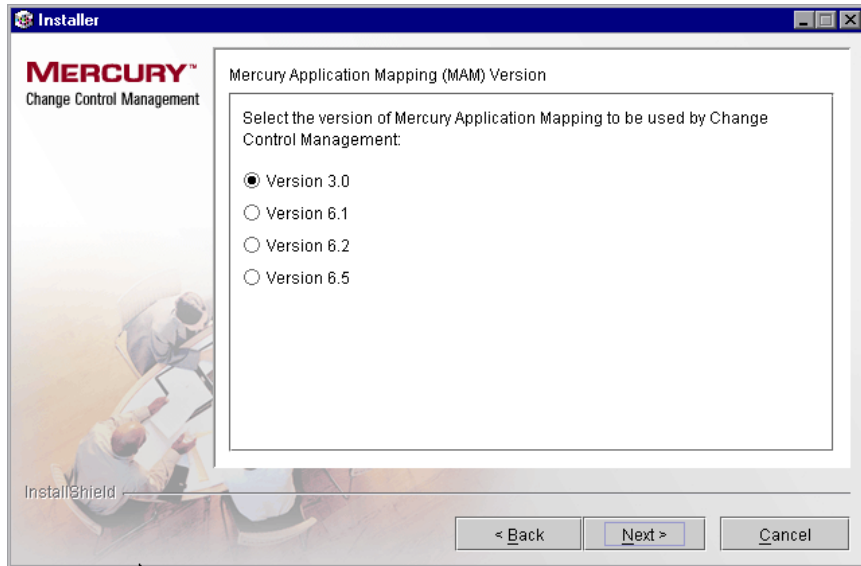
Click **Next**.

 8 Ensure that the information in the summary screen is correct.
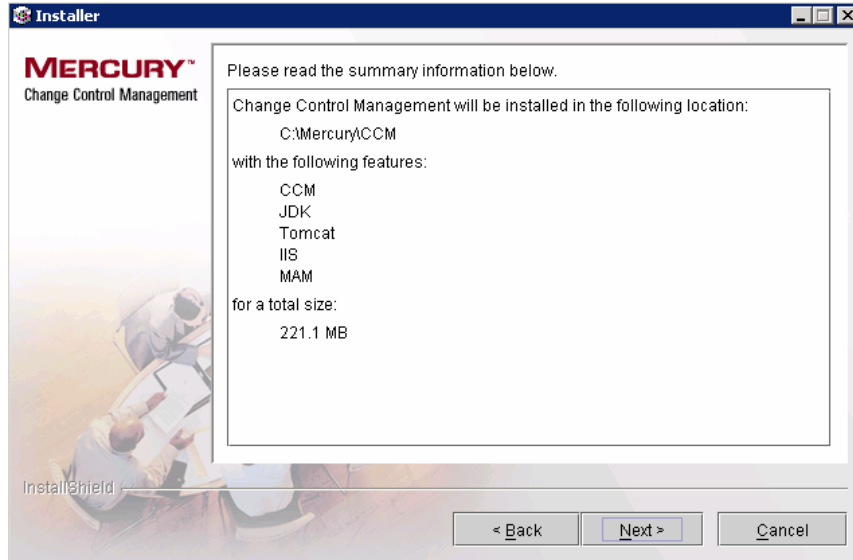
To review or change any settings, click **Back**. To accept the settings and begin installing Change Control Management, click **Next**.

 9 When the installation process has successfully been completed, click **Finish**
   in the final InstallShield Wizard screen.
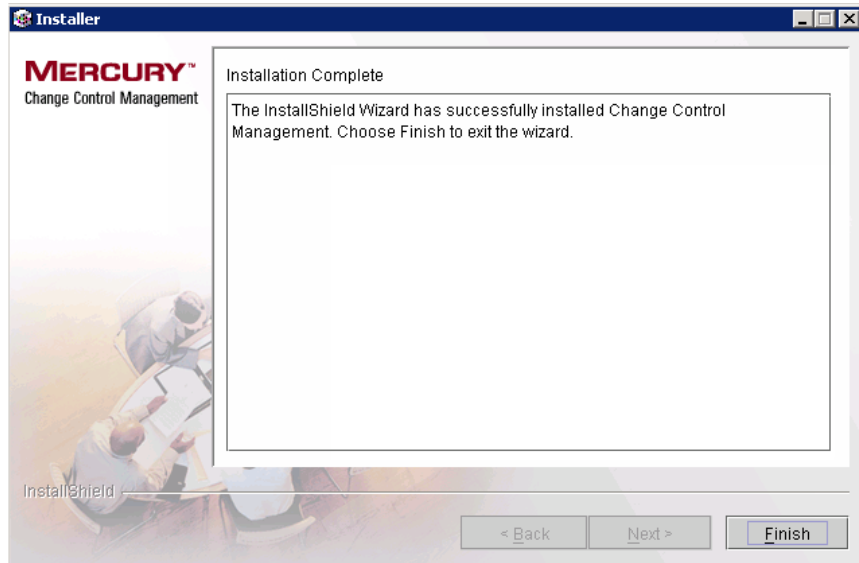
Post-Installation Procedures

After you have finished installing Change Control Management, you must perform the following post-installation procedure before you can begin working with Change Control Management.

To enable Change Control Management:

1 Create a database or user schema and configure database connection properties as described in "Configuring the Change Control Management Database or User Schema" on page 144.

2 If you are working with Mercury Application Mapping 3.0, copy the **weblogic.jar** file from the **bea81\weblogic81\server\lib** directory on the Mercury Application Mapping server to the **<Change Control Management installation directory>\tomcat\common\lib** directory.

If you are working with Mercury Application Mapping 6.1 or later, deploy the **<Change Control Management installation directory>/MAM/<version number>/extension/ccm_package.zip** package as described in "Configuring Mercury Application Mapping Settings when Working with Mercury Application Mapping 6.x" on page 110.

3 Configure a user within Mercury Application Mapping whose views reflect the IT applications affected by the change requests that Change Control Management will be processing, as described in "Configuring Mercury Application Mapping Connection Properties for the Change Control Management User" on page 108.

4 After configuring Change Control Management, change the command line directory to **<Change Control Management installation directory>\ tomcat\webapps\ccm** and run the following command: **populate.bat -ir**

5 Start the Change Control Management service (**Start** > **Programs** > **Change Control Management** > **Start Service**).

6 In a Web browser, enter the URL **http://<server_name>/ccm**, where **server_name** is the name or IP address of the Change Control Management server. If, during the installation process, you selected not to use a Web server and a Tomcat server is being used instead, this URL should point to port 8080. If you changed the Apache server port, the URL should point to the port you defined.

7 Log in to Change Control Management with the user name **admin** and the password **admin**. Ensure that you change this password once you log in. For details on changing your password and creating Change Control Management users, refer to the *Mercury Change Control Management User's Guide*.

Part III

Configuration

3

Introduction to Mercury Change Control Management Configuration

This chapter provides an overview of the Mercury Change Control Management configuration process and describes the way in which you should approach Change Control Management configuration.

This chapter describes:	On page:
Overview of the Change Control Management Configuration Process	26
How to Approach Change Control Management Configuration	30

Overview of the Change Control Management Configuration Process

To work with Change Control Management, you must configure the following within the settings and properties files located in the **<Change Control Management installation directory>/conf** directory:

➤ the way in which service desk application requests are converted to generic requests

➤ the way in which Change Control Management processes requests

➤ a Change Control Management–Mercury Application Mapping user

➤ Mercury Application Mapping settings (if you are working with Mercury Application Mapping 6.1 or later)

➤ Change Control Management system preferences

In addition, you can configure certain elements of the Change Control Management application and reconfigure Change Control Management–Mercury Application Mapping integration settings, if necessary.

Note: This section outlines the Change Control Management configuration process. For information on collecting the data necessary to begin this process, see the following section, "How to Approach Change Control Management Configuration" on page 30.

Configuring Service Desk Application Request Conversion

For requests to be processed by Change Control Management, they must be converted from their service desk application formats to a generic format. You must therefore configure a conversion policy containing a detailed service desk application field to generic field mapping scheme for standard, predefined fields, including an enumeration field value mapping scheme. In addition, your conversion policy should specify a list of service desk application customized fields to be included as additional fields in the generic request.

For details on configuring the conversion of service desk application requests to generic requests, see Chapter 4, "Configuring the Conversion of Service Desk Application-Specific Requests to Generic Requests."

Configuring Change Control Management Request Processing

To process the converted, generic requests you must configure the following:

➤ the collection of generic requests. You specify the frequency with which you want the Change Control Management server to collect the generic requests.

➤ the analysis of the collected requests. You specify the analysis rules you want Change Control Management to use in order to locate the CIs within the fields of each generic request.

➤ the calculation of impact analysis for the requests. You configure the script that determines the points at which Change Control Management calculates the impact of the identified CIs on the various components of your IT system.

➤ the sending of notifications. You format notification content and configure the thresholds for which Change Control Management will send notifications.

➤ the risk calculation factors and when to calculate collisions.

For details on configuring each of the above Change Control Management request processing components, see Chapter 5, "Configuring the Change Control Management Processing of Requests."

Configuring Mercury Application Mapping-Related Settings

To work with Mercury Application Mapping—a key component in the processing of Change Control Management requests—you must configure a user within Mercury Application Mapping whose views reflect the IT applications affected by the change requests that Change Control Management will be processing. You then specify the Mercury Application Mapping connection properties for this user within Change Control Management. For details on configuring this user, see "Configuring Mercury Application Mapping Connection Properties for the Change Control Management User" on page 108.

In addition, you must ensure that your Mercury Application Mapping correlation rules properly reflect your IT system. For details on configuring Mercury Application Mapping, refer to the Mercury Application Mapping documentation. If you are working with Mercury Application Mapping 6.2, Change Control Management uses certain correlation rules, by default, in performing an impact analysis. If required, you can specify additional or alternative correlation rules to be used.

If you are working with Mercury Application Mapping 6.1 or later, you must install a Change Control Management package on your Mercury Application Mapping server and configure connections between hosts (or other CITs) and business services within your Mercury Application Mapping views. For details, see "Configuring Mercury Application Mapping Settings when Working with Mercury Application Mapping 6.x" on page 110.

Change Control Management configuration files contain a list of preconfigured CITs (or class types) and attributes according to which you want Change Control Management to locate changed CIs in order to perform an impact analysis on them. They also contain a list of preconfigured CITs and their attributes that can be included in the results of an impact analysis, as well as Change Control Management–Mercury Application Mapping impact severity mappings. Although these elements are preconfigured, they can be reconfigured, if necessary, to better reflect your IT system. For details, see "Configuring Change Control Management–Mercury Application Mapping Integration Settings" on page 111.

Configuring the Change Control Management Application

You can choose to configure the following elements of the Change Control Management application:

➤ user name and password constraints

➤ the default Change Requests pane display settings, the default Request Details tab display settings, and the default Filter Definition pane settings

➤ the way in which customized change request fields are displayed and the filter categories in which they are included

➤ the way in which enumeration fields are displayed

In addition, if you changed certain default enumeration fields in the enumeration field configuration file, you must update the dashboard settings file with your changes.

For details on configuring the above elements of the Change Control Management application, see Chapter 7, "Configuring the Change Control Management Application."

Configuring Change Control Management System Preferences

To work with Change Control Management, you must configure the following Change Control Management system preferences:

➤ the connection properties for the Change Control Management database or user schema

➤ the connection properties for the SMTP mail server responsible for sending Change Control Management e-mail notifications

In addition, you can reconfigure the predefined Change Control Management log file properties, if required.

For details on configuring the above Change Control Management system preferences, see Chapter 8, "Configuring the Change Control Management System Preferences."

How to Approach Change Control Management Configuration

Before you begin the Change Control Management configuration process, you must collect certain information regarding the change requests for which you want Change Control Management to perform impact analysis and make decisions as to how to configure Change Control Management based on the information collected.

This section describes how to approach Change Control Management configuration, outlining the pre-configuration steps that you must perform in order to be able to properly configure Change Control Management. It also provides examples of how to work with change requests in order to collect the information to be used in the Change Control Management configuration process.

The following steps outline the Change Control Management configuration preparation process:

1 Analyze the types of change requests that exist in the service desk application.

Your service desk application may contain a number of different types of change requests. For some of these change requests, such as a request from product marketing to modify a feature, impact analysis may be highly beneficial and you will want to ensure that Change Control Management performs an impact analysis on these requests.

2 Analyze the processing workflow of the change requests for which you want Change Control Management to perform impact analysis.

Once you have identified the types of change requests for which you want Change Control Management to perform impact analysis, it is important that you attend a Change Advisory Board meeting to gain a better understanding of the way in which change requests are managed in the organization.

After you have gained an understanding of the way in which the organization manages its change requests, you can more effectively analyze the processing workflow of the requests for which you want to perform impact analysis and determine the points in the workflow at which it would be beneficial to perform impact analysis. Note that these impact analysis points may be related to request field changes, or they may be associated with certain steps in the workflow.

The following is an example of a typical change request workflow:
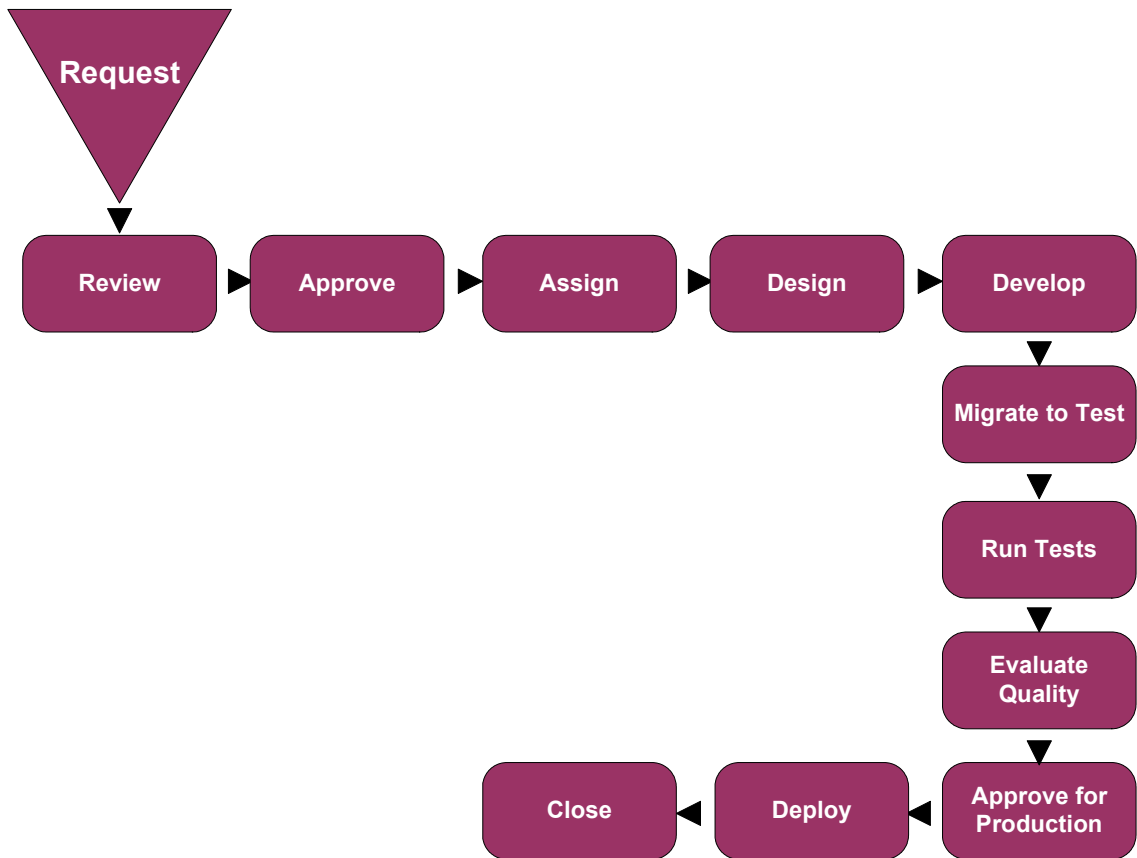
In this case, it would be beneficial to have Change Control Management perform an impact analysis before the change is approved for production.
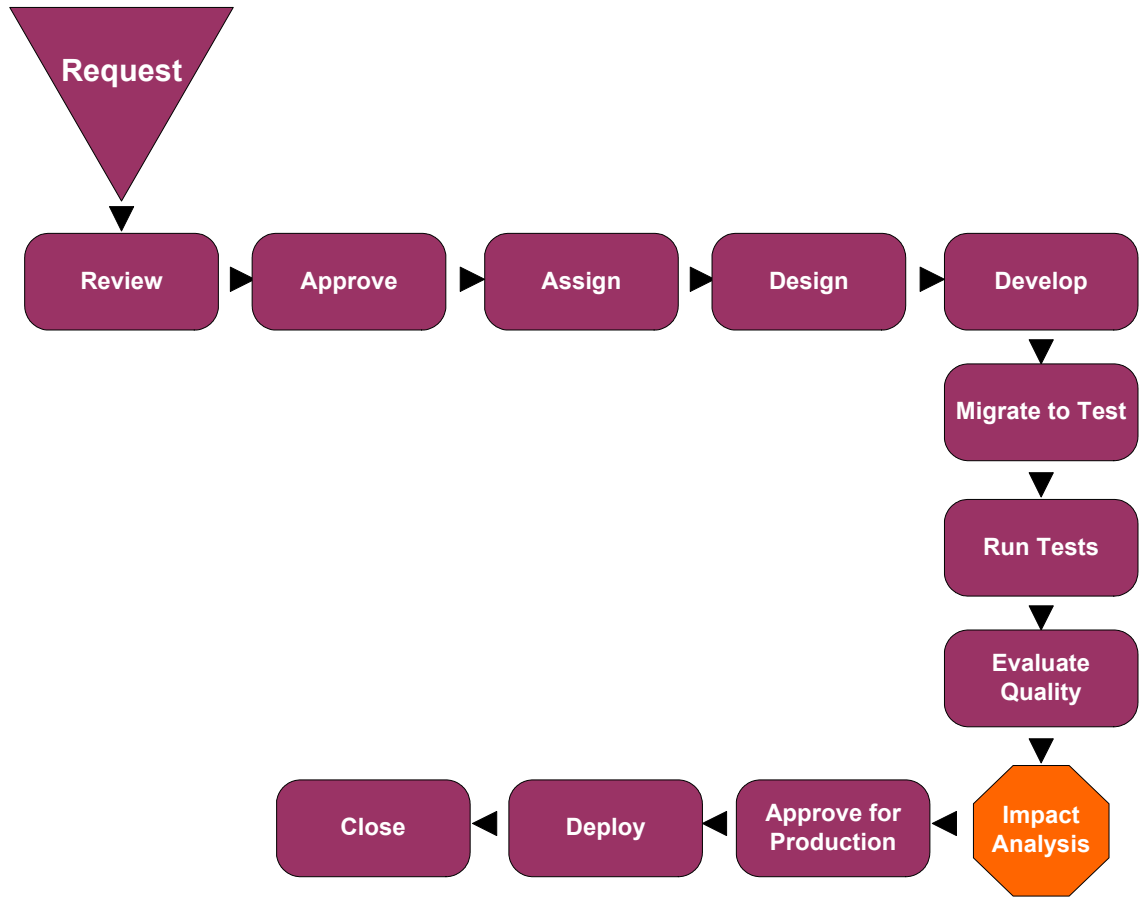
Running an impact analysis before a software or hardware change is approved for production provides you with an indication of the effect the change will have on your production environment. This allows you to ensure that any modifications that may have been made to your system's infrastructure during development will not have an adverse effect on your system once the change is deployed in production.

3 Consider the pre- and post-conversion filters you want to use.

Once you have determined the points in the workflow at which you want Change Control Management to perform impact analysis, it is recommended that you decide how to filter out the requests or request updates that you want Change Control Management to ignore. This helps ensure that the Change Control Management server will not be overloaded with unnecessary request data. For example, you could set a filter that prevents requests that are of the status **New** or **Assigned** from reaching the Change Control Management server if you are interested in performing an impact analysis on requests that have at least reached the **Pending Approval** stage.

You can use either a pre-conversion or a post-conversion filter for this purpose. A pre-conversion filter is written using the terminology of the service desk application. If a request does not meet the filter requirements, it is not converted to a generic request. A post-conversion filter is written using Change Control Management request terminology and operates on requests once they have been converted from service desk application-specific to generic requests.

4 Analyze the service desk application's request fields and the values that can be assigned to each field.

In particular, ensure that you identify the following types of fields:

➤ standard ITIL fields (predefined fields in Change Control Management). These include fields such as the request ID number and open/updated dates, as well as enumeration fields, such as the priority, severity, and status fields, which contain values.

➤ fields that will serve as input for the impact analysis. These can include both standard and customized fields that contain information on the system's impacted CIs, such as servers, routers, or host machines.

➤ fields that decision-makers will want to view in the Change Control Management application.

➤ fields that will contribute to the risk and collision analysis calculations.

5 **Determine how to map the service desk application enumeration fields and field values to the generic enumeration fields and field values.**

For each of the enumeration fields, determine which fields and field values in your service desk application requests should be mapped to each generic request field and field value. For example, you might determine that both the **High – 2** and **Urgent – 3** priority field values in your service desk application requests should be mapped to the **Immediate – 3** generic request priority field value. You might also determine that two different fields in your service desk application (for example, the status field and the approval field) should be mapped to a single generic request field (for example, the status field).

6 **Analyze the way in which the CIs appear in the service desk application requests.**

You instruct Change Control Management to identify and use CIs in impact analysis by specifying analysis rules for these values. In order to specify analysis rules, you must first identify the location and format of the CIs in the service desk application requests. For example, it is important to note the field in which a machine host name appears and the pattern that the host name follows (such as **US_CA_DOCTEAM_1**). You can then create an analysis rule that instructs Change Control Management to locate this host name and use it within an impact analysis.

7 **Determine when you want Change Control Management to calculate the impact of the identified CIs on the components of your IT system.**

Change Control Management performs impact analysis according to a calculation rule that you configure. A calculation rule determines the point or points at which an impact analysis is performed, such as when a certain step in the workflow is reached or a certain field is changed. For example, you can create a calculation rule that instructs Change Control Management to perform an impact analysis if a change is made to a request's Change Process field. If a change is made to the Change Process field, Change Control Management "looks up" the identified CIs in this field and calculates the impact of any change made to these CIs.

 8 Ensure that both your Mercury Application Mapping configuration settings and your Mercury Application Mapping–Change Control Management integration settings properly reflect your IT system.

Change Control Management locates impacted CIs, presents a list of changed and affected CIs, and calculates impact severity based on Mercury Application Mapping configuration settings within Change Control Management properties files. These settings are preconfigured, however they can be reconfigured to more accurately reflect your IT system, if necessary.

In addition, you should ensure that your Mercury Application Mapping correlation rules reflect your IT system. If you are working with Mercury Application Mapping 6.2 or later, Change Control Management uses certain correlation rules, by default, in performing an impact analysis. If required, you can specify additional or alternative correlation rules to be used.

If you are working with Mercury Application Mapping 6.1 or later, ensure that you configure connections between hosts (or other CITs) and business services as required.

If you are working with Mercury Application Mapping 6.5, configure the settings of the latent changes feature.

 9 Determine the risk calculation factors

 10 Determine when to calculate collisions.

 11 Determine the thresholds for which notifications should be sent.

Change Control Management sends notifications as a result of changes in the status of requests. It is recommended that you configure notifications to be sent only as a result of meaningful changes in status, such as a change from **Pending Approval** to **Approved**.

4

Configuring the Conversion of Service Desk Application-Specific Requests to Generic Requests

This chapter describes how to convert change requests that originate in various service desk applications to generic requests that can be processed by Change Control Management. It also describes how to customize Change Control Management fields.

Customizing Change Control Management Fields

Before you can begin converting service desk application requests to Change Control Management requests, you must define the fields you want to include in your Change Control Management requests. These include both standard ITIL, predefined fields and customized fields, which you define in the **<Change Control Management installation directory>/conf/ fields.settings** file. For details on customizing fields in the **fields.settings** file, see "Configuring Change Request Field Settings" on page 121.

In addition, you must define the enumeration fields to be used by Change Control Management in the **<Change Control Management installation directory>/conf/enumerations.settings** file. The **enumerations.settings** file contains a default list of status, priority, severity, estimated risk, and request (change/task) levels and the numeric value assigned to each level. The numeric values determine the order in which the enumeration levels are displayed in the Change Control Management application. You can modify the status, priority, severity, and estimated risk enumeration levels and values as required. For example, if you want Change Control Management to use the status **Completed** instead of **Closed**, you would change the following:

```
<entry>
    <name>CLOSED</name>
    <value>4</value>
</entry>
```

to:

```
<entry>
    <name>COMPLETED</name>
    <value>4</value>
</entry>
```

Notes:

➤ After the Change Control Management server is launched an **<id>** element is added to each enumeration entry. This element should not be modified or removed.

➤ The request level enumeration settings should not be modified.

➤ If you add or modify an enumeration setting, you must configure the way in which the enumeration setting is displayed in the Change Control Management application. You do so within the **<Change Control Management installation directory>/conf/enumeration-labels.properties** file. For details on configuring the **enumeration-labels.properties** file, see "Configuring Enumeration Field Display Settings" on page 141. If you do not configure the way in which the enumeration setting is displayed, a warning message is recorded in the Change Control Management log files.

➤ 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 the Conversion Scripts" on page 70. If you modify the way in which the enumeration setting is displayed in the Change Control Management application, you need not modify your conversion scripts.

➤ If you add or modify a severity enumeration setting, you must modify the corresponding severity enumeration setting in the **<Change Control Management installation directory>/conf/mam-integration.settings** file. For details on configuring the impact severity level settings in the **mam-integration.settings** file, see "Mapping Change Control Management–Mercury Application Mapping Severity Levels" on page 115.

About Converting Service Desk Application-Specific Requests to Generic Requests

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 organized according to their original change/task hierarchy and transferred to the Change Control Management server.

The following diagram illustrates the service desk application request conversion process performed by the Service Desk Integration module:
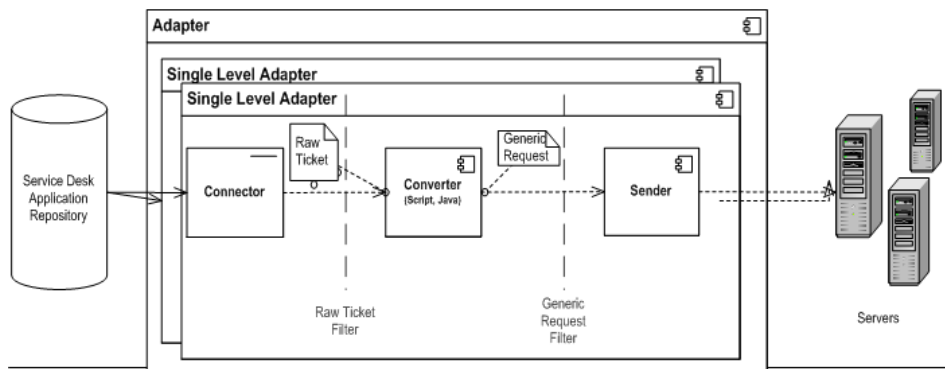
As shown above, each service desk application-specific adapter contains two single-level adapters—one to convert changes, and the other to convert tasks. Each single-level adapter contains the following three subcomponents:

➤ **Connector**. Collects new changes/tasks from the service desk applications.

➤ **Converter**. Converts the changes/tasks from their service desk application formats to a generic format that Change Control Management can recognize.

➤ **Sender**. Organizes the converted changes/tasks according to their original change/task hierarchy and transfers them to the Change Control Management server.

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 Change Control Management 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 Change Control Management server.

The Service Desk Integration module supports the following service desk applications:

Application	Version
Mercury IT Governance Center	➤ 6.0 Service Pack 10 and later – Web Services ➤ 5.5 and later – RML (RML must be enabled)
Remedy Action Request System	5.1
Peregrine ServiceCenter	➤ 6.1 Service Pack 1 – Web Services ➤ 6.2 ➤ All versions that support Peregrine Connect-It, with XML target enabled.
Mercury Service Desk	6.5

Overview of Adapter Configuration

To convert service desk application requests using the Service Desk Integration module, you must configure the appropriate adapter for each service desk application.

To configure an adapter, you must:

➤ set up the adapter configuration file

➤ write 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 several servers 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.

For details on configuring the adapter attributes, see "Configuring the Common Adapter Attributes" on page 44.

➤ 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.

For details on configuring the connector attributes, see "Configuring the Connector Attributes" on page 48.

➤ 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.

For details on configuring the converter attributes, see "Configuring the Converter Attributes" on page 69.

Conversion Scripts

Conversion scripts are called by the adapter and are responsible for the actual conversion of changes and tasks from their service desk application format to a generic format.

Each script must contain certain functions. For a detailed list and explanation of these functions, see "Writing the Conversion Scripts" on page 70.

Location and Naming Conventions of Service Desk Integration Files

The Service Desk Integration files are located in the **<Change Control Management installation directory>/examples** directory. This directory contains the following:

➤ A configuration file for each adapter. This file must have a **.settings** extension. In addition, it is recommended that the name of the configuration file be identical to the name defined for the adapter within the configuration file, as follows:

```
<adapter name>.settings
```

For example, if the name defined for the adapter is **peregrine-adapter**, the configuration file name must be **peregrine-adapter.settings**.

➤ A subdirectory for each adapter configuration file. The subdirectory holds the conversion scripts responsible for the actual conversion of requests from their service desk application format to a generic format.

The name of the subdirectory must be identical to the name defined for the adapter in the configuration file and must have a **.ext** extension, as follows:

```
<adapter name>.ext
```

Following the example above, there must be a subdirectory called **peregrine-adapter.ext** to hold all the conversion script files for the Peregrine ServiceCenter adapter.

After you have properly named the adapter configuration file and subdirectory, you must move both of these entities to the **<Change Control Management installation directory>/conf** directory.

Configuring the Common Adapter Attributes

The top section of the adapter configuration file contains the following adapter attributes, which are common to all service desk applications:

Property Name	Description	Default Value
adapter-name (mandatory)	A logical name that represents the adapter's name within the Change Control Management system. For example: peregrine-adapter **Note:** This name is also used for the scripts (**.ext**) directory, as explained in "Location and Naming Conventions of Service Desk Integration Files" on page 43. In addition, this name is used to identify the adapter in the log files.	—
version (mandatory)	The version of the adapter, which is identical to the version of Change Control Management that you are using. **Note:** This property should not be modified.	—

Property Name	Description	Default Value
service-desk-application (mandatory)	A unique, logical name for the service desk system that you are using. This can be any name you select. For example: Service Center **Note:** This is the name that will be used for the service desk within the Change Control Management application.	—
number-of-tickets	Sets the number of requests that are processed at a time, ensuring that Change Control Management 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 Change Control Management or your service desk application. It should be high enough to retrieve all requests from the service desk application and should 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** should exceed 50. In processing requests, Change Control Management attempts to use the **number-of-tickets**, but may return more or fewer requests from the service desk application. **Note:** To determine the **number-of-tickets**, consult with the people responsible for the service desk application(s) within your organization.	**50**

Property Name	Description	Default Value
polling-schedules	A list of cron expressions separated by the new line character. Format: 30 * * * * <new line> 0 * * * *	—
polling-frequency	The frequency (in seconds) that the service desk application is polled for change requests.	If **polling-schedules** and **polling-frequency** are undefined, then the default is **30 seconds**.
initial-load-state	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. Format: MM/dd/yy HH:mm:ss z	**null**

Property Name	Description	Default Value
request-types (mandatory)	Lists all request types that the adapter collects, including all request type levels. By default, level 1 is used for changes are and level 2 is used for tasks. (For details on configuring request type levels, see "Customizing Change Control Management Fields" on page 38.) \<request-type level="1"\> \<connector\> \<connector-type\>peregrine\</connector-type\> \<properties\> timeZone=PST wsDateFormatPattern=yyyy-MM-dd'T'HH:mm:ss.SSS'Z' queryDateFormatPattern=MM/dd/yy HH:mm:ss idProperty=header.changeNumber lastUpdatedPropertyForQuery=sysmodtime lastUpdatedPropertyForResult=sysmodtime creationDatePropertyForQuery=orig.date.entered creationDatePropertyForResult=header.openedTime keyMethodName=ChangeNumber serviceUrl=http://labm1ccm01:12670/scserver61/ws userName=falcon password= \</properties\> \</connector\> \<converter\> \<converter-type\>scriptConverter\</converter-type\> \<properties\> scripts=convert.js \</properties\> \</converter\> \</request-type\>	—

47

Property Name	Description	Default Value
sender	Specifies where requests should be sent. In the **<sender>** section, you specify where requests should be sent by setting the **<sender-type>** element to one of the following values: ➤ **sender.** Requests are sent to the Change Control Management server. ➤ **xmlsender.** Requests are sent to XML files (used for debugging) rather than the Change Control Management server.	**sender**

Configuring the Connector Attributes

The connector attributes, which enable the adapter to connect to the service desk application, differ according to the service desk application from which you are converting requests.

Note: You must specify the connector attributes separately for each request type included in the adapter configuration file.

This section describes:

➤ "Remedy Action Request System Connector Settings" on page 49

➤ "Peregrine ServiceCenter Connect-It Connector Settings" on page 50

➤ "Peregrine ServiceCenter Web Services Connector Settings" on page 52

➤ "IT Governance Center Web Services Connector Settings" on page 56

➤ "IT Governance Center RML Connector Settings" on page 57

➤ "Database Connector Settings" on page 60

➤ "Oracle Database Connector Settings" on page 64

➤ "Mercury Service Desk Connector Settings" on page 66

Remedy Action Request System Connector Settings

To connect to the Remedy Action Request System service desk application, you must first ensure that the certain Remedy Action Request System files are accessible to the Change Control Management server.

➤ Copy **arapi50.dll**, **arjni50.dll**, **arrpc50.dll**, and **arutl50.dll** from the Remedy Action Request System installation directory to an arbitrary directory on the Change Control Management server machine. Set the **PATH** environment variable to point to this directory.

➤ Copy **arapi50.jar** and **arutil50.jar** from the Remedy Action Request System installation directory to the **<Tomcat server installation directory>/ common/lib** directory.

The following connector attributes must then be configured in the Remedy Action Request System adapter configuration file (by default, **remedy-adapter.settings**):

Property Name	Description	Default Value
connector-type (mandatory)	The logical name of the adapter. This must be set to remedy.	—
serverName (mandatory)	The name of the Remedy Action Request System server.	—
serverTcpPort	The TCP port of the Remedy Action Request System server.	**0**
serverRpcNum	The RPC number of the Remedy Action Request System server.	**0**
userName (mandatory)	The user name with which Change Control Management connects to the Remedy Action Request System server.	—
userPassword (mandatory)	The password with which Change Control Management connects to the Remedy Action Request System server. Note that the password should be encrypted. For details on encrypting passwords, see Appendix A, "Password Encryption."	—

Property Name	Description	Default Value
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.	—

Peregrine ServiceCenter Connect-It Connector Settings

The following Peregrine ServiceCenter Connect-It connector attributes must be configured in the Peregrine ServiceCenter Connect-It adapter configuration file (by default, **peregrine-folder-adapter.settings**):

Property Name	Description	Default Value
connector-type (mandatory)	This must be set to: xmlFolderWatcher	—
idPropertyName (mandatory)	The property name of the request's ID in each XML file to which the Peregrine Connect-It application sends service desk application requests.	—

Property Name	Description	Default Value
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 Peregrine Connect-It application places service desk application requests in XML file format.	—
pattern	The file name pattern as a regular expression. For more details, see http://java.sun.com/j2se/1.4.2/docs/api/java/util/regex/Pattern.html	No pattern - all files will be read.

Note: Ensure that the Change Control Management user has read permissions to the directory in which Peregrine ServiceCenter Connect-It places service desk application requests in XML file format.

Peregrine ServiceCenter Web Services Connector Settings

The following Peregrine ServiceCenter Web Services connector attributes must be configured in the Peregrine ServiceCenter Web Services adapter configuration file (by default, **peregrine-ws-adapter.settings**):

Property Name	Description	Default Value
connector-type (mandatory)	For changes, this must be set to: peregrineChange For tasks, this must be set to: peregrineTask	—
idProperty (mandatory)	The property name of the ID field in the instance returned from the Web service.	—
lastUpdatedPropertyForQuery (mandatory)	The property name of the **last-update** field used to query the Peregrine ServiceCenter Web service (the field name used in an expert search on the Peregrine ServiceCenter client machine).	—
creationDatePropertyForQuery (mandatory)	The property name of the **creation-date** field used to query the Peregrine ServiceCenter Web service.	—
lastUpdatedPropertyForResult (mandatory)	The property name of the **last-update** field in the instance returned from the Peregrine ServiceCenter Web service (usually the field name exposed as API).	—

Property Name	Description	Default Value
creationDatePropertyForResult (mandatory)	The property name of the **creation-date** field in the instance returned from the Peregrine ServiceCenter Web service.	—
keyMethodName (mandatory)	The name of the method for request keys (usually the ID field name).	—
timeZone (mandatory)	The Peregrine ServiceCenter server time zone, used for converting the last updated time of a request from Peregrine. **Note:** To handle Daylight Savings Time, use an area time zone instead of specifying a time relative to GMT.	—
wsDateFormatPattern (mandatory)	The date format used in the Web service answer. For available formats, see: http://java.sun.com/j2se/1.4.2/docs/api/java/text/SimpleDateFormat.html	—
queryDateFormatPattern (mandatory)	The date format used for querying the service center 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.html	—
serviceUrl (mandatory)	The Web service URL.	—

Property Name	Description	Default Value
userName (mandatory)	The user name with which Change Control Management connects to the service center system.	—
password (mandatory)	The password with which Change Control Management connects to the service center system. Note that the password should be encrypted. For details on encrypting passwords, see Appendix A, "Password Encryption."	—

Note: Peregrine ServiceCenter Web service requests are not always sorted by the last modification or creation date when they are returned, which is necessary in order for the Peregrine ServiceCenter Web Services adapter to work correctly. You must therefore apply the following workaround to return Peregrine ServiceCenter Web service requests sorted by the last modification or creation date:

In the Peregrine ServiceCenter Web service database table, under **System definition** > **Tables** > **<request table name>** > **Keys**, click **New** and add a **not null: <last updated field name>** key constraint. Click **New** again, and add a **not null: <creation date>** key constraint.

To verify that the workaround yields the required results, run an expert search by entering a query for requests that are newer than a specific modification or creation date, and ensure that the requests are returned sorted.

Using Peregrine ServiceCenter Web Services, you can modify the availability of request fields. Each time you modify these settings, a new WSDL is created and you must regenerate the Web Services stub (**.jar**) file from the new WSDL.

To generate the .jar file:

 1 Locate the **create-peregrine-jar.bat** script in the **<Change Control Management installation directory>utilities/peregrine-wsdl-generator** directory and activate it using the following command:

create-peregrine-jar <WSDL URL>

 2 Copy the **peregrine-changeRequestClient.jar** file from the **<Change Control Management installation directory>utilities/peregrine-wsdl-generator** directory and place it in the **<Change Control Management installation directory>/tomcat/webapps/ccm/WEB-INF/lib** directory.

IT Governance Center Web Services Connector Settings

This section describes how to connect to the IT Governance Center Web Services service desk application.

To connect to the IT Governance Center Web Services service desk application:

1 The following files have to be copied to **<Change Control Management installation directory>\tomcat\webapps\ccm\WEB-INF\classes:**

➤ For ITG 6, copy the **<Change Control Management installation directory>\examples\service-desk-examples\itg-ws-adapter.ext\itg6\itg-wss-config.wsdd** file.

➤ For ITG 7, copy the **<Change Control Management installation directory>\examples\service-desk-examples\itg-ws-adapter.ext\itg7\itg-wss-config.wsdd** file.

2 In the **<Change Control Management installation directory>\examples\service-desk-examples\itg-ws-adapter.ext** directory, modify the LINK variable in both scripts to point to your ITG server.

In the same directory, modify the scripts to use the ITG tokens which are relevant to your ITG request types.

3 For each change request level (release and change), the following connector attributes must then be configured in the IT Governance Center Web Services adapter configuration file (by default, **itg-ws-adapter.settings**):

Property Name	Description	Default Value
connector-type (mandatory)	This must be set to: itg	—
requestTypeName (mandatory)	The name of the IT Governance Center request type to be retrieved. Note that this field is case-sensitive.	—

Property Name	Description	Default Value
parentRequestTypeName (mandatory, if the request is a change with a parent release)	The name of the IT Governance Center parent request type to be retrieved, if the request is a task (meaning it has a parent change associated with it).	—
username (mandatory)	The user name with which Change Control Management connects to IT Governance Center.	—
password (mandatory)	The password with which Change Control Management connects to IT Governance Center. Note that the password should be encrypted. For details on encrypting passwords, see Appendix A, "Password Encryption."	—
serviceUrl (mandatory)	The URL of the IT Governance Center Web service.	—

4 Add a new change request field named **mam-ticket-id** of type **text**.

Apply the analysis rule **mam-ticket** to this field with the analysis rule level set to **All**.

For information about creating new change request fields and applying analysis rules, see "Creating or Modifying Change Request Fields" on page 123.

IT Governance Center RML Connector Settings

To work with the IT Governance Center RML adapter, you must first enable RML. For details on enabling RML when working with IT Governance Center, refer to the IT Governance Center documentation.

The following connector attributes must then be configured in the IT Governance Center RML adapter configuration file (by default, **itg-rml-adapter.settings**):

Property Name	Description	Default Value
connector-type (mandatory)	This must be set to: rmlItgConnector	—
dbUrl (mandatory)	The URL of the IT Governance Center database.	—
userName (mandatory)	The user name with which Change Control Management connects to the IT Governance Center database. **Note:** The Change Control Management user should have read permissions to the database schema.	—
password (mandatory)	The password with which Change Control Management connects to the IT Governance Center database. Note that the password should be encrypted. For details on encrypting passwords, see Appendix A, "Password Encryption."	—
driverClassName	The name of the JDBC driver. Ensure that the driver exists in the **<Tomcat server installation directory>/common/lib** directory.	**oracle.jdbc. OracleDriver**

Property Name	Description	Default Value
sqlQueryByLastUpdate (mandatory)	The SQL query that returns the change request set according to the requests' **last-update** field values. **Note:** SQL queries must have one parameter which is the **last-update** field value. Query results must be sorted according to the **last-update** values.	—
sqlQueryByCreationDate (mandatory)	The SQL query that returns the change request set according to the requests' **creation-date** field values. **Note:** SQL queries must have one parameter which is the **creation-date** field value. Query results must be sorted according to the **creation-date** values.	—
lastUpdatedFieldName	The name of the column in the result set that contains the **last-update** field value.	**LAST_UPDATE_ DATE**
lastUpdatedFieldType	One of the following values: **time**, **timestamp**, **date**, **milliseconds**, or **seconds**	**timestamp**
creationDateFieldName	The name of the column in the result set that contains the **creation-date** field value.	**CREATION_ DATE**
creationDateFieldType	One of the following values: **time**, **timestamp**, **date**, **milliseconds**, or **seconds**	**timestamp**
idFieldName	The name of the column in the result set that contains the ID field value.	**REQUEST_ ID**

Property Name	Description	Default Value
dbHelper-class-name	The class name used for the db helper.	**com.mercury. onyx.sdi.sdk. db. DBHelperImpl**
connectionProperties	The IT Governance Center database properties, in java.util.Properties format. For example: key1=value1; key 2=value2	**oracle.jdbc.V8 Compatible= true**
connectionPoolProperties	The IT Governance Center database pool connection properties, in java.util.Properties format. For possible values, see: http://www.mchange.com/projects/ c3p0/index.html	—
maxRowsToReturn	A limitation on the number of rows a request query should return. Not currently for use.	The working bulk size set in the adapter.

Database Connector Settings

The following database connector attributes must be configured in the appropriate database adapter configuration file:

Property Name	Description	Default Value
connector-type (mandatory)	This must be set to: dbConnector	—
dbUrl (mandatory)	The URL of the database.	—
userName (mandatory)	The user name with which Change Control Management connects to the database.	—

Property Name	Description	Default Value
password (mandatory)	The password with which Change Control Management connects to the database. Note that the password should be encrypted. For details on encrypting passwords, see Appendix A, "Password Encryption."	—
driverClassName (mandatory)	The name of the JDBC driver. Ensure that the driver exists in the **<Tomcat server installation directory>/common/lib** directory.	—
sqlQueryByLastUpdate (mandatory)	The SQL query that returns the change request set according to the requests' **last-update** field values. To make use of a stored procedure, use the following syntax: { call <procedure_name> (?) } **Note:** Both SQL queries and stored procedures must have one parameter which is the **last-update** field value. Query results must be sorted according to the **last-update** values.	—

Property Name	Description	Default Value
sqlQueryByCreationDate (mandatory)	The SQL query that returns the change request set according to the requests' **creation-date** field values. To make use of a stored procedure, use the following syntax: { call <procedure_name> (?) } **Note:** Both SQL queries and stored procedures must have one parameter which is the **creation-date** field value. Query results must be sorted according to the **creation-date** values.	—
lastUpdatedFieldName (mandatory)	The name of the column in the result set that contains the **last-update** field value.	—
lastUpdatedFieldType (mandatory)	One of the following values: **time**, **timestamp**, **date**, **milliseconds**, or **seconds**	—
creationDateFieldName (mandatory)	The name of the column in the result set that contains the **creation-date** field value.	—
creationDateFieldType (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.	—
dbHelper-class-name	The class name used for the db helper.	**com.mercury. onyx.sdi.sdk. db. DBHelperImpl**

Property Name	Description	Default Value
connectionProperties	The database properties, in java.util.Properties format. For example: key1=value1; key 2=value2	Empty properties
connectionPoolProperties	The database pool connection properties, in java.util.Properties format. For possible values, see: http://www.mchange.com/projects/c3p0/index.html	—
maxRowsToReturn	A limitation on the number of rows a request query should return. Not currently for use.	The working bulk size set in the adapter.

Note: A sample database adapter configuration file, **sample-db-adapter.settings**, is available in the **<Change Control Management installation directory>/examples** directory.

Oracle Database Connector Settings

The Oracle database connector attributes are identical to the above database connector attributes, except for the following:

Property Name	Description	Default Value
connector-type (mandatory)	This must be set to: oracleDbConnector	—
sqlQueryByLastUpdate (mandatory)	The SQL query that returns the change request set according to the requests' **last-update** field values. To make use of a stored procedure, use the following syntax: { ? = call <procedure_name> (?) } **Note:** Both SQL queries and stored procedures must have one parameter which is the **last-update** field value. Query results must be sorted according to the **last-update** values. Stored procedures should return a **REF CURSOR** type.	—

Property Name	Description	Default Value
sqlQueryByCreationDate (mandatory)	The SQL query that returns the change request set according to the requests' **creation-date** field values. To make use of a stored procedure, use the following syntax: { ? = call <procedure_name> (?) } **Note:** Both SQL queries and stored procedures must have one parameter which is the **creation-date** field value. Query results must be sorted according to the **creation-date** values. Stored procedures should return a **REF CURSOR** type.	—
dbHelper-class-name	The class name used for the db helper.	**com.mercury. onyx.sdi.sdk.db. OracleDB ConnectorHelper**

Note: A sample Oracle database adapter configuration file, **sample-db-oracle-adapter.settings**, is available in the <**Change Control Management installation directory**>/**examples** directory.

Mercury Service Desk Connector Settings

This section describes how to connect to the Mercury Service Desk application.

To connect to the Mercury Service Desk application:

1 The following Mercury Service Desk connector attributes must be configured in the Mercury Service Desk adapter configuration file (by default, **msd-adapter.settings**):

Property Name	Description	Default Value
connector-type (mandatory)	This must be set to: MSD	MSD
wsDateFormatPattern (mandatory)	The date format used in the Web service answer. The format should be as follows: yyyy-MM-dd HH:mm:ss	—
callForm (mandatory)	The call form from which you want to get the data. In most cases this would be: it_release for a release it_pso_request for a change (These values are the Categories defined in the Call Forms settings in Mercury Service Desk)	—

Property Name	Description	Default Value
serviceUrl (mandatory)	The Web service URL. This should be in the following format: http://<MSD ip>[:MSD port]/<MSD context path>/svc?service=esql The MSD context path is composed of the MSD version and MSD instance and should be something similar to: /MSD62SP1-BIN/MSDISA62.DLL/MSD62SP1/MSDDEMO62SP1/	—
userName (mandatory)	The user name with which Change Control Management connects to Mercury Service Desk.	—
password (mandatory)	The password with which Change Control Management connects to Mercury Service Desk.	—
fieldsToFetch (advanced)	A comma-separated list of request fields to retrieve, or ***** to collect all request fields.	—

2 Add the following new change request fields of type **text** to the Change Control Management application:

- ➤ **Topic**
- ➤ **Service**
- ➤ **Category**
- ➤ **Urgency**

For information about creating new change request fields, see "Creating or Modifying Change Request Fields" on page 123.

3 Apply the analysis rule **mam-object-id** to the **changed-ci-list** field with the analysis rule level set to **All**. For details about how to apply analysis rules, see "Apply analysis rules to the field settings" on page 131.

4 Within Mercury Service Desk, you define the following settings to make a Mercury Service Desk ticket eligible for Change Control Management processing.

➤ Set the call form to **Allow Exposure to CCM**.

➤ Set the selected classification to **Allow exposure of calls with this classification to CCM**.

➤ **Expose this project to CCM** should be set on the workflow step which should cause the ticket to be exposed to CCM.

Note: For more information about the required Mercury Service Desk settings for Change Control Management integration, refer to the Mercury Service Desk documentation.

Configuring the Converter Attributes

The converter attributes, which call the conversion script files where the field mapping and filter functions are defined, must be configured separately for each request type included in the adapter configuration file.

You configure the following converter attributes in the adapter configuration file:

Property Name	Description	Default Value
converter-type (mandatory)	This must be set to: scriptConverter	—
scripts (mandatory)	A comma-separated list of script file names. The adapter searches for these files in the adapter's extension subdirectory (**conf/<adapter name>.ext**) or in the **conf** directory. For examples of conversion script files, see the sample scripts in the **<Change Control Management installation directory>/examples** directory.	—
preFilterMethodName	The name of the pre-filter method in the script.	**preFilter**
postFilterMethodName	The name of the post-filter method in the script.	**postFilter**
convertMethodName	The name of the convert method in the script.	convert

Note: If you specify method names, conversion script files can be shared by multiple adapters.

Writing the Conversion Scripts

Conversion scripts are responsible for the field mapping that occurs during the conversion of changes and tasks from their service desk application format to a generic format, as well as for the filtering of requests.

Note: Ensure that no line within a script exceeds 256 characters.

In particular, it is important that the conversion scripts contain a detailed mapping scheme for the service desk application enumeration fields. Note that each Change Control Management enumeration field appears by default in the conversion scripts in the following format (upper case letters):

```
<enumeration field type>_<Change Control Management enumeration name>
```

For example:

```
genericRFC.setField("priority",PRIORITY_HIGH);
```

If a script refers to an enumeration field that does not exist, an error message will be recorded in the script log file.

For details on customizing the Change Control Management enumeration fields to which the service desk application enumeration fields can be mapped, see "Customizing Change Control Management Fields" on page 38.

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, located in the **docs/pdfs** directory of the Mercury Change Control Management CD-ROM.

➤ **convert.** This function maps the fields of the service desk application to generic request fields. Below is an example of the **convert** function:

```
convert(remedyRFC, genericRFC)
```

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

➤ **preFilter.** This function filters the changes or tasks before they are converted, ensuring that no unnecessary requests are converted and sent to the Change Control Management 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 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 Change Control Management server. The function is written using Change Control Management request terminology. For example, the following **postFilter** function specifies that only generic requests with the status **Approved** be transferred to the Change Control Management server:

```
function postFilter(genericRFC){
    ccmStatus==genericRFC.get("status");
    if (ccmStatus==STATUS_APPROVED)
        return true;
    else
        return false;
```

Notes:

➤ If you are converting requests from IT Governance Center, IT Governance Center RML, or a database service desk application, refer to all column names using lower case letters.

➤ If you are converting requests from Remedy Action Request System, IT Governance Center RML, or a database service desk application, 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 using the relevant connector property.

➤ You can use logging objects in the conversion scripts to log statements from the request conversion process. For details, see "Conversion Script Log Files" on page 73.

Conversion Script 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 **<Change Control Management installation directory>/script-logs** 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.

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);
```

5

Configuring the Change Control Management Processing of Requests

This chapter describes how to configure the collection of converted change requests, the analysis of collected requests, the calculation of impact analysis for these requests, and the sending of notifications as a result of impact analysis calculations.

Note: An XML schema, **change-flow_settings.xsd**, is available to assist you in the customization of the **change-flow.settings** file. Using an XML editor that supports **.xsd** files to customize the **change-flow.settings** file enables you to minimize the number of customization errors that can be made.

About the Processing of Requests

The processing of converted, generic requests by Change Control Management involves the following four stages:

➤ **Collecting generic requests**

The Change Control Management server collects the converted, generic requests according to the collection frequency you specify. For details on configuring the frequency with which Change Control Management collects converted requests, see "Configuring the Collection of Converted Requests" on page 77.

➤ **Analyzing the collected requests**

To analyze the collected requests, Change Control Management 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 Change Control Management to use, see "Configuring the Analysis of Collected Requests" on page 77.

➤ **Calculating impact analysis for the requests**

Change Control Management 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 "Configuring the Impact Analysis of Collected Requests" on page 79.

➤ **Sending notifications as a result of an impact analysis calculation**

Change Control Management sends notifications as a result of an impact analysis calculation, based on the notification rules that you configure. For details on formatting the notification content and configuring the status and severity thresholds for which Change Control Management sends notifications, see "Configuring Notifications" on page 80.

Configuring the Collection of Converted Requests

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

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

Configuring the Analysis of Collected Requests

To analyze the impact of the collected change requests, Change Control Management must first identify the location and format of the CIs contained in the requests, using specific analysis rules. You specify the analysis rules you want Change Control Management to use in the **<rfc-analysis-rules>** section of the **<Change Control Management installation directory>/conf/change-flow.settings** file.

Each analysis rule contains the following elements:

➤ **name.** The name of the CIT that you want Change Control Management to locate in the collected requests, as well as the logical name of the analysis rule that can be referenced in the field settings (for details, see "Configuring Change Request Field Settings" on page 121). The name of the CIT must appear as it is defined in the **<Change Control Management installation directory>/conf/mam-integration.settings** file.

Note: The **ip-range** analysis rule is an exception to the above specifications, as it corresponds to the **ip** CIT in Mercury Application Mapping.

➤ **pattern.** The format in which the CI appears within the collected requests. Change Control Management searches for the CI according to the pattern you define using regular expressions. 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

You define a pattern using the following two elements:

➤ **match-pattern.** Defines the pattern of the CI, using regular expressions.

➤ **ci-backreferences**. Specifies the exact part of the pattern in which the CI is located, using regular expressions. 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 Change Control Management to use the entire pattern in locating the CI.

Note: An analysis rule can have multiple patterns. For example:

```
<rfc-analysis-rule>
        <name>host</name>
        <patterns>
                <pattern>
                    <match-pattern>([a-zA-Z][\w-]*)([.][a-zA-Z][\w-]*)*</match-pattern>
                    <ci-backreferences>0,1</ci-backreferences>
                </pattern>
                <pattern>
                    <match-pattern>IL-([a-zA-Z][\w-]*)</match-pattern>
                    <ci-backreferences>0</ci-backreferences>
                </pattern>
</rfc-analysis-rule>
```

By default, the **change-flow.settings** file contains analysis rules for the **host** and **ip** CITs. In addition, there are two predefined, built-in analysis rules that can be used when your service desk application is synchronized with the Mercury Application Mapping CMDB server. The **mam-object-id** analysis rule locates CIs using Mercury Application Mapping CI IDs. The **mam-ticket** analysis rule locates CIs using change request IDs.

You apply these analysis rules to change request fields in the Administration module Fields tab. For more information about applying analysis rules, see "Apply analysis rules to the field settings" on page 131.

Configuring the Impact Analysis of Collected Requests

You configure the rules that determine the points at which Change Control Management calculates the impact of the CIs identified in the collected requests in the **<Change Control Management installation directory>/conf/scripts.ext/change-flow.js** script using the **shouldCalcImpact** function.

By default, this script contains the following syntax for the **shouldCalcImpact** function:

```
function shouldCalcImpact (prevChangeInfo, changeInfo)
{
     status= changeInfo.getField("status");
     shouldCalc= (status==STATUS_ASSIGNED ||
status==STATUS_PENDING_APPROVAL || status==STATUS_APPROVED ||
status==STATUS_CLOSED || status==STATUS_IN_PROGRESS);

     shouldCalc= shouldCalc &&
!(changeInfo.isAnalysisRulesEqual(prevChangeInfo));

     return shouldCalc;
}
```

The above function instructs Change Control Management to compare each new request that has a certain status to the version of the request that was previously collected and, if changes were made to fields in which CIs are located, calculate the impact of the request.

For an explanation of the objects that can be included in this function, refer to the **GenericRFC** class in the **API_Reference.chm** file, located in the **docs/pdfs** directory of the Mercury Change Control Management CD-ROM.

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

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

Configuring Notifications

When a change request affects a specific application, users associated with that application, are eligible to receive notification about the change request in the User Notifications pane. You define under what circumstances and to whom notification is sent in the **<Change Control Management installation directory>/conf/scripts.ext/change-flow.js** script using the **getUsersToNotify** function.

In addition, you can configure Change Control Management to send notification by e-mail. You configure e-mail notification properties in the **<notifications>** section of the **<Change Control Management installation directory>/conf/change-flow.settings** file. You configure the format of e-mail notifications in the FTL files located in the **<Change Control Management installation directory>/conf/notifications.ext** directory.

Configuring Notification Properties

In the **<Change Control Management installation directory>/conf/scripts.ext/change-flow.js** script, you use the **getUsersToNotify** function to define:

➤ when notification should be sent.

➤ who receives notifications.

➤ the content of the notification header message.

For an explanation of the objects that can be included in this function, refer to the **notificationContext** and **GenericRFC** class in the **API_Reference.chm** file, located in the **docs/pdfs** directory of the Mercury Change Control Management CD-ROM.

Configuring the Format of E-mail Notifications

You configure the format of the notifications that Change Control Management sends in the **ftl** files, located in the **<Change Control Management installation directory>/conf/ notifications.ext** directory.

➤ **mailSubject.ftl.** Defines the subject line of a notification e-mail. By default, Change Control Management displays **<request-id> – <request summary>** (for example, **Critical – Upgrade database server**) as the subject line of the notification.

➤ **subject.ftl.** Defines the subject line to be displayed for a notification in the Change Control Management application's Notifications pane. By default, Change Control Management displays **<request-id> – <request summary>** (for example, **Critical – Upgrade database server**) as the subject line of the notification.

➤ **mailbody-text.ftl.** Defines the content of a notification sent in text format.

➤ **mailbody-html.ftl.** Defines the content of a notification sent in HTML format.

➤ **user-mailbody-text.ftl.** Defines the content of the e-mail that a user sends by clicking the **Send E-Mail** button from the Change Requests pane.

➤ **user-mailbody-html.ftl.** Defines the content of the e-mail that a user sends in HTML format.

➤ **free-text-only-html.ftl.** Defines the content of the e-mail (in HTML format) that a user sends by clicking the **Send E-Mail** button from the Notifications and Comments tab.

➤ **free-text-only-text.ftl.** Defines the content of the e-mail that a user sends by clicking the **Send E-Mail** button from the Notifications and Comments tab.

By default, the above files make use of the following Change Control Management objects:

Object	Description
notificationRuleSummary	References the **<summary>** element of the relevant notification rule defined in the **change-flow.settings** file.
freeTextBody	The text entered by the user when sending an e-mail from the Change Requests pane of the Change Control Management application.
request	The request object for which the notification is being sent. Using this object, you can reference all of the request fields. For details of the methods that can be used for this object, refer to the **GenericRFC** class in the **API_Reference.chm** file, located in the **docs/pdfs** directory of the Mercury Change Control Management CD-ROM.
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, located in the **docs/pdfs** directory of the Mercury Change Control Management CD-ROM.
affectedViews	Returns a list of the applications that are impacted by a change request.
viewInfo	Returns information about applications that are part of the Change Control Management user's view, in the context of an impact analysis of a specific change request. For details of the methods that can be used for this object, refer to the **ViewInfo** class in the **API_Reference.chm** file, located in the **docs/pdfs** directory of the Mercury Change Control Management CD-ROM.

Notes:

➤ The FTL files are written using FreeMarker syntax. For details on using FreeMarker, refer to http://freemarker.sourceforge.net/docs/index.html.

➤ For a detailed explanation of the objects that can be used in the FTL files, refer to the **API_Reference.chm** file, located in the **docs/pdfs** directory of the Mercury Change Control Management CD-ROM.

➤ The Change Control Management fields that can be used in the FTL files are those that are defined in the **Fields** tab of the **Administration** module. For more information, see "Configuring Change Request Field Settings" on page 121.

Configuring E-mail Notification Properties

You can enable notifications to be sent by e-mail and modify the notification sender and frequency in the **<notifications>** section of the **<Change Control Management installation directory>/conf/change-flow.settings** file.

To enable the Change Control Management notification mechanism:

Change the value of the **<send-notification-email-enabled>** element to **true**.

To modify the notification sender:

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

To modify notification frequency:

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

Configuring Risk Analysis

Change Control Management performs risk analysis on each change request, enabling change managers to compare change requests in terms of the risks involved in their implementation. This section includes the following topics:

➤ "Understanding Risk Analysis" on page 84

➤ "Example of Risk Analysis Calculation" on page 85

➤ "Defining Risk Factors" on page 88

Understanding Risk Analysis

For each change request, Change Control Management 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 0-100 where a higher number indicates 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 requested change being implemented. Potential Damage is calculated as a weighted value between 0-10 where a higher number indicates 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 0-10 where a higher number indicates a higher probability of failure.

Potential Damage and Probability of Failure are calculated based on *risk factors* that are defined by the Change Control Management 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 0-10, and assigns a weight to the factor.

The administrator can also define override rules for the risk calculation. For example, the administrator can define 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 describes a detailed example of the process involved in calculating the risk value for the change requests.

During the configuration process, the Change Control Management 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 Change Control Management.

The data source for the New_technology risk factor originates from 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 1-36.

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

Original data (range)	Factor score
1-12 months	10

Original data (range)	Factor score
12-24 months	5
24-36 months	0

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

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

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

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

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

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

Factor name	Factor score
New_technology	10
QA_approval	4

Factor name	Factor score
Affected_CIs	2
Duration_of_change	0

Change Control Management 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 Change Control Management configuration process.

Total Weight is the sum of all the weights assigned 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 Change Control Management configuration process.

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

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

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

Factor name	Factor score	Weight	Weighted value
New_technology	10	4	2
QA_approval	4	8	1.6
Affected_CIs	2	6	0.6

Factor name	Factor score	Weight	Weighted value
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 following formula, amounts to 21:

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

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

Defining Risk Factors

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

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

Factor weight distribution chart. Display the weight of each factor in the risk calculation.

Factor Definition section. You define the properties of each risk factor in the Factor Definition pane.

Mapping Definition section. You define mapping rules for the selected risk factor that translate the source data into factor values between 0-10.

To modify or create a risk factor.

1 **Select the type of risk factor you want to create.**

Above the Factor table, select either the Potential Damage tab or the Probability of Failure tab.

2 **Select an existing risk factor from the Factor table or create a new risk factor by clicking the Add Factor. button**

3 **Define the risk factor properties in the Factor Definition section**

Define the following properties:

➤ **Name.** The name of the risk factor. This is the name displayed in the Change Analysis module Risk tab.

➤ **Description.** A description of the risk factor.

➤ **Weight.** The relative weight of the risk factor to be used in the risk calculation.

➤ **Source.** You can choose one of the following sources of data:

  ➤ **Field.** A specific change request field whose data originates in the service desk application.

  ➤ **Planned Duration.** The planned duration of the change request (from the planned start to the planned end). This is calculated by CCM.

  ➤ **Number of CCIs.** The number of CIs that will be directly affected as a result of the change request. This is calculated by CCM.

  ➤ **Application Importance.** The overall importance of the application affected by the change. An importance level is assigned to each application in the Administration module Applications tab.

➤ **Field Name.** The name of the change request field (If you selected **Field** as your source)

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

4 Define the mapping definition

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

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

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

6 Save your changes.

Ensure that you are satisfied with all your changes. Before you save your changes, you can undo any changes you made by clicking the **Refresh settings** button.

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

To save your changes and commit these changes to the server, click the **Commit settings** button.

A message opens asking you to confirm that you want to save these changes. Bear in mind that once you save these changes, they cannot be undone. Click **Yes** to save the changes.

7 To recalculate the risk for all the change requests based on your new settings, click the **Recalculate Risk** button. A message opens informing you of the number of change requests for which risk will be recalculated.

Confirm whether you want to continue recalculating the risk.

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

Defining Risk Calculation Overrides

You can override the risk calculation using the **overrideRisk** function in the **Change Control Management installation directory>/conf/scripts.ext/change-flow.js** script.

For an explanation of the objects that can be included in this function, refer to the **API_Reference.chm** file.

Configuring Risk Calculation Properties

By default, risk is calculated for change requests that have the default statuses defined in the **Change Control Management installation directory>/conf/enumerations.settings.**

You can change the definitions for which change requests' risk should be calculated using the **shouldCalcRisk** function in the **Change Control Management installation directory>/conf/scripts.ext/change-flow.js** script.

For an explanation of the objects that can be included in this function, refer to the **API_Reference.chm** file, located in the **docs/pdfs** directory of the Mercury Change Control Management CD-ROM.

Configuring Collisions

Change Control Management automatically identifies change requests involving common key elements, which are scheduled to take place over the same or adjacent time periods.

Change requests are defined as colliding when:

➤ an application or configuration item (CI) is involved in more than one change over the same or adjacent time periods.

➤ the same implementor is responsible for implementing more than one change over the same or adjacent time periods.

Change Control Management measures collisions in terms of their proximity level and the cause of the collision.

You can configure the way in which Change Control Management identifies and calculates collisions. This section includes:

Configuring Collision Calculation Properties

You customize the way in which Change Control Management identifies and calculates collisions in the **collision-calculation** section of the **Change Control Management installation directory>\conf\change-flow.settings** file.
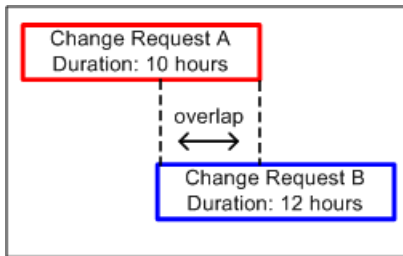
This section explains how to configure the collision calculation properties in the **collision-calculation** section and includes the following sections:

Configuring Collision Proximity Level

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

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

➤ **Overlap Warning.** In reality, planned changes often exceed their original planned duration, which can result in an unforeseen overlap between two change request schedules. In certain cases, if 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 one another when the time gap between the first and second change requests is shorter than 10% of the duration of the first change request.

An example of Overlap Warning between Change Request A and Change Request B is illustrated below, where the gap between the two change requests is 30 minutes, which is less than 10% of the duration of **Change Request A** (10 hours).
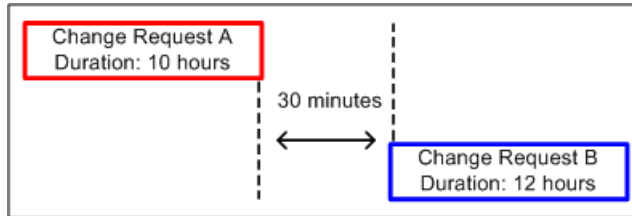
You configure the definition of an **Overlap Warning** in the **warning-ratio** element of the of the **collision calculation** section.

```
<collision-calculation version="2.1.0">
    ...
        <warning-ratio>1.1</warning-ratio>
```

By setting a value for the **warning-ratio** element, you define the time gap according to which Change Control Management determines that two change requests are in close proximity (proximity level of **overlap warning**).

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

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

Configuring Collision Severity Level

If two change requests overlap, there is not necessarily a collision between them. They could be taking place at the same time without having any effect on one another. Change Control Management only defines change requests as colliding if they 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).

Assume for example that a change request involves increasing the memory on Server A. In this case, 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.

➤ **Affected Application.** Two change requests affect at least one common application.

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

Change Control Management determines a collision severity level for each collision based on the cause of the collision and the proximity level of the change requests.

By default, Change Control Management determines the following collision severity levels for each combination of collision cause and proximity level:

	Proximity Level	
Cause	**Overlap**	**Overlap Warning**
CCI-CCI	Critical	Critical
CCI-ACI	High	High
ACI-ACI	(Not defined as a collision)	(Not defined as a collision)

	Proximity Level	
Cause	**Overlap**	**Overlap Warning**
Application	Medium	Medium
Implementor	Medium	Very Low

For example, change requests which share a **CCI** (Changed CI) in common and whose proximity level is defined as **Overlap** would have a **Critical** collision severity level.

Note: If there is more than one cause for a collision, the collision severity level is determined by the cause with the highest severity.

You can change the way in which Change Control Management determines the severity level for any combination of collision cause and proximity level in the **collision-types** element of the of the **collision calculation** section.

```
<collision-calculation version="2.1.0">
    ...
      <collision-types>
          <collision-type>
                  <type-name>CCI_CCI</type-name>
                  <proximity-severity-correlations>
                      <proximity-severity-correlation>
                          <proximity>OVERLAP</proximity>
                          <severity>CRITICAL</severity>
                      </proximity-severity-correlation>
                      <proximity-severity-correlation>
                          <proximity>OVERLAP_WARNING</proximity>
                          <severity>CRITICAL</severity>
                      </proximity-severity-correlation>
                  </proximity-severity-correlations>
          </collision-type>
```

Each combination of collision cause and proximity level is defined in a **collision-type** element that includes the following sub-elements:

➤ **type-name.** The cause of the collision. The following collision causes can be defined:

Cause	Description
CCI_CCI	Two change requests involve at least one common CCI (Changed CI).
CCI_ACI	The same CI is affected by one change and changed by another.
ACI_ACI	Two change requests involve at least one common ACI (Affected CI)
AAP_AAP	Two change requests affect at least one common application.
IMPLEMENTOR	The same implementor is responsible for implementing both change requests.

Note: You can exclude a particular **type-name** from collision calculations by commenting out the **collision-type** element containing that **type-name**. By default, the **collision-type** element containing the **ACI_ACI** type-name is commented out. This means that if two change requests involve a common ACI, Change Control Management will not necessarily define these two change requests as colliding.

➤ **proximity-severity-correlations.** For each collision cause that you defined in the **type-name** element you specify a proximity level and an associated severity level by defining the following sub-elements.

➤ **proximity.** the proximity level of the colliding change requests. This can be defined as either **OVERLAP** or **OVERLAP_WARNING**. For more information about collision proximity levels, see "Configuring Collision Proximity Level" on page 92.

➤ **severity.** The severity level that you want Change Control Management to define for the combination of collision cause and proximity level defined above.

The following example defines that if the cause of the collision was two change requests affecting a common application (AAP_AAP) and the proximity level of the collision was **Overlap**, then the collisions severity level should be defined as **High**.

```
.    <collision-types>
        <collision-type>
                <type-name>AAP_AAP</type-name>
                <proximity-severity-correlations>
                    <proximity-severity-correlation>
                        <proximity>OVERLAP</proximity>
                        <severity>HIGH</severity>
                    </proximity-severity-correlation>
                </proximity-severity-correlations>
        </collision-type>
```

Change Request Statuses Included in Collision Calculation

You define the statuses of the change requests to be included in the collision calculation in the **statuses** element of the **collision calculation** section.

```
<collision-calculation version="2.1.0">
    <statuses>
        <status>ASSIGNED</status>
        <status>PENDING_APPROVAL</status>
        <status>APPROVED</status>
        <status>IN_PROGRESS</status>
        <status>CLOSED</status>
    </statuses>
```

By default, change requests of all statuses are included in the collision calculation. However, you may want to exclude change requests of a certain status from the collision calculation.

For example, if you want to exclude change requests with the status of **closed** from collision calculations, remove the following sub-element:

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

Including Change Requests in Collision Calculations

You define which change requests are included in the collision calculation using the **shouldCalcCollision** function in the **Change Control Management installation directory**>/conf/scripts.ext/change-flow.js script.

The main use of this script is to exclude problematic or irrelevant change requests from the collision calculation. By default, the script excludes any change request with a duration of over eight weeks, as illustrated in the following example:

```
function shouldCalcCollision(prevChangeInfo, changeInfo){
        eightWeeks = 1000*60*60*24*7*8;
     plannedStartTime= changeInfo.getField("planned-start-time");
     plannedEndTime= changeInfo.getField("planned-end-time");
     changeDuration = plannedEndTime - plannedStartTime;
     if (changeDuration > eightWeeks){
         return false;
     }

     return true;
```

For example, a change request may have a particularly long duration because a mistake was made entering the start or finish time. The above script will therefore exclude such change requests from the collision calculation, thereby avoiding misleading results and a lot of unnecessary overhead on the system.

You can use the script to define whatever other criteria should be met in order for a change request to be included in the collision calculation.

For an explanation of the objects that can be included in this function, refer to the **GenericRFC** class in the **API_Reference.chm** file, located in the **docs/pdfs** directory of the Mercury Change Control Management CD-ROM.

Configuring Latent and Detected Changes

Change Control Management contains all the changes that are scheduled to take place in your environment.

If you are working with Mercury Application Mapping 6.5, you can configure Mercury Application Mapping to periodically discover actual changes to your environment and send data about these changes to Change Control Management.

The latent changes feature enables you to determine whether changes discovered in your environment (**discovered changes**) correspond to changes that which were already scheduled in Change Control Management (**scheduled changes**).

This section includes:

➤ "Understanding Latent and Detected Changes" on page 99

➤ "Configuring the Latent Change Feature Properties" on page 103

Understanding Latent and Detected Changes

Important: There are different ways that you can work with the latent changes feature. This section assumes that the latent changes feature is fully activated (**latent-and-detected** mode). For more information about the different work modes, see "Configuring the Latent Change Feature Properties" on page 103

When a change is discovered, Change Control Management tries to match the discovered change with scheduled changes according to the following criteria:

1 Time period. Change Control Management checks whether the discovered change took place during the same time period as a scheduled change.

Regarding the time period of the scheduled change, Change Control Management first checks the actual time of the scheduled change. If there is no actual time recorded, it checks the planned time.

2 Host. If the discovered change took place during the same time period as a scheduled change, Change Control Management checks whether Change CIs (CCIs) in the discovered change and in the scheduled change are linked to a common host.

3 Change type. If the discovered change and a scheduled change share the above criteria (time and host), Change Control Management checks whether the discovered change and the scheduled change are of the same change type. The change type can either be one involving adding hardware or adding software.

The type of the discovered change is determined by Mercury Application Mapping.

The type of the scheduled change is determined by the information in the **change-types-orig** field. This field contains the change type assigned to this change request as defined in the original service desk.

Note: To enable Change Control Management to use the change type criteria, you need to have a field in your service desk application, where you identify the change type of the change request. You then need to map this field to the **change-types-orig** field. For more information about converting and mapping service desk fields, see Chapter 4, "Configuring the Conversion of Service Desk Application-Specific Requests to Generic Requests."

Handling the Discovered Change

According to the extent to which these matching criteria were met, Change Control Management handles the discovered change in one of the following ways:

➤ **Change Control Management displays the change as a detected change.**

When a discovered change matches a scheduled change according to all of the above criteria (time, host and change type), it is defined by Change Control Management as a **detected change**. In the Change Analysis module, detected changes are displayed with the corresponding change request, in the Detected Changes tab.

➤ **Change Control Management 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 Change Control Management as a **latent change**.

Note: The exception to this rule is when the change type is unknown. See the case below ("Change Control Management disregards the change.")


For example, if the discovered change took place during the same period as the scheduled change but they do not share a common host, the discovered change is defined as latent.

In the Change Analysis module, latent changes are displayed as separate changes in the Change Requests pane.

➤ **Change Control Management disregards the change.**

If the discovered change matches the scheduled change according to the first two criteria (time and host) but the scheduled change does not include information regarding its **change type** (meaning that the change type is unknown), Change Control Management will disregard this change and the change will not be displayed.

The following flow chart summarizes the way in which Change Control Management handles the discovered change:
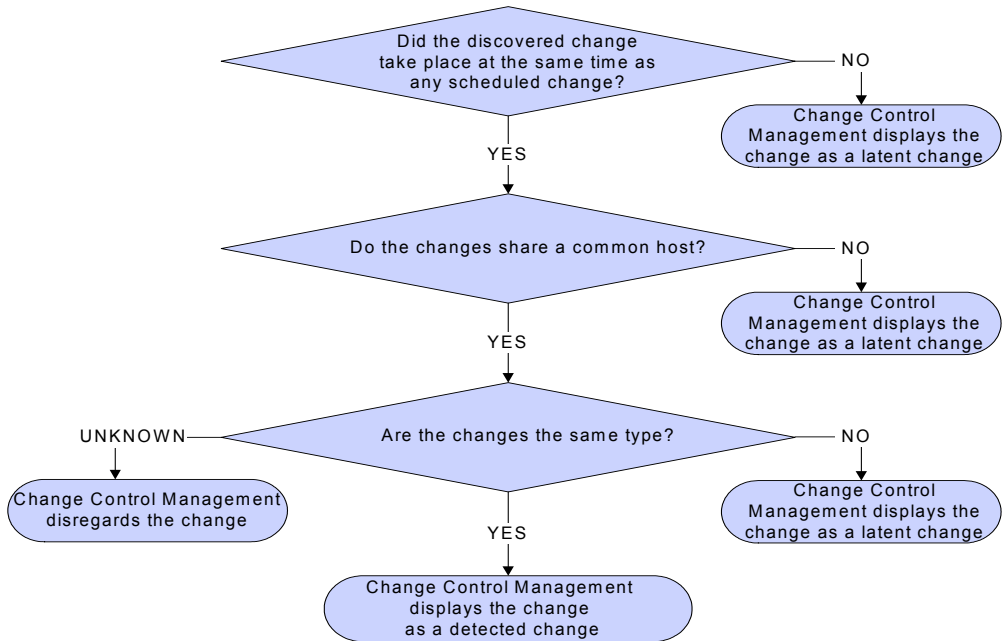
Example

Assume for example that **NewChange** is the name of a discovered change that was detected by Mercury Application Mapping and **CCMrequest1**, **CCMrequest2**, and **CCMrequest3** are all the scheduled changes included in Change Control Management.

Change Control Management 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, Change Control Management checks whether **NewChange** and **CCMrequest2** have changed CIs which share a common host. If they do, Change Control Management 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 Change Control Management cannot identify the change type of **CCMrequest2**, then **NewChange** is disregarded and is not displayed anywhere.

Configuring the Latent Change Feature Properties

You configure the latent changes feature in the **Change Control Management installation directory>/conf/mam-integration.settings** file, in the **latent changes** section.

You can define values for the following elements:

➤ <**latent-changes-mode**>. You choose how to work with the latent changes feature, by defining a value for this element. You can define one of the following values:

Value	Description
disabled	The latent changes feature is inactivated. Change Control Management does not receive information about new changes in your environment. This is the default setting.
latent-and-detected	The latent changes feature is fully activated. Latent and detected changes are displayed according to the criteria described in "Understanding Latent and Detected Changes" on page 99.

Value	Description
latent-consider-change-types	The latent changes feature is partially activated. Detected changes are ignored and latent changes are displayed. Latent changes detected in your environment are displayed according to the criteria described in "Understanding Latent and Detected Changes" on page 99.
latent-ignore-change-types	The latent changes 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 host) but the change types are different, then: ➤ in **latent-ignore-change-types** mode, the change would not be defined as latent. ➤ in **latent-consider-change-types** mode, the change would be defined as latent.

➤ **<detect-changes-schedule>.** Define the schedule for when Change Control Management requests information from Mercury Application Mapping about newly discovered changes. This value is entered as a cron expression.

➤ **<detect-changes-duration-in-hours>.** Define the block of time for which Change Control Management requests information from Mercury Application Mapping about newly discovered changes.

➤ **<detect-changes-recovery-duration-in-hours>.** When the Change Control Management server starts up, it searches for cases where there were problems encountered during the calculation of detected changes, for example, if the server stopped during the calculation process. In this element, you define how far back in time Change Control Management should search for such problem cases. The default setting is one month.

➤ **<latent-change-level>.** Latent changes are displayed as separate changes in the Change Analysis module. Define whether you want latent changes to be displayed as top-level (parent) change requests or second-level (child) requests.

➤ **<latent-change-ref-id>.** Latent changes are displayed as separate changes in the Change Analysis module. Define a format for the Request ID assigned to the latent changes by defining a value for the following sub-elements.

  ➤ **<initial-counter-value>.** The number that will be included in the Request ID for the first latent change recorded in you system.

  ➤ **<format>.** The format of the latent change Request ID.

➤ **<detected-changes-query>.** Define values for the following sub-element:

  ➤ **<name>.**The name of the TQL in Mercury Application Mapping that describes the type of objects in which Mercury Application Mapping should search for changes.

➤ **<host-grouping-query>.** Define values for the following sub-elements:

  ➤ **<name>.** The name of the TQL in Mercury Application Mapping that describes the relationship between the searched objects and their hosts.

  ➤ **<cis-list-object-name>.** The label of the object in the TQL that represents the CCI.

Note: For more information about TQLs, refer to the Mercury Application Mapping documentation.

6

Configuring Mercury Application Mapping-Related Settings

This chapter describes how to configure Mercury Application Mapping connection properties for the Change Control Management user you created within Mercury Application Mapping. It also describes how to configure Mercury Application Mapping, if you are working with version 6.x and how to reconfigure the default Change Control Management–Mercury Application Mapping integration settings, if required.

Note: This chapter uses Mercury Application Mapping 6.x terminology. Objects are therefore referred to as CIs and class types as CITs.

This chapter describes:	On page:
Configuring Mercury Application Mapping Connection Properties for the Change Control Management User	108
Configuring Mercury Application Mapping Settings when Working with Mercury Application Mapping 6.x	110
Configuring Change Control Management–Mercury Application Mapping Integration Settings	111

Configuring Mercury Application Mapping Connection Properties for the Change Control Management User

Mercury Application Mapping is a key component in the processing of Change Control Management requests. To work with Mercury Application Mapping in the context of Change Control Management, you must configure a user within Mercury Application Mapping whose views reflect the IT applications affected by the change requests that Change Control Management will be processing. For details on configuring a user within Mercury Application Mapping, refer to the Mercury Application Mapping documentation.

Once you have created a Change Control Management user within Mercury Application Mapping, you must configure the Mercury Application Mapping connection properties for this user within the **<Change Control Management installation directory>/conf/mam-integration.settings** file. You specify the following properties in the **<mam-connection>** section of this file:

Property	Description
mam-version	The version of Mercury Application Mapping—3.0, 6.1, 6.2, or 6.5—that is being used. **Note:** The value of this property should not be modified.
mam-server	The name of the Mercury Application Mapping server to which the Change Control Management user should connect.
cmdb-server (versions 6.x only)	The name of the Mercury Application Mapping CMDB server to which the Change Control Management user should connect. (The Mercury Application Mapping server and Mercury Application Mapping CMDB server may be installed on separate machines.)
port	The port through which the Change Control Management user should connect to Mercury Application Mapping.

Property	Description
username	The user name required for the Change Control Management user to connect to Mercury Application Mapping.
password	The password required for the Change Control Management user to connect to Mercury Application Mapping. If the password must be encrypted, see Appendix A, "Password Encryption" for details on encrypting passwords.
installation-type (versions 6.x only)	The type of Mercury Application Mapping installation you have. The following installation types exist: ➤ **typical.** Both the Mercury Application Mapping server and CMDB server are located on the same machine. ➤ **distributed.** The Mercury Application Mapping server and CMDB server are located on separate machines. ➤ **shared.** The Mercury Application Mapping CMDB server is shared with Business Availability Center.
view-refresh-schedule (versions 6.x only)	The time at which Change Control Management accesses Mercury Application Mapping to refresh the Change Control Management user's views. It is recommended that a refresh be performed once a day, after Mercury Application Mapping discovery has been completed, when a minimal number of users are connected to Mercury Application Mapping. By default, a view refresh takes place at 4 A.M. **Note:** You define the **view-refresh-schedule** using cron expressions.

Configuring Mercury Application Mapping Settings when Working with Mercury Application Mapping 6.x

When working with Mercury Application Mapping 6.x, you must configure connections between hosts (or other CITs) and business services within the Mercury Application Mapping views that pertain to the Change Control Management user. If a CIT is directly linked to a business service, the CIT will be displayed in Change Control Management only under the application with which its business service is directly associated. If a CIT is not linked to a business service, the CIT will be displayed in Change Control Management under each application with which the business services of its parent CITs (the CITs with which it is associated in Change Control Management) are directly associated.

To configure settings for Mercury Application Mapping 6.x:

1 Copy the **<Change Control Management installation directory>/ MAM/<version number>/extension/ccm_package.zip** package to:

➤ the **<Mercury Application Mapping server>/root/lib/packages** directory, if you are working with a typical or distributed Mercury Application Mapping installation. Mercury Application Mapping then automatically loads the package.

➤ the **<Business Availability Center Data Processing Modeling Server>/ mam_lib/packages** directory, if you are working with a shared Mercury Application Mapping installation. Instruct Mercury Application Mapping to load the new package by opening the Business Availability Center Data Processing Modeling Server console (**http://<Business Availability Center server>:8080/jmx-console/**), selecting **MAM > Service=Package manager > deployPackages**, specifying 1 under **customerId** and ccm_package.zip under **packagesNames**, and clicking the **Invoke** button.

2 Increase the maximum number of business service links that can be created by changing the value of **appilog.map.BusinessService.MaxLinksInView** in the **appilogConfig.properties** file to **5000**. For details on the location of this file, refer to the Mercury Application Mapping documentation.

3 Open the Mercury Application Mapping Service View Manager. Within each view definition, locate the hosts or other CITs that you want to link to a business service. Right-click each host or CIT and select **Add to Business Service**. For more information on linking CITs to business services, refer to the Mercury Application Mapping documentation.

Note: If you linked CITs other than hosts to a business service, you must add these CITs to the **appilog.map.BusinessService.Classes** section of both the **appilogConfig.properties** file and the **<MAM installation directory>\root\lib\web\gui.properties** file. Use commas to separate the CITs you add. For details on the location of the **appilogConfig.properties** file, refer to the Mercury Application Mapping documentation.

---

4 Update your Mercury Application Mapping settings by opening the Business Availability Center Data Processing Modeling Server console, selecting **MAM** > **Service=View System** > **reloadServerConfiguration**, and clicking the **Invoke** button. Refer to the Mercury Application Mapping documentation for instructions on accessing the console.

Configuring Change Control Management–Mercury Application Mapping Integration Settings

In addition to the Change Control Management user Mercury Application Mapping connection properties, the **<Change Control Management installation directory>/conf/mam-integration.settings** file contains the following preconfigured settings:

➤ the frequency of Change Control Management and Mercury Application Mapping CMDB synchronization

➤ the Mercury Application Mapping CMDB initialization delay (Mercury Application Mapping 3.0 only)

➤ the Mercury Application Mapping correlation rules that you want Change Control Management to use in performing an impact analysis (Mercury Application Mapping 6.2 or later)

➤ a list of Mercury Application Mapping CITs and attributes according to which you want Change Control Management to locate changed CIs in order to perform an impact analysis on them

➤ Change Control Management–Mercury Application Mapping impact severity mappings

➤ a list of preconfigured CITs and their attributes that can be included in the results of an impact analysis

If required, the above settings can be reconfigured to more accurately reflect your IT system.

Configuring Synchronization Frequency

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

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

Configuring Initialization Delay

When working with Mercury Application Mapping 3.0, Change Control Management waits 1200 seconds, by default, for Mercury Application Mapping views to be loaded before impact analysis calculations are begun. To lengthen or shorten the Mercury Application Mapping initialization delay, modify the value in the following line of the **mam-integration.settings** file's **<cmdb-synchronizations>** section:

```
<cmdb-init-views-delay>1200</cmdb-init-views-delay>
```

Configuring Correlation Rules

When working with Mercury Application Mapping 6.2 or later, Change Control Management performs an impact analysis, by default, using only correlation rules with the prefix **ccm**. If you want Change Control Management to use additional or alternative correlation rules, you must define these rules in the **<patterns>** element of the **mam-integration.settings** file's <correlation-rules> section, using regular expressions.

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

```
<patterns>        operations.*
                  database.*
</patterns>
```

Each expression you use should appear on a separate line. 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.

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

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

Configuring CI Search Directives

By default, Change Control Management searches for changed CIs that belong to either the **host** or **ip** CIT and whose format matches one of the Mercury Application Mapping attributes listed in the **<cmdb-lookup-attributes>** section of the **mam-integration.settings** file. An impact analysis is then performed on the located CIs.

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

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

Notes:

➤ Use only key attributes by which the CIT is defined.

➤ The "first found" matching attribute is used in locating CIs.

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

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

Mapping Change Control Management–Mercury Application Mapping Severity Levels

By default, Change Control Management uses the following scheme in mapping Change Control Management impact severity levels to Mercury Application Mapping severity levels:

➤ a value of **Very Low** in Change Control Management = **2 or below** in Mercury Application Mapping

➤ a value of **Low** in Change Control Management = **3 or 4** in Mercury Application Mapping

➤ a value of **Medium** in Change Control Management = **5 or 6** in Mercury Application Mapping

➤ a value of **High** in Change Control Management = **7 or 8** in Mercury Application Mapping

➤ a value of **Critical** in Change Control Management = **9** in Mercury Application Mapping

To modify this mapping scheme, change the maximum Mercury Application Mapping impact severity values you want to map to each Change Control Management severity level. For example, if you want to map the Mercury Application Mapping impact severity value of **8** to the Change Control Management severity level **Critical**, you would change the following lines in the **<enum-mappings>** section of the **mam-integration.settings** file:

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

to:

```
<entry-name>High</entry-name>
<high-value>7</high-value>
```

Note: The default mapping scheme should be modified only if the Change Control Management impact severity levels or Mercury Application Mapping severity levels have changed.

Configuring CITs and Attributes for Impact Analysis Results

The **<ci-classes-attributes>** section of the **mam-integration.settings** file contains a list of CITs and attributes belonging to each CIT. This list indicates which CITs and attributes are to be included in the results of an impact analysis. These are also the CITs and attributes that will be displayed in the Change Control Management application for each changed or affected CI.

For example, the following attributes will be included in the impact analysis results of a **host** CIT and are displayed for a changed or affected host machine, which belongs to the **host** CIT:

REGARD - (host)

DNS Name:	regard.mercury.com
Host Name:	REGARD
Host OS:	Windows 2000
SNMP Name:	REGARD
Vendor:	Intel

This display is based on the following definition in the **<ci-classes-attributes>** section of the **mam-integration.settings** file:

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

Note: The Change Control Management application also displays the attributes of the CIT based on the Mercury Application Mapping CIT hierarchy. For example, if the displayed CIT is a router, the attributes of the router's host are also displayed.

If you are working with Mercury Application Mapping 3.0 and have configured CITs for which a lot of CIs will be collected, it is recommended that you improve Change Control Management's performance by choosing to view these CIs under the applications with which the parent CIs are associated. To do so, add the following line to the relevant CITs in the **<ci-classes-attributes>** section of the **mam-integration.settings** file:

```
<view-resolution-method>inherit-from-parent</view-resolution-method>
```

For example, to view a CI that is a disk under the applications with which its relevant host is associated, you would specify the following in the **mam-integration.settings** file:

```
<ci-class-attributes>
    <class-type>disk</class-type>
    <attributes>
        <attribute-name>data_name</attribute-name>
    </attributes>
    <view-resolution-method>inherit-from-parent</view-resolution-method>
</ci-class-attributes>
```

This instructs Change Control Management to display the disk CI under the application with which its host is associated, even though the disk itself is not associated with this application.

7

Configuring the Change Control Management Application

This chapter describes how to configure various elements of the Change Control Management application.

This chapter describes:	On page:
Configuring User Name and Password Constraints	120
Configuring Change Request Field Settings	121
Configuring Dashboard Settings	139
Configuring Enumeration Field Display Settings	141

Configuring User Name and Password Constraints

You can configure the following Change Control Management application user name and password constraints and properties in the **<Change Control Management installation directory>/conf/application.settings** file:

➤ **minimum length.** Specify the minimum number of characters the user name/password can contain. By default, a user name/password must contain at least one character.

➤ **maximum length.** Specify the maximum number of characters the user name/password can contain. By default, the a user name/password can contain no more than 50 characters.

➤ **pattern.** Using regular expressions, specify the characters that each user name/password can contain. For example, use the following expression to indicate that a user name/password can be any upper-case or lower-case letter, as well as any digit: ^[A-Z,a-z,0-9]$

➤ **pattern error message.** Specify the type of error message to be displayed if the user name/password contains a character that is not allowed. You can enter the error text itself here, or **properties-file** if you want to reference a properties file for the error message. If you reference a properties file, the error message text itself should be written in the following file: **onyxCommonResources.properties**

Configuring Change Request Field Settings

This section describes how to configure change request fields for which you want to view data in the Change Control Management application.

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

This section includes the following topics:

➤ "Understanding the Fields Tab" on page 122

➤ "Creating or Modifying Change Request Fields" on page 123

➤ "Deleting a Change Request Field" on page 135

➤ "Customizing the Grid View" on page 137

➤ "Customizing the Request Details Tab" on page 137

Understanding the Fields Tab

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

Field tree

View pane

Definition and Layout pane
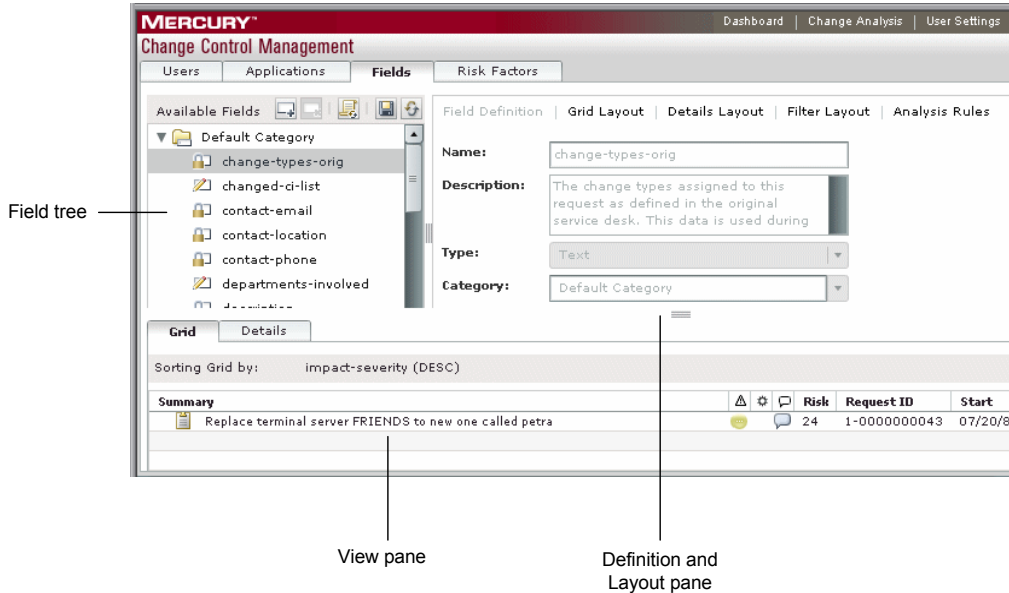
The Fields tab is divided into the following 3 sections:

➤ **Field tree**. Contains a list of all the change request fields. A field selected in the Field tree can be modified in the Definition and Layout pane. For filtering purposes, fields are organized into four default categories (**Default Category**, **General**, **Analysis Information**, and **Time**). Fields defined as filterable will appear in the filter, under the category that is defined here in the Field tree. New categories can be created as part of creating a new field.

➤ **Definition and Layout pane.** You define or modify the properties of the selected change request field in the Definition and Layout pane. This pane is divided into four tabs (**Field Definition**, **Grid Layout**, **Details Layout**, **Filter Layout**, and **Analysis Rules**). In each tab, you configure a different aspect of the field.

➤ **View pane.** In the View pane, you can see a preview of the selected field as it will appear in the Change Analysis module Grid view and Request Details tab. You can also customize the general layout of the Grid view and the Request Details tab as they appear in the Change Analysis module.

Creating or Modifying Change Request Fields

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

To change or modify change request fields:

1 **In the Fields tab of the Administration module, select an existing field from the Field tree or click the Add Field button to create a new field.**

There are two types of change request fields that appear in the Field tree:

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

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

2 **Define or modify the basic properties of the field in the Field Definition tab.**

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

You can define the following properties in the **Field Definition** tab:

Property	Description
Name	In the **Name** box, type the name of the field. This is the name used to define the field for various configuration purposes and is not the name that appears in the UI (user interface).
	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.
	Note that when you define a customized field (except for fields of type **Long Text**), a new column is added to the Change Control Management database for this field. Data for **Long Text** fields is stored in a different table.
	Note: Once a new field has been saved, the name cannot be modified.
Description	In the **Description** box, type a short description of the field to remind administrators about the usage of this field. This description does not appear anywhere in the UI (user interface).
Type	From the **Type** list, select the field's value type. The following types can be used:
	➤ **Short Text.** The request field's value is a simple text string up to 64 characters.
	➤ **Long Text.** The request field's value is a simple text string with an unlimited number of characters. Note that fields of this type cannot be displayed in Grid 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. Note that you cannot filter according to fields of this type.
	➤ **Numeric.** The request field's value is a numeric string.

Property	Description
Category	In the **Category** box, type or select 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 to the Field tree.
	Since the filter categories and the fields they include are predefined and non-configurable, you cannot include a customized field in an existing filter category (**General**, **Applications**, **Time Conditions**). Instead, you must either select the **Default Category** or create a new filter category for the customized field.
Sample Value	To see a preview of the field in either Grid view or the Request details tab, type a sample value in the **Sample Value** box. You will only see a preview if you configure the field to be displayed in either Grid view or the Request details tab.
Sortable	Select **Sortable** to be able to sort according to the selected field in the Change Control Management application.
	Only fields that are displayable in the grid can be made sortable. If a field cannot be displayed in the grid, the **sortable** option is disabled.
Filterable	Select **Filterable** to enable the field to be used as one of the filter criteria. In the **Filter Layout** tab, you define how the field should appear in the Filter Definition pane.
Gridable (not editable)	The check box indicates whether the selected field is of a type that can be displayed in the grid. This check box is not editable

3 Define how the field will appear in the Change Analysis module Grid view.

If the field is defined as **Gridable** in the **Field Definition** tab, you can customize how the field will appear in Grid view. You define these properties in the **Grid Layout** tab.

Property	Description
Header	In the **Header** box, type the text to appear in the header of the column in which the change request field value is to be displayed.
Header Tooltip	In the **Header Tooltip** box, type the text of the tooltip that will appear when you hold your mouse on the column header. **Note:** If this element is left unspecified, the name of the header is displayed as the tooltip.
Value Type	From the **Value Type** list, select the type of value that will be displayed in the grid for the selected field. The following value 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 Format** box.
Value Format	In the **Value Format** box, you specify the format in which the field will appear. For information about valid formats for each value type, see "Valid Field Value Formats" on page 134. **Note:** You cannot define a value format for Boolean value types.

Property	Description
Value Tooltip Type	From the **Value Tooltip Type** list, select the type of value that will be displayed in the tooltip describing the selected field. The following value 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 same information in a different format to the way it appears in the grid. You customize the way the value appears in the **Value Tooltip Format** box, described below.
Value Tooltip Format	In the **Value Tooltip Format** box, specify the text and format of the tooltip that will appear when you hold your mouse on the field value. For information about valid formats for each value type, see "Valid Field Value Formats" on page 134.
Resizable	Select **Resizable** to make the column width resizable. For more information about resizing columns, see "Customizing the Grid View" on page 137.
Show in Grid	Select **Show in Grid** to display the field in the Change Analysis module Grid view.

Note: If you selected **Show in Grid**, the View pane displays a preview of how the field will appear in Grid view. To see how a sample value is displayed, type a sample value in the **Sample Value** box, in the **Field Definition** tab.

 4 Define how the field will appear in the Change Analysis module Request Details tab.

You can define whether this field will be included in the Request Details tab and how it will appear. You define these properties in the **Details Layout** tab.

Property	Description
Label	In the **Label** box, type the text to appear as the label preceding the displayed field value in the Request Details tab.
Value Type	From the **Value Type** list, select the type of value that will be displayed in the grid for the selected field. The following value types are available: ➤ **Short Text.** The value is displayed adjacent to the label, as simple text. ➤ **Long Text.** The value is displayed underneath the label, as simple text. Where necessary, the text will wrap. ➤ **Boolean.** The value is displayed as a check box (supports true/false, yes/no, and 1/0). ➤ **Date.** The value is displayed as a date. ➤ **Link.** Displays the name of another field, which contains a URL. Clicking on that field name takes you to the destination specified in the URL. You customize the way the value appears in the **Value Format** box, described below
Value Format	In the **Value Format** box, you specify the format in which the field will appear. For information about valid formats for each value type, see "Valid Field Value Formats" on page 134. **Note:** You cannot define a value format for Boolean or Long Text value types.
Tooltip	In the **Tooltip** box, type the text of the tooltip that will appear when you hold your mouse on the label.
Show in Details	Select **Show in Details** to display the field in the Change Analysis module Request Details tab.

Note: If you selected **Show in Details**, the View pane displays a preview of how the field will appear in the Request Details tab. To see how a sample value is displayed, type a sample value in the **Sample Value** box, in the **Field Definition** tab.

---

 5 **Define how the field will appear in the Filter Definition pane.**

If you defined the field as **Filterable** in the **Field Definition** tab, you can customize how the field will appear in the Filter Definition pane. You define these properties in the **Filter Layout** tab.

Property	Description
Label	In the **Label** box, type the text to appear as the label preceding the displayed field value in the Filter Definition pane.
Tooltip	In the **Tooltip** box, type the text of the tooltip that will appear when you hold your mouse on the label.

Property	Description
Type	From the **Type** list, select one of the following ways in which the selected field will operate as a filter:
	Note: The options that are available in the **Type** list depend on the field type you defined earlier in the Field Definition tab.
	➤ **Numeric.** Users can filter by specific numbers.
	➤ **Numeric Range.** Users can filter by numeric range. If you select this option, you need to specify the range in the relevant boxes below the **Type** list.
	➤ **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 **Type** list. These are the labels that will appear in the Filter Definition pane.
	➤ **Short Text.** Users enter a string that matches the filter value. An asterisk (*) can be used to match a string to several possible values. (For example, if you use the string Da*, both David and Danny will match.)
	➤ **Selection.** Users can select only one filter value option from a drop-down list box.
	➤ **Multi Selection.** Users can select multiple filter value options from a drop-down group box.
	If you select **Selection** or **Multi Selection** from the **Type** list, a table is displayed below the **Type** list, enabling you to add the filter value options.
	To add a new filter value option:
	1 Click the **Add Filter Value** button.
	2 In the boxes below the table, enter the value of the option in the **Value** column and the way the value will be displayed in the **Display** column.
	3 Click the **Update Value** button to update the new value.
	4 To change the order of appearance of the filter values as they will appear in the Filter Definition pane, select the relevant filter value and click the **Move Up** or **Move Down** buttons.
	To delete an option:
	Select the option and click the **Delete Filter Value** button.

Property	Description
Show in Filter	Select **Show in Filter** to include this field as one of the filter criteria in the Filter Definitions pane.

6 Apply analysis rules to the field settings

Note: This step only applies to change request fields of type **Short Text** or **Long Text**. For other types of change requests continue with 7 on page 133.

To analyze various aspects of the collected change requests, Change Control Management must first identify the location and format of the CIs contained in the requests.

For change request fields containing text, Change Control Management uses **analysis rules** to identify the location and format of the CIs contained in the text. You specify these analysis rules in **change-flow.settings** file. (For more information, see "Configuring the Analysis of Collected Requests" on page 77). You apply these analysis rules to change request fields in the **Analysis Rules** tab.

The Analysis Rules tab contains all the analysis rules specified in the **change-flow.settings** file. When you add a rule to the **change-flow.settings** file it appears as the last rule in the Analysis Rules tab.

For relevant change request fields, you can apply specific analysis rules and choose the level —for example, change or task—at which to apply the specified rules.

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

Rule	Description
everything	Applies all existing analysis rules listed in the **change-flow.settings** file to the change request field except for **mam-ticket** or **mam-object-id**.
host	Identifies hosts
ip	Identifies IP addresses
ip range	Defines a range of IP addresses
mam-object-id	Predefined, built-in analysis rule that can only be used when your service desk application is synchronized with the Mercury Application Mapping CMDB server. This rule locates CIs using Mercury Application Mapping CI IDs.
mam-ticket	Predefined, built-in analysis rule that can only be used when your service desk application is synchronized with the Mercury Application Mapping CMDB server. This rule locates CIs using change request IDs.

For each analysis rule that you selected, select the level at which to apply the rule. You do this by selecting one of the following levels from the list box in the **Level** column:

Level	Description
All	The analysis rule applies to all requests in which this field appears.
Change	The analysis rule applies to this field only when the field belongs to a top-level request (change).
Task	The analysis rule applies to this field only if it belongs to a second-level request (task).

Note: The levels **Change** and **Task** refer to top-level and second-level change requests, respectively. The names of these levels are configurable in the **enumeration-labels.properties file**. For more information see "Configuring Enumeration Field Display Settings" on page 141.

By default, the following change requests fields have the analysis rule set to **everything** and the level set to **All**: **summary**, **description**, **changed-ci-list**, and **work_log**. You can modify these settings.

 7 **Save your changes to the Field settings.**

Ensure that you are satisfied with all your changes. Before you save your field settings, you can undo any changes you made by clicking the **Refresh and Undo Changes** button in the Field tree. This restores the fields to their most recent saved settings.

To save your changes and commit these changes to the server, click the **Commit changes for all fields** button in the Field tree.

A message opens asking you to confirm that you want to save these changes. Bear in mind that once you save these changes, they cannot be undone. Click **Yes** to save the changes.

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

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

Valid Field Value Formats

In the Fields tab, there are a number of places where you need to define the format in which a specific field appears. According to the value type of your field, a different value format applies. The following table describes valid formats for each value type:

Value Type	Value Format
Short Text	If you selected **Short Text** as your value type, you can include parameters that contain the names of defined fields, surrounded by two percentage signs on each side of the field.
	For example, if you defined your value format as **Please contact %%contact-person%%** , the parameter **%%contact-person%%** would return the name of the contact person for the request.

Value Type	Value Format
Date	If you selected **Date** as your value type, you can specify the way in which the date should be displayed by making use of letter patterns containing the following letters: ➤ **Y.** Year ➤ **M.** Month ➤ **D.** Day in the month ➤ **E.** Day of the week ➤ **A.** AM/PM indicator ➤ **J.** Hour of the day (0-23) ➤ **H.** Hour of the day (1-24) ➤ **K.** Hour in the AM/PM (0-11) ➤ **L.** Hour in the AM/PM (1-12) ➤ **N.** Minute in the hour ➤ **S.** Second in the minute For example, to display **Sat 04 Mar 2006 09:43AM**, you would use the following date format: EEE DD MMM YYYY LL:NNA
Link	If you selected **Link** as your value type, you need to specify the name of a field that contains a URL. You enter the field as a parameter that contains the name of the field, surrounded by two percentage signs on each side of the field (**%%field_name%%**). The value displayed for this format is the value of the current field (not the field that contains the URL) and the tooltip of this value is the URL. Clicking on the field leads you to the URL destination.

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

Deleting a Change Request Field

You can delete a change request field in the **Administration** Module **Fields** tab.

You can delete Custom fields which are provided by default or manually added by the user.

Predefined fields that are integral to the proper functioning of the Change Control Management application, cannot be deleted.

Important! When you delete a change request field, all data related to that field is removed.

To delete a change request field:

1 In the **Administration** Module **Fields** tab, select the field that you want to delete from the Field tree.

2 Click the **Delete Field** button in the Field tree.

3 A message opens asking you to confirm that you want to delete this change request field. Click **Yes** to confirm.

Note: The field is only deleted once you save your field setting changes. Before you save your field settings, you can still undo the delete action by clicking the **Refresh and Undo Changes** button in the Field tree. This restores the fields to their most recent saved settings.

---

4 To save your changes and commit these changes to the server, click the **Commit changes for all fields** button in the Field tree.

A message opens asking you to confirm that you want to save these changes. Bear in mind that once you save these changes, they cannot be undone. Click **Yes** to save the changes.

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

Customizing the Grid View

In the Administration module **Fields** tab, you can customize the layout of the Change Analysis module Grid view.

To customize the Grid view:

1 In the Administration module Fields tab, in the View pane, select the Grid tab.

In the Grid tab, a preview of the Change Analysis module Grid view is displayed. The fields, for which you selected **Show in Grid** in the **Grid Layout** tab, are displayed in the Grid tab.

2 Adjust the width of the columns.

You can only adjust the width of the column if you selected **Resizable** for the selected column in the **Grid Layout** tab.

To adjust the column width, rest the pointer on the column boundary you want to move until it becomes a resize pointer, and then drag the boundary until the column is the width you want.

3 Change 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** buttons.

4 Select the column by which the grid should be sorted by default.

You can only select a column to sort by, if you selected **Sortable** for the selected column in the **Grid Layout** tab.

➤ To sort the grid by a selected column, select the relevant column heading.

➤ Once the column heading is selected, click it again to sort the grid according to this column. An arrow is displayed next to the column header to indicate that the grid is sorted by this column.

➤ To change the sorting order, click the column heading again. The arrow points in the opposite direction.

Customizing the Request Details Tab

In the Administration module **Fields** tab, you can customize the layout of the Change Analysis module Request Details tab.

To customize the Request Details tab:

1 **In the Administration module Fields tab, in the View pane, select the Details tab.**

In the Details tab, a preview of the Change Analysis module Request Details tab is displayed. The fields, for which you selected **Show in Details** in the **Details Layout** tab, are displayed in the Details tab.

2 **Add or remove columns.**

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

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

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

To move the field to a different column, select the relevant field and click the **Move Right** or **Move Left** buttons. You can also move an entire column to the left or to the right by selecting a whole column and using the **Move Right** or **Move Left** buttons.

To change the order of appearance of the fields within each column, select the relevant field and click the **Move Up** or **Move Down** buttons.

Configuring Dashboard Settings

The **<Change Control Management installation directory>/conf/ dashboard.settings** file maps the two types of roles in Change Control Management—**user** and **administrator**—to the **users** and **administrators** Dashboard groups, respectively, and defines the privileges granted to each group. This file also contains other definitions related to the display of Dashboard pages and portlets.

Note: The definitions in this file should not be modified.

The **<Change Control Management installation directory>/conf/ Dashboard_Objects_Export.xml** file contains definitions for the Change Control Management Default Page in the Dashboard. If you changed the **Pending Approval** or **Closed** status in the **<Change Control Management installation directory>/conf/enumerations.settings** file, you must update the **Dashboard_Objects_Export.xml** file with the alternative status or statuses that you are using.

To update the Closed status:

1 Locate the following line within the **Dashboard_Objects_Export.xml** file:

```
[CLOSED][Closed]
```

Note that there are two occurrences of this line in the file.

2 Replace **[CLOSED]** with the alternative status defined in the **<Change Control Management installation directory>/conf/enumerations.settings** file. For details on configuring the **enumerations.settings** file, see "Customizing Change Control Management Fields" on page 38.

3 Replace **[Closed]** with the label you assigned to the above status in the **<Change Control Management installation directory>/conf/ enumeration-labels.properties** file. For details on configuring the **enumeration-labels.properties** file, see "Configuring Enumeration Field Display Settings" on page 141.

To update the Pending Approval status:

1 Locate the following line within the **Dashboard_Objects_Export.xml** file:

```
[PENDING_APPROVAL][Pending_Approval]
```

Note that there are four occurrences of this line in the file.

2 Replace **[PENDING_APPROVAL]** with the alternative status defined in the **<Change Control Management installation directory>/conf/ enumerations.settings** file. For details on configuring the **enumerations.settings** file, see "Customizing Change Control Management Fields" on page 38.

3 Replace **[Pending_Approval]** with the label you assigned to the above status in the **<Change Control Management installation directory>/conf/ enumeration-labels.properties** file. For details on configuring the **enumeration-labels.properties** file, see "Configuring Enumeration Field Display Settings" on page 141.

After you have updated the **Dashboard_Objects_Export.xml** file with the alternative status or statuses that you are using, you must run the **populate_dashboard.bat** command from the **<Change Control Management installation directory>/tomcat/webapps/ccm** command line directory. Note that when you run this command, any previous Dashboard data that you configured is automatically deleted.

Configuring Enumeration Field Display Settings

The displayed severity, priority, status, estimated risk, and request levels that correspond to the configured enumeration fields are defined in the **<Change Control Management installation directory>/conf/enumeration-labels.properties** file. This file also includes a list of available icons and the severity levels to which they correspond.

You can modify the way in which the Change Control Management application displays each of the enumeration fields listed. For example, you may want to display the status **Closed** as **Completed**. To do so, you would change the line:

```
StatusEnum.CLOSED=Closed
```

to:

```
StatusEnum.CLOSED=Completed
```

You can also modify the icon color that corresponds to each severity level. For example, to display a red icon rather than an orange icon for a severity level of **High**, you would change the line:

```
SeverityEnum.High.color=orange
```

to:

```
SeverityEnum.High.color=red
```

Note: You cannot modify the color icons themselves; red, orange, yellow, green_yellow, green, and gray are the only colors available.

By default, top-level or parent change requests are referred to as **changes** and second-level or child change requests are referred to as **tasks** in the Change Control Management application. Other request hierarchy levels are referred to as **unknown**. You can modify this terminology by changing the following lines in the **enumeration-labels.properties** file:

```
LevelEnum.1=Change
LevelEnum.2=Task
LevelEnum.Level.UNKNOWN=Unknown
```

8

Configuring the Change Control Management System Preferences

To work with Change Control Management, you must create a database or user schema, configure the connection properties for the Change Control Management database or user schema, and configure the SMTP mail server responsible for sending Change Control Management e-mail notifications. In addition, you can reconfigure the Change Control Management application server address and predefined Change Control Management log file properties, if required.

Configuring the Change Control Management Database or User Schema

To work with Change Control Management, you must create either a Microsoft SQL Server database or an Oracle Server user schema (see "System Requirements" on page 10 for MS SQL Server and Oracle Server system requirements). You then configure connection properties for the Change Control Management database or user schema.

Note: For information and guidelines about configuring and maintaining MS SQL and Oracle Server databases, see Appendix E, "Configuring and Maintaining Mercury Change Control Management Databases."

Microsoft SQL Server

After you have created an MS SQL Server database, copy the contents of the **<Change Control Management installation directory>/examples/database-config-examples/database.properties.mssql** file to the **<Change Control Management installation directory>/conf/database.properties** file and configure the following properties:

➤ **server name.** Specify the name of the MS SQL Server.

➤ **database name.** Specify the name of the MS SQL Server database.

➤ **password.** Specify the password required to connect to the MS SQL Server database. If the password must be encrypted, see Appendix A, "Password Encryption" for details on encrypting passwords.

➤ **user name.** Specify the user name required to connect to the MS SQL Server database.

Oracle Server

After you have created an Oracle Server user schema, copy the contents of the **<Change Control Management installation directory>/examples/ database-config-examples/database.properties.oracle** file to the **<Change Control Management installation directory>/conf/database.properties** file and configure the following properties:

➤ **server name.** Specify the name of the Oracle Server.

➤ **service name.** Specify the service name for the Oracle Server user schema.

➤ **password.** Specify the password required to connect to the Oracle Server user schema. If the password must be encrypted, see Appendix A, "Password Encryption" for details on encrypting passwords.

➤ **user name.** Specify the user name required to connect to the Oracle Server user schema.

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, Change Control Management does not log MS SQL or Oracle Server database statements. To modify this default setting, change the following line in the **database.properties** file:

```
hibernate.show_sql=false
```

to:

```
hibernate.show_sql=true
```

Note: No other settings in the **database.properties** file should be modified.

Configuring the SMTP Mail Server

To work with Change Control Management, you must configure connection properties for the SMTP mail server responsible for sending Change Control Management e-mail notifications. The following are the properties you must configure in the **<Change Control Management installation directory>/ conf/integrations.settings** file:

➤ **user name.** Specify the user name required to connect to the SMTP mail server, if one is required.

➤ **password.** Specify the password required to connect to the SMTP mail server, if one is required. If the password must be encrypted, see Appendix A, "Password Encryption" for details on encrypting passwords.

➤ **SMTP host.** Specify the host name of the SMTP mail server machine.

➤ **SMTP port.** Specify the port to be used to connect to the SMTP mail server.

Configuring the Change Control Management Server

The Change Control Management application server name and address are configured automatically during the Change Control Management installation process. Change Control Management uses these settings to create links to requests in the Change Control Management application from e-mail notifications.

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

For example, change:

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

to:

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

Configuring Log File Properties

The **<Change Control Management installation directory>/conf/ ccmlog4j.properties** file contains a list of log file definitions, some of which you may want to modify.

Modifying the Types of Messages Displayed

The following three types of log message commands can be used:

➤ **WARN.** Warning and error messages are displayed.

➤ **INFO.** Info messages that record the processing activity that the system performs are displayed, in addition to warning and error messages.

➤ **DEBUG.** All types of log messages are displayed.

The Change Control Management log files are located in the **<Change Control Management installation directory>/logs** directory. For a description of each of the log files contained in this directory, see Appendix D, "Using CCM Logs."

The Tomcat server log files are located in the **<Change Control Management installation directory>/tomcat/logs/stdout.log** file.

Modifying File Size and Backup Policy

By default, the maximum size of a log file is set to 4000 KB. To change this setting for all log files, modify the following line at the top of the **ccmlog4j.properties** file:

```
def.file.max.size=4000KB
```

By default, there are 10 backup log files at any given time. To change this setting for all log files, modify the following line at the top of the **ccmlog4j.properties** file:

```
def.files.backup.count=10
```

Modifying Time Zones

By default, log messages are recorded using the GMT time zone. To use a different time zone, specify the required zone in the following line at the bottom of the **ccmlog4j.properties** file:

```
ConversionPattern=%d{ISO8601} [%t] %-5.5p %C{1} -  %m%n
```

For example, if you want to use Eastern Standard Time, you would specify the following:

```
ConversionPattern=%d{ISO8601@EST} [%t] %-5.5p %C{1} -  %m%n
```

For a list of GMT time zones for locations throughout the world, see Appendix B, "GMT Time Zones."

Configuring User Login Settings

When users log on to Change Control Management from the opening page, they can select **Remember my login on this computer** so that the next time they log on from the same computer, they do not need to enter a username and password.

You can disable the **Remember my login on this computer** option in the **<Change Control Management installation directory>/conf/ security.settings** file, by setting the value of the **<remember-me-enabled>** element to **false** and then restarting the Change Control Management server.

```
<settings>
    <session-settings version="2.1.0">
        <remember-me-enabled>false</remember-me-enabled>
    </session-settings>
</settings>
```

The **Remember my login on this computer** option, no longer appears on the opening screen.
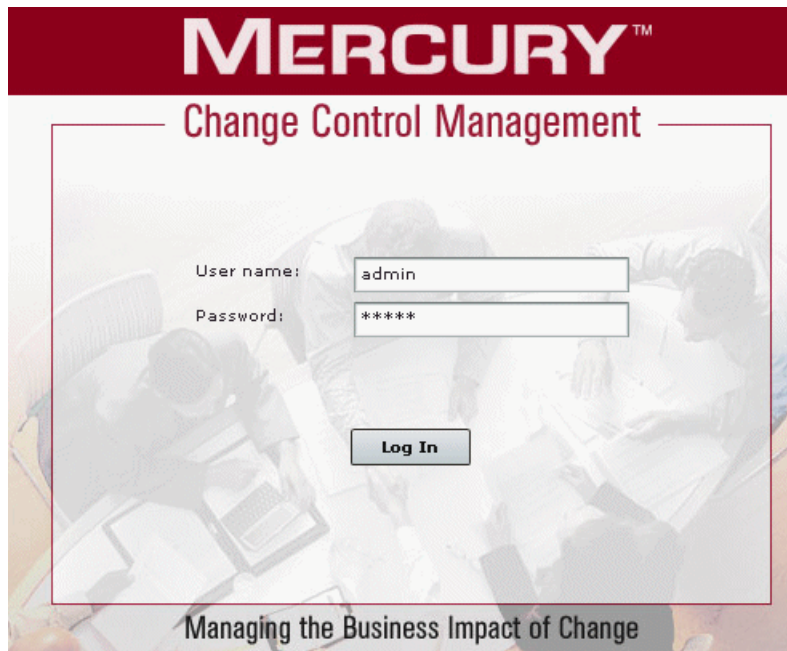
To restore the **Remember my login on this computer** option, set the value of the **<remember-me-enabled>** element to **true** and restart the Change Control Management server.

9

Configuring Users and Applications

This chapter describes how the administrator can define and edit user settings, associate applications with certain users, view the users associated with each application, and associate users with specific applications.

Note: This chapter describes the Administration module, which can be viewed by the administrator only.

This chapter describes:	On page:
Configuring Users	152
Associating Applications with Users	155
Assigning Importance Levels to Applications	157

Configuring Users

You can configure user settings for new Mercury Change Control Management users, edit the settings of existing users, and delete users in the Users tab.

Configuring User Settings

You define a new user by configuring settings—including basic user details and associated applications—for the user.

To configure user settings:

1 In the **Administration** module **Users** tab, click **New** at the bottom of the page. The User Settings dialog box opens.

2 Enter the following user settings:

Column	Description
Login name	The user name by which the user will be able to log in to Change Control Management.
First name	The first name of the user you are defining.
Last name	The surname of the user you are defining.

Column	Description
E-Mail address	The e-mail address of the user you are defining. This is the e-mail address to which notifications will be sent for this user.
Password	The password by which the user will be able to log in to Change Control Management.
Retype password	Confirms the password entered in the previous box.

3 From the **User role** box, select **Administrator** or **User** to define the type of user you want to create. Note that only the administrator has administrative privileges.

4 To associate applications with the user you are defining, click the **User Applications** tab, select the applications you want to associate with the user from the **Available Applications** list, and click the top arrow. The applications appear in the **Selected Applications** list.
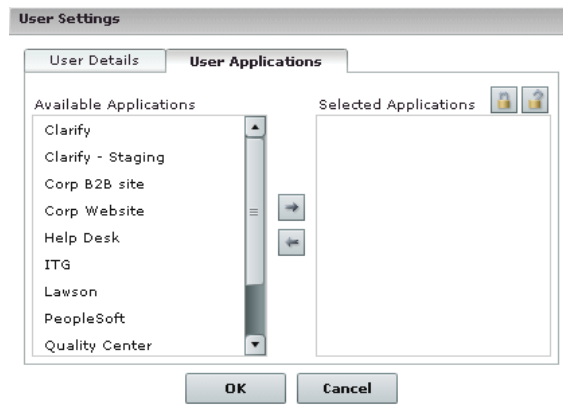
5 To ensure that the user will receive notifications related to a specific application, select the application and click the **Enforce Application** button. When this option is selected, the user cannot remove the association with the application.

To restore the user's ability to choose whether or not to receive notifications related to this application, select the application and click the **Stop Enforcing Application** button.

153

6 Click **OK** to save your settings and close the User Settings dialog box. The new user is added to the Change Control Management database and is listed in the Users tab.

Modifying User Settings

As an administrator, you can modify the settings of an existing Change Control Management user.

To modify user settings:

1 In the **Administration** module **Users** tab, select the user whose settings you want to modify and click **Edit** at the bottom of the page. The User Settings – <Name of User> dialog box opens.

2 Modify the user details and applications associated with the user as required. For a description of user settings, see "Configuring User Settings" on page 152.

3 Click **OK** to save your changes and close the User Settings – <Name of User> dialog box.

Deleting Users

You can delete any previously defined Change Control Management users.

To delete users:

1 In the **Administration** module **Users** tab, select the user(s) you want to delete and click the **Delete** button at the bottom of the page.

2 Click **Yes** to confirm deletion. Change Control Management deletes the user(s) from the application.

Associating Applications with Users

You can view details of the IT applications affected by the change requests that Change Control Management processes and associate specific users with these applications in the Applications tab.

To associate specific Change Control Management users with an application:

1 In the **Administration** module, click the **Applications** tab and select the application you want to associate with one or more users.

2 Click **Edit** at the bottom of the Applications tab. The Application Properties – <Application Name> dialog box opens, displaying a description of the application as well as other Mercury Application Mapping-related details of the application.

3 Click the **Application Users** tab. A list of the Change Control Management users previously defined by the administrator is displayed in the **Available Users** column.
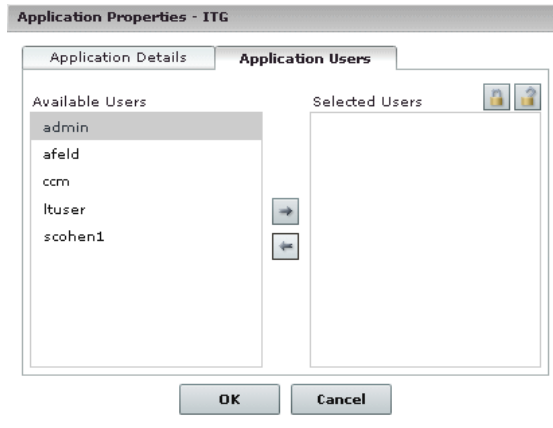
4 Select the users you want to associate with the application from the **Available Users** list, and click the top arrow. The users appear in the **Selected Users** list.
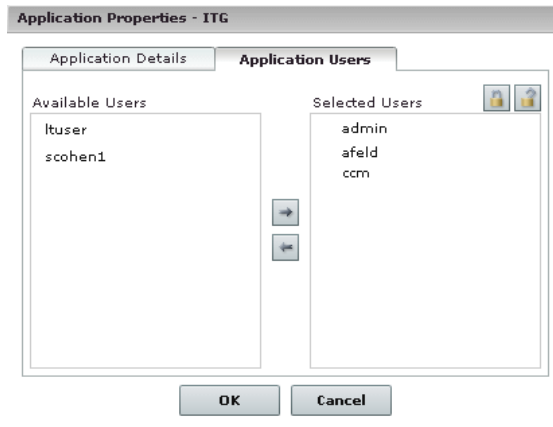
5 To ensure that a user will receive notifications related to this application, select the user and click the **Enforce Application** button. When this option is selected, the user cannot remove the association with the application.

To restore the user's ability to choose whether or not to receive notifications related to this application, select the user and click the **Stop Enforcing Application** button.

6 Click **OK** to save your settings and close the Application Properties – <Application Name> dialog box.

7 To view the users you associated with the application, click the **Refresh** button at the bottom of the Applications tab. The users are displayed in the **Users** column.

Assigning Importance Levels to Applications

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

To assign importance levels to applications:

1 Click the **Applications** tab and select the application for which you want to assign an importance level.

2 Click **Edit** at the bottom of the Applications tab. The Application Properties – <Application Name> dialog box opens, displaying a description of the application as well as other Mercury Application Mapping-related details of the application.

3 From the **Application importance** list, select an application importance level between 1 and 10.

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

In this case, the default mapping is used for the **application importance** risk factor in the risk calculation. For more information about defining risk factors, see "Defining Risk Factors" on page 88.

Part IV

Appendixes

A

Password Encryption

All Change Control Management passwords may be encrypted, if required.

To encrypt a specific password:

1 In the **<Change Control Management installation directory>/utilities/ security** directory, run the following:

EncryptPassword.bat <password to encrypt>

2 Copy and paste the generated encrypted password (**{ENCRYPTED} <encrypted password>**) into the appropriate Change Control Management 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 **<Change Control Management installation directory>/utilities/ security** directory, run the following:

EncryptPassword.bat -f <file name>

A file with the same name and the extension **.enc** is created. This file includes an encrypted password for each password included in the original file.

3 Copy and paste each generated encrypted password (**{ENCRYPTED} <encrypted password>**) into the appropriate Change Control Management configuration file.

B

GMT Time Zones

The following list describes GMT time zones for locations throughout the world.

(GMT -11) Pacific/Niue
(GMT -11) MIT
(GMT -10) Pacific/Tahiti
(GMT -10) Pacific/Honolulu
(GMT -10) America/Adak
(GMT -9) Pacific/Marquesas
(GMT -9) America/Anchorage
(GMT -8) Pacific/Pitcairn
(GMT -8) America/Tijuana
(GMT -8) PST
(GMT -7) America/Phoenix
(GMT -7) America/Edmonton
(GMT -7) America/Denver
(GMT -6) America/Belize
(GMT -6) Pacific/Galapagos
(GMT -6) America/Tegucigalpa
(GMT -6) America/Costa_Rica
(GMT -6) Pacific/Easter
(GMT -6) America/Chicago
(GMT -5) America/Porto_Acre
(GMT -5) America/Guayaquil
(GMT -5) America/Cayman
(GMT -5) America/Panama
(GMT -5) America/Indianapolis
(GMT -5) America/Nassau

(GMT -11) Pacific/Apia
(GMT -11) Pacific/Pago_Pago
(GMT -10) Pacific/Fakaofo
(GMT -10) HST
(GMT -10) Pacific/Rarotonga
(GMT -9) Pacific/Gambier
(GMT -9) AST
(GMT -8) America/Vancouver
(GMT -8) America/Los_Angeles
(GMT -7) America/Dawson_Creek
(GMT -7) PNT
(GMT -7) America/Mazatlan
(GMT -7) MST
(GMT -6) America/Regina
(GMT -6) America/Guatemala
(GMT -6) America/El_Salvador
(GMT -6) America/Winnipeg
(GMT -6) America/Mexico_City
(GMT -6) CST
(GMT -5) America/Bogota
(GMT -5) America/Jamaica
(GMT -5) America/Managua
(GMT -5) America/Lima
(GMT -5) IET
(GMT -5) America/Montreal

(GMT -5) America/Havana	(GMT -5) America/Port-au-Prince
(GMT -5) America/Grand_Turk	(GMT -5) America/New_York
(GMT -5) EST	(GMT -4) America/Antigua
(GMT -4) America/Anguilla	(GMT -4) America/Curacao
(GMT -4) America/Aruba	(GMT -4) America/Barbados
(GMT -4) America/La_Paz	(GMT -4) America/Manaus
(GMT -4) America/Dominica	(GMT -4) America/Santo_Domingo
(GMT -4) America/Grenada	(GMT -4) America/Guadeloupe
(GMT -4) America/Guyana	(GMT -4) America/St_Kitts
(GMT -4) America/St_Lucia	(GMT -4) America/Martinique
(GMT -4) America/Montserrat	(GMT -4) America/Puerto_Rico
(GMT -4) PRT	(GMT -4) America/Port_of_Spain
(GMT -4) America/St_Vincent	(GMT -4) America/Tortola
(GMT -4) America/St_Thomas	(GMT -4) America/Caracas
(GMT -4) Antarctica/Palmer	(GMT -4) Atlantic/Bermuda
(GMT -4) America/Cuiaba	(GMT -4) America/Halifax
(GMT -4) Atlantic/Stanley	(GMT -4) America/Thule
(GMT -4) America/Asuncion	(GMT -4) America/Santiago
(GMT -3) America/St_Johns	(GMT -3) CNT
(GMT -3) America/Fortaleza	(GMT -3) America/Cayenne
(GMT -3) America/Paramaribo	(GMT -3) America/Montevideo
(GMT -3) America/Buenos_Aires	(GMT -3) AGT
(GMT -3) America/Godthab	(GMT -3) America/Miquelon
(GMT -3) America/Sao_Paulo	(GMT -3) BET
(GMT -2) America/Noronha	(GMT -2) Atlantic/South_Georgia
(GMT -1) Atlantic/Jan_Mayen	(GMT -1) Atlantic/Cape_Verde
(GMT -1) America/Scoresbysund	(GMT -1) Atlantic/Azores
(GMT +0) Africa/Ouagadougou	(GMT +0) Africa/Abidjan
(GMT +0) Africa/Accra	(GMT +0) Africa/Banjul
(GMT +0) Africa/Conakry	(GMT +0) Africa/Bissau
(GMT +0) Atlantic/Reykjavik	(GMT +0) Africa/Monrovia
(GMT +0) Africa/Casablanca	(GMT +0) Africa/Timbuktu
(GMT +0) Africa/Nouakchott	(GMT +0) Atlantic/St_Helena
(GMT +0) Africa/Freetown	(GMT +0) Africa/Dakar
(GMT +0) Africa/Sao_Tome	(GMT +0) Africa/Lome
(GMT +0) GMT	(GMT +0) UTC

(GMT +0) Atlantic/Faeroe
(GMT +0) Atlantic/Canary
(GMT +0) Europe/Dublin
(GMT +0) Europe/Lisbon
(GMT +0) Europe/London
(GMT +1) Africa/Luanda
(GMT +1) Africa/Porto-Novo
(GMT +1) Africa/Bangui
(GMT +1) Africa/Kinshasa
(GMT +1) Africa/Douala
(GMT +1) Africa/Libreville
(GMT +1) Africa/Malabo
(GMT +1) Africa/Niamey
(GMT +1) Africa/Lagos
(GMT +1) Africa/Ndjamena
(GMT +1) Africa/Tunis
(GMT +1) Africa/Algiers
(GMT +1) Europe/Andorra
(GMT +1) Europe/Tirane
(GMT +1) Europe/Vienna
(GMT +1) Europe/Brussels
(GMT +1) Europe/Zurich
(GMT +1) Europe/Prague
(GMT +1) Europe/Berlin
(GMT +1) Europe/Copenhagen
(GMT +1) Europe/Madrid
(GMT +1) Europe/Gibraltar
(GMT +1) Europe/Budapest
(GMT +1) Europe/Rome
(GMT +1) Europe/Vaduz
(GMT +1) Europe/Luxembourg
(GMT +2) Africa/Tripoli
(GMT +1) Europe/Monaco
(GMT +1) Europe/Malta
(GMT +1) Africa/Windhoek
(GMT +1) Europe/Amsterdam
(GMT +1) Europe/Oslo
(GMT +1) Europe/Warsaw
(GMT +1) Europe/Stockholm
(GMT +1) Europe/Belgrade
(GMT +1) Europe/Paris
(GMT +1) ECT
(GMT +2) Africa/Bujumbura
(GMT +2) Africa/Gaborone
(GMT +2) Africa/Lubumbashi
(GMT +2) Africa/Maseru
(GMT +2) Africa/Blantyre
(GMT +2) Africa/Maputo
(GMT +2) Africa/Kigali
(GMT +2) Africa/Khartoum
(GMT +2) Africa/Mbabane
(GMT +2) Africa/Lusaka
(GMT +2) Africa/Harare
(GMT +2) CAT
(GMT +2) Africa/Johannesburg
(GMT +2) Europe/Sofia
(GMT +2) Europe/Minsk
(GMT +2) Asia/Nicosia
(GMT +2) Europe/Tallinn
(GMT +2) Africa/Cairo
(GMT +2) ART
(GMT +2) Europe/Helsinki
(GMT +2) Europe/Athens
(GMT +2) Asia/Jerusalem
(GMT +2) Asia/Amman
(GMT +2) Asia/Beirut
(GMT +1) Europe/Vilnius
(GMT +2) Europe/Riga
(GMT +2) Europe/Chisinau
(GMT +2) Europe/Bucharest
(GMT +2) Europe/Kaliningrad
(GMT +2) Asia/Damascus

(GMT +2) Europe/Kiev	(GMT +2) Europe/Istanbul
(GMT +2) EET	(GMT +3) Asia/Bahrain
(GMT +3) Africa/Djibouti	(GMT +3) Africa/Asmera
(GMT +3) Africa/Addis_Ababa	(GMT +3) EAT
(GMT +3) Africa/Nairobi	(GMT +3) Indian/Comoro
(GMT +3) Asia/Kuwait	(GMT +3) Indian/Antananarivo
(GMT +3) Asia/Qatar	(GMT +3) Africa/Mogadishu
(GMT +3) Africa/Dar_es_Salaam	(GMT +3) Africa/Kampala
(GMT +3) Asia/Aden	(GMT +3) Indian/Mayotte
(GMT +3) Asia/Riyadh	(GMT +3) Asia/Baghdad
(GMT +2) Europe/Simferopol	(GMT +3) Europe/Moscow
(GMT +3) Asia/Tehran	(GMT +3) MET
(GMT +4) Asia/Dubai	(GMT +4) Indian/Mauritius
(GMT +4) Asia/Muscat	(GMT +4) Indian/Reunion
(GMT +4) Indian/Mahe	(GMT +4) Asia/Yerevan
(GMT +4) NET	(GMT +4) Asia/Baku
(GMT +4) Asia/Aqtau	(GMT +4) Europe/Samara
(GMT +4) Asia/Kabul	(GMT +5) Indian/Kerguelen
(GMT +4) Asia/Tbilisi	(GMT +5) Indian/Chagos
(GMT +5) Indian/Maldives	(GMT +5) Asia/Dushanbe
(GMT +5) Asia/Ashkhabad	(GMT +5) Asia/Tashkent
(GMT +5) Asia/Karachi	(GMT +5) PLT
(GMT +5) Asia/Bishkek	(GMT +5) Asia/Aqtobe
(GMT +5) Asia/Yekaterinburg	(GMT +5) Asia/Calcutta
(GMT +5) IST	(GMT +5) Asia/Katmandu
(GMT +6) Antarctica/Mawson	(GMT +6) Asia/Thimbu
(GMT +6) Asia/Colombo	(GMT +6) Asia/Dacca
(GMT +6) BST	(GMT +6) Asia/Almaty
(GMT +6) Asia/Novosibirsk	(GMT +6) Indian/Cocos
(GMT +6) Asia/Rangoon	(GMT +7) Indian/Christmas
(GMT +7) Asia/Jakarta	(GMT +7) Asia/Phnom_Penh
(GMT +7) Asia/Vientiane	(GMT +7) Asia/Saigon
(GMT +7) VST	(GMT +7) Asia/Bangkok
(GMT +7) Asia/Krasnoyarsk	(GMT +8) Antarctica/Casey
(GMT +8) Australia/Perth	(GMT +8) Asia/Brunei
(GMT +8) Asia/Hong_Kong	(GMT +8) Asia/Ujung_Pandang

(GMT +8) Asia/Macao

(GMT +8) Asia/Manila

(GMT +8) Asia/Taipei

(GMT +8) CTT

(GMT +8) Asia/Irkutsk

(GMT +9) Asia/Pyongyang

(GMT +9) Pacific/Palau

(GMT +9) JST

(GMT +9) Australia/Darwin

(GMT +9) Australia/Adelaide

(GMT +10) Australia/Hobart

(GMT +10) Pacific/Truk

(GMT +10) Pacific/Saipan

(GMT +10) Australia/Brisbane

(GMT +10) Australia/Sydney

(GMT +10) Australia/Lord_Howe

(GMT +11) Pacific/Efate

(GMT +11) SST

(GMT +11) Asia/Magadan

(GMT +12) Pacific/Kosrae

(GMT +12) Pacific/Majuro

(GMT +12) Pacific/Funafuti

(GMT +12) Pacific/Wallis

(GMT +12) Antarctica/McMurdo

(GMT +12) Pacific/Auckland

(GMT +12) Pacific/Chatham

(GMT +13) Pacific/Tongatapu

(GMT +14) Pacific/Kiritimati

(GMT +8) Asia/Kuala_Lumpur

(GMT +8) Asia/Singapore

(GMT +8) Asia/Shanghai

(GMT +8) Asia/Ulan_Bator

(GMT +9) Asia/Jayapura

(GMT +9) Asia/Seoul

(GMT +9) Asia/Tokyo

(GMT +9) Asia/Yakutsk

(GMT +9) ACT

(GMT +9) Australia/Broken_Hill

(GMT +10)
Antarctica/DumontDUrville

(GMT +10) Pacific/Guam

(GMT +10) Pacific/Port_Moresby

(GMT +10) Asia/Vladivostok

(GMT +10) AET

(GMT +11) Pacific/Ponape

(GMT +11) Pacific/Guadalcanal

(GMT +11) Pacific/Noumea

(GMT +11) Pacific/Norfolk

(GMT +12) Pacific/Tarawa

(GMT +12) Pacific/Nauru

(GMT +12) Pacific/Wake

(GMT +12) Pacific/Fiji

(GMT +12) Asia/Kamchatka

(GMT +12) NST

(GMT +13) Pacific/Enderbury

(GMT +13) Asia/Anadyr

C

Preconfigured Change Request Fields

By default, Change Control Management contains a set of preconfigured change request fields. There are two types of fields:

➤ **Predefined fields.** Fields based on ITIL standards, which are common to most service desk applications.

➤ **Custom fields.** Fields which are recommended for use in order to optimize Change Control Management analysis features.

The following **Predefined** fields are included in Change Control Management:

name	description
actual-end-time	The actual change activity's completion time
actual-start-time	The actual change activity's start time
calculated-risk	The risk value calculated for this change request
change-types-orig	The change types assigned to this request as defined in the original service desk. This data is used during latent and detected change analysis.
collision-severity	colliding-severity collision-severity The collision severity level evaluated for his request
contact-email	The e-mail 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	The person who serves as a contact regarding this change request

name	description
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 this change request was created
description	A description of the change request
ignore-detection	Signifies whether to try and detect the change request or skip it during the detection stage.
impact-severity	The impact severity level evaluated for his request
implementor	The person assigned to implement the change
internal-id	An id value used internally by CCM
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 this change request.
origin-url	A URL address that points to the original ticket in the creating service desk
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 creating user
request-id	An id value that originated from the creating service desk
source-itil-entity	The ITIL entity out of which, this change request was created (incident, problem, requirement)
status	The current status of the change request

name	description
summary	A short summary of the change request
user-estimated-risk	The risk level of the change request as evaluated by the creating user

The following **Custom** fields are included in Change Control Management:

name	description
changed-ci-list	The list of ci's that are part of the planned change
departments-involved	From how many different departments do the change implementors come from?
implementor-experience	What is the implementor's level of experience with regards to the work involved in this change?
involved-users	How many users use the applications involved with the change?
is-backout-possible	Is there a valid backout plan?
is-outage-planned	Is an outage planned as part of the change?
is-sox-app-involved	Is a SOX application involved in this change
is-tested	Was this change tested on a testing environment?
new-deployment	Is this change a deployment of a new hardware, major feature or application?
past-experience	What was the success ratio of similar changes in the past?
recent-incidents	Has an application involved in the change had major incidents within the last two weeks?
sla-status	Is the SLA of an application involved in the change close to being breached?

name	description
technology-experience	How long ago (in quarters) was the technology involved in this change introduced to the organization?
vip-users	Are there any VIP users using applications involved with the change?

D

Using CCM Logs

This appendix describes the log files available in Change Control Management. These log files are located in the **<Change Control Management installation directory>/logs** directory.

The following table describes each of the Change Control Management log files:

Log name	Usage
ccm_sdi	Log for the Service Desk Integration module (SDI): the process of collection and conversion of tickets, until they reach the CCM_QUEUED_CHANGES input queue of the Change Control Management platform.
ccm_platform	Log for the main Change Control Management platform. Contains information regarding the ticket analysis process (for example, impact and collision analysis), notification deliveries, risk recalculations, and other information.
ccm_mam	Log for the module responsible for interfacing with Mercury Application Mapping (MAM).
ccm_client	Log for requests initiated from the UI or from web-services.
ccm_datamodel	Log for most of the interactions between Change Control Management and the database.
ccm_hibernate	Log for the interactions with the database involving the **hibernate** object to data-base mapper.

Log name	Usage
ccm_c3p0	Log for the interactions with the database involving the **c3p0** database connection pool.
ccm_genericinfra	Log for infrastructure utilities such as settings, scripting, and security.
ccm_onyxinfra	Log for infrastructure utilities that depend on the database and enumerations.

When you are investigating an incident, it is recommended you begin by looking through the logs for the Service Desk Integration module (**ccm_sdi**) or for the main Change Control Management platform (**ccm_platform**), depending on which part of the ticket process you want to investigate.

Note: You configure the log file properties in the **<Change Control Management installation directory>/conf/ccmlog4j.properties** file. This file contains a list of log file definitions, which you can modify. For more information about configuring the log file properties, see "Configuring Log File Properties" on page 147.

E

Configuring and Maintaining Mercury Change Control Management Databases

This appendix provides important guidelines for configuring and maintaining both Microsoft SQL Server and Oracle Server databases.

This appendix describes:	On page:
Configuration and Maintenance Guidelines for MS SQL Server Databases	176
Configuration and Maintenance Guidelines for Oracle Server Databases	178

Configuration and Maintenance Guidelines for MS SQL Server Databases

This section includes the following guidelines:

➤ "Data and Index Page Reorganization" on page 176

➤ "Updating Statistics" on page 177

Data and Index Page Reorganization

The Change Control Management database may become fragmented after processing a certain number of requests. To prevent fragmentation from seriously affecting client-side performance, it is recommended that you design a maintenance plan that causes the indexes on the database tables to be dropped and recreated.

To create a maintenance plan:

1 Open the MS SQL Server Enterprise Manager.

2 Under the relevant MS SQL Server registration, select **Management**.

3 Right-click **Database Maintenance Plans** and select **New Maintenance Plan**. The Database Maintenance Plan Wizard opens to guide you through the required definition parameters.

4 Choose the database for which you want to create a maintenance plan and click **Next**.

5 Select the **Reorganize data and index pages** check box and choose the **Change free space per page percentage to** option.

6 Set the free space per page to **10** percent and click **Next**.

7 Accept all the other default settings in the wizard and save your maintenance plan.

Note: After the maintenance plan has been executed, statistics should be updated.

Updating Statistics

MS SQL Server 2000 allows statistical information regarding the distribution of values in a column to be created. This statistical information can be used by the query processor to determine the optimal strategy for evaluating a query. When an index is being created, MS SQL Server automatically stores statistical information regarding the distribution of values in the indexed column(s). The query optimizer in MS SQL Server uses these statistics to estimate the cost of using the index for a query. As the data in a column changes, index and column statistics can become out-of-date and cause the query optimizer to make less than optimal decisions regarding the processing of a query.

It is recommended that you update index statistics to provide the query optimizer with up-to-date information about the distribution of data values in the tables. With more information about the data stored in the database, the query optimizer is able to make better judgments about the best way to access data.

By default, the **auto update statistics** database option is enabled, but if this option has been disabled, it is strongly recommended that you create an automatic task to update statistics for the database on a daily basis, as the data is frequently changed. The job should execute the **sp_updatestats** API against the specific database.

Configuration and Maintenance Guidelines for Oracle Server Databases

This section includes the following guidelines:

➤ "Cache Attribute Settings" on page 178

➤ "Gathering Statistics" on page 178

Cache Attribute Settings

Set the **cache\nocache** attribute of the **CCM_CHANGES** table to **cache** by executing the following statement:

```
alter table CCM_CHANGES cache;
```

Gathering Statistics

It is recommended that you gather statistics once a day. To do so effectively, you should follow the steps in the following procedure:

To gather statistics once a day:

1 Turn on the **MONITORING** flag to the tables in the CCM schema by executing the following procedure:

```
exec dbms_stats.alter_schema_tab_monitoring('<name of oracle schema>',TRUE);
```

2 Create a 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;
/
```

Important:

➤ 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. Therefore, if this job is active in your DB, there is no need to perform the actions described in the above procedure.

Index

T

time zones
    list of 163
    modifying in log files 148
typographical conventions x

U

updates, documentation ix
user name constraints, configuration 120
user schema configuration 144
user settings
    configuring (administrator) 152
    modifying (administrator) 154
user, configuring for Mercury Application
       Mapping 108
user-mailbody-html.ftl file 81
user-mailbody-text.ftl file 81
users
    associating with applications
      (administrator) 155
    deleting (administrator) 155