

OPTIMIZE

MERCURY CHANGE CONTROL MANAGEMENT™

Installation and Configuration Guide

Version 1.1

MERCURY™
BUSINESS TECHNOLOGY OPTIMIZATION

Mercury Change Control Management

Installation and Configuration Guide

Version 1.1

Document Release Date: May 31, 2006

MERCURY™

Mercury Change Control Management Installation and Configuration Guide, Version 1.1

This manual, and the accompanying software and other documentation, is protected by U.S. and international copyright laws, and may be used only in accordance with the accompanying license agreement. Features of the software, and of other products and services of Mercury Interactive Corporation, may be covered by one or more of the following patents: United States: 5,511,185; 5,657,438; 5,701,139; 5,870,559; 5,958,008; 5,974,572; 6,137,782; 6,138,157; 6,144,962; 6,205,122; 6,237,006; 6,341,310; 6,360,332; 6,449,739; 6,470,383; 6,477,483; 6,549,944; 6,560,564; 6,564,342; 6,587,969; 6,631,408; 6,631,411; 6,633,912; 6,694,288; 6,738,813; 6,738,933; 6,754,701; 6,792,460 and 6,810,494. Australia: 763468 and 762554. Other patents pending. All rights reserved.

Mercury, Mercury Interactive, the Mercury logo, the Mercury Interactive logo, LoadRunner, WinRunner, SiteScope and TestDirector are trademarks of Mercury Interactive Corporation and may be registered in certain jurisdictions. The absence of a trademark from this list does not constitute a waiver of Mercury's intellectual property rights concerning that trademark.

All other company, brand and product names may be trademarks or registered trademarks of their respective holders. Mercury disclaims any responsibility for specifying which marks are owned by which companies or which organizations.

Mercury provides links to external third-party Web sites to help you find supplemental information. Site content and availability may change without notice. Mercury makes no representations or warranties whatsoever as to site content or availability.

Mercury Interactive Corporation
379 North Whisman Road
Mountain View, CA 94043
Tel: (650) 603-5200
Toll Free: (800) TEST-911
Customer Support: (877) TEST-HLP
Fax: (650) 603-5300

© 2006 Mercury Interactive Corporation, All rights reserved

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

Table of Contents

Welcome to This Guide	v
How This Guide Is Organized	v
Who Should Read This Guide	vi
Change Control Management Documentation.....	vi
Additional Online Resources.....	vii
Documentation Updates	vii
Typographical Conventions.....	viii

PART I: INTRODUCTION

Chapter 1: Introduction to Mercury Change Control Management ...	3
Working with Change Control Management.....	3

PART II: INSTALLATION AND DEPLOYMENT

Chapter 2: Installing Mercury Change Control Management	9
System Requirements	10
Installation Procedures.....	11
Post-Installation Procedures	20

PART III: CONFIGURATION

Chapter 3: Introduction to Mercury Change Control Management Configuration	25
Overview of the Change Control Management Configuration Process	26
How to Approach Change Control Management Configuration.....	30
Chapter 4: Configuring the Conversion of Service Desk Application-Specific Requests to Generic Requests	37
Customizing Change Control Management Fields	38
About Converting Service Desk Application-Specific Requests to Generic Requests	40
Overview of Adapter Configuration.....	42
Location and Naming Conventions of Service Desk Integration Files	43
Configuring the Common Adapter Attributes.....	45
Configuring the Connector Attributes.....	48
Configuring the Converter Attributes.....	64
Chapter 5: Configuring the Change Control Management Processing of Requests	71
Configuring the Collection of Converted Requests.....	72
Configuring the Analysis of Collected Requests	72
Configuring the Impact Analysis of Collected Requests	74
Configuring Notifications	74
Chapter 6: Configuring the Change Control Management Environment	77
Configuring the Change Control Management Database or User Schema	78
Configuring the SMTP Mail Server.....	79
Configuring Log File Properties	80
Chapter 7: Configuring Mercury Application Mapping-Related Settings	83
Configuring Mercury Application Mapping Connection Properties for the Change Control Management User	84
Configuring Settings for Mercury Application Mapping 6.1.....	86
Configuring Change Control Management-Mercury Application Mapping Integration Settings	87

Chapter 8: Configuring the Change Control Management	
Application	93
Configuring User Name and Password Constraints.....	94
Configuring Change Request Field Settings.....	95
Configuring Default Change Requests Pane Display Settings	106
Configuring Default Request Details Tab Display Settings.....	107
Configuring Default Filter Display Settings	109
Configuring Dashboard Settings	110
Configuring Enumeration Field Display Settings	112

PART IV: APPENDIXES

Appendix A: Password Encryption	117
Appendix B: GMT Time Zones	119

Table of Contents

Welcome to This Guide

Welcome to the *Mercury Control Management Installation and Configuration 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.”
<i>Arguments</i>	This style indicates method, property, or function arguments and book titles. For example, “Refer to the <i>Mercury User’s Guide</i> .”
<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

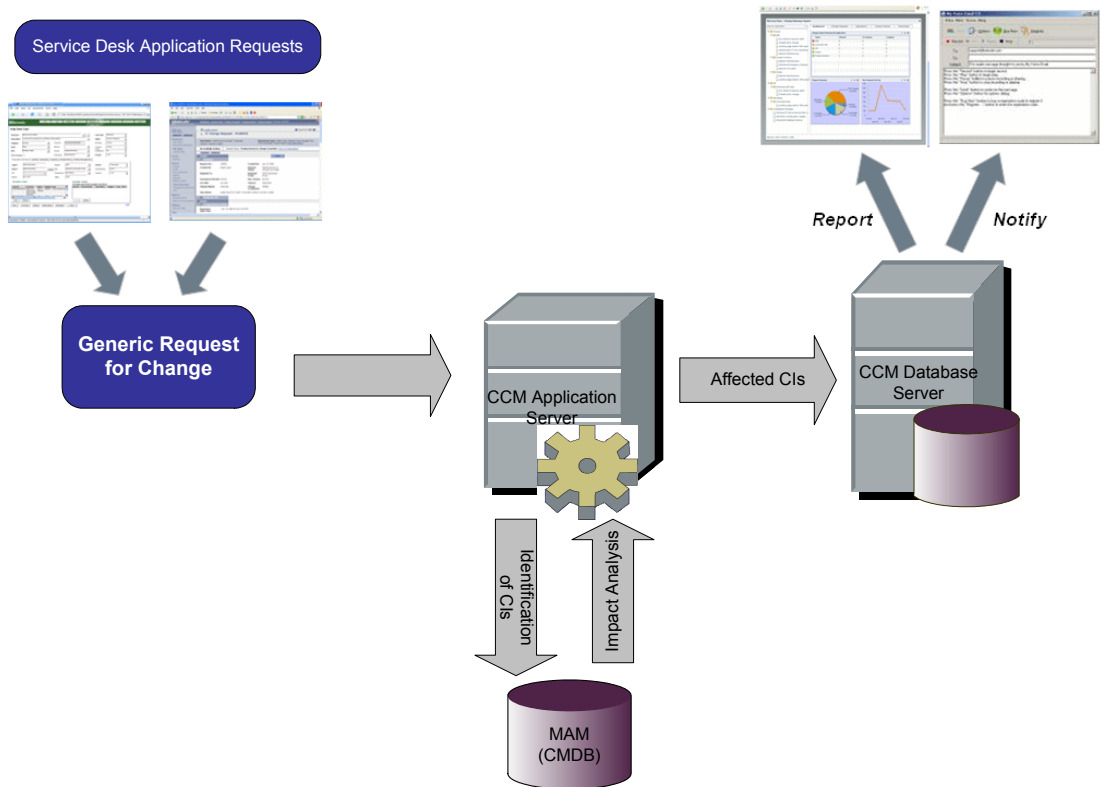
You use Change Control Management to analyze the effect of proposed software changes on the infrastructure components of your IT system. By running an impact analysis at various points in the workflow of a requested change, you can acquire a better picture of the effect the change will have and use this 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 provides you with a report showing the components in your IT environment that 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, Mercury Service Desk, or other third-party application requests) to generic requests that can be processed by the Change Control Management server.
- ▶ the transferring of generic requests to 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	<ul style="list-style-type: none"> ▶ Microsoft SQL Server 2000 Enterprise Edition Service Pack 4 ▶ Oracle 9i, 10
Mercury Application Mapping (MAM)	<p>Version 3.0 or 6.1</p> <p>For a full list of system requirements for each of these versions, refer to the Mercury Application Mapping documentation.</p>

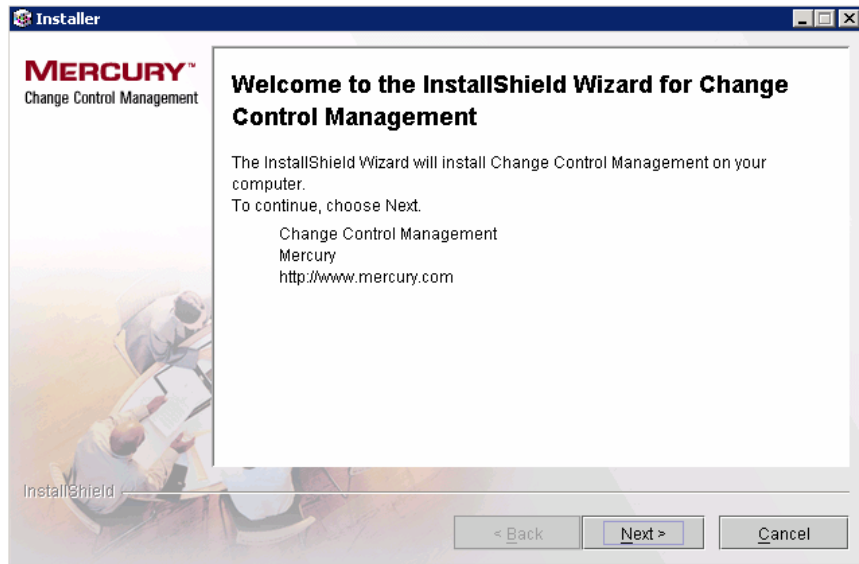
Note: For a list of the service desk applications supported, see “About Converting Service Desk Application-Specific Requests to Generic Requests” on page 40.

Installation Procedures

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

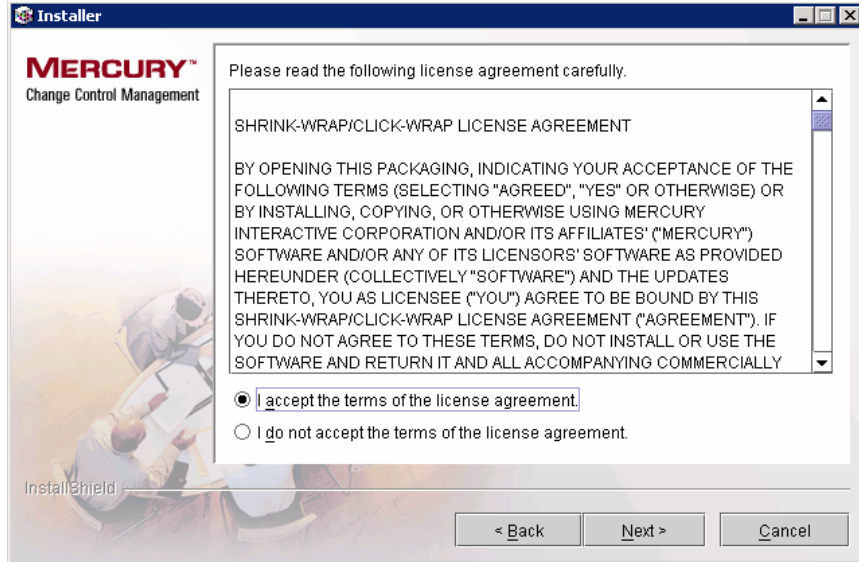
To install Change Control Management:

- 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.



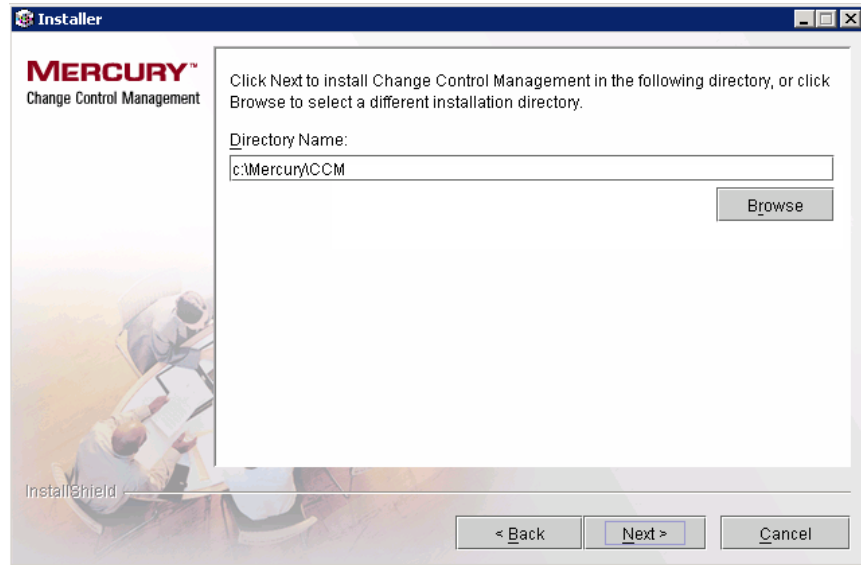
Click **Next**.

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



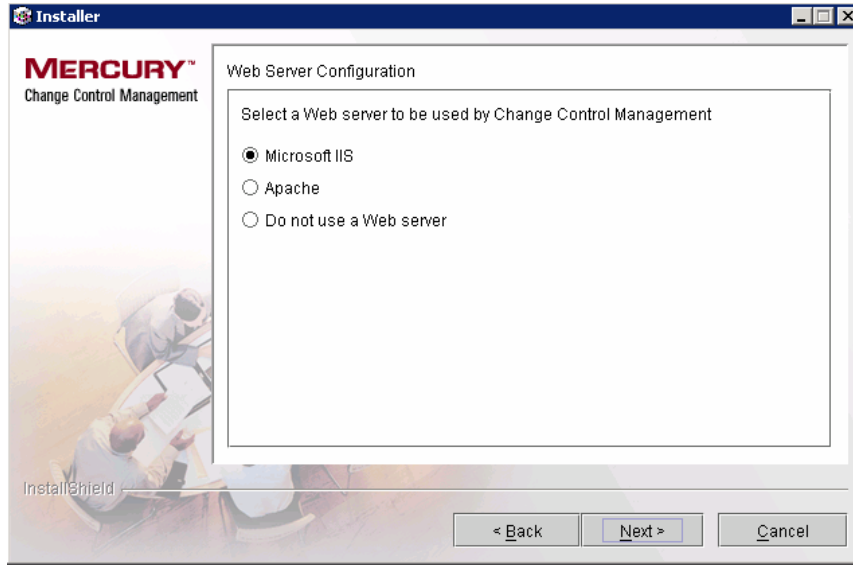
Click **Next**.

- 3 In the following screen, accept the default installation directory or click **Browse** to select a different directory.



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.

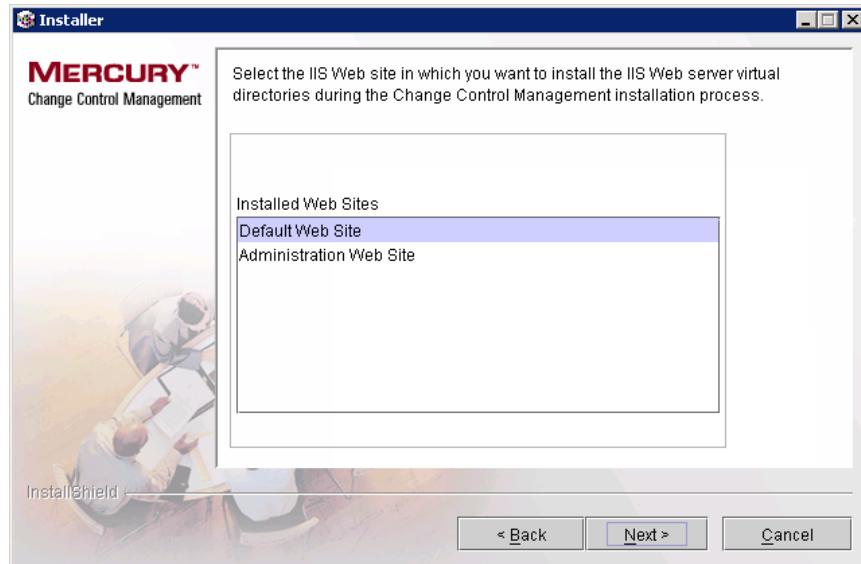


Notes:

- ▶ 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 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.”)

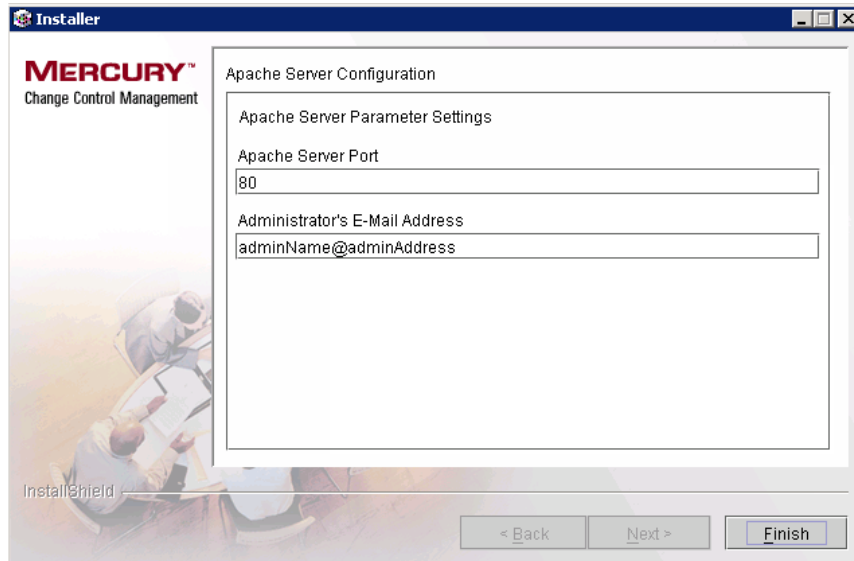
Click **Next**. If you selected **Microsoft IIS**, proceed to step 5. If you selected **Apache**, proceed to step 6. If you selected **Do not use a Web server**, proceed to step 7.

- 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.



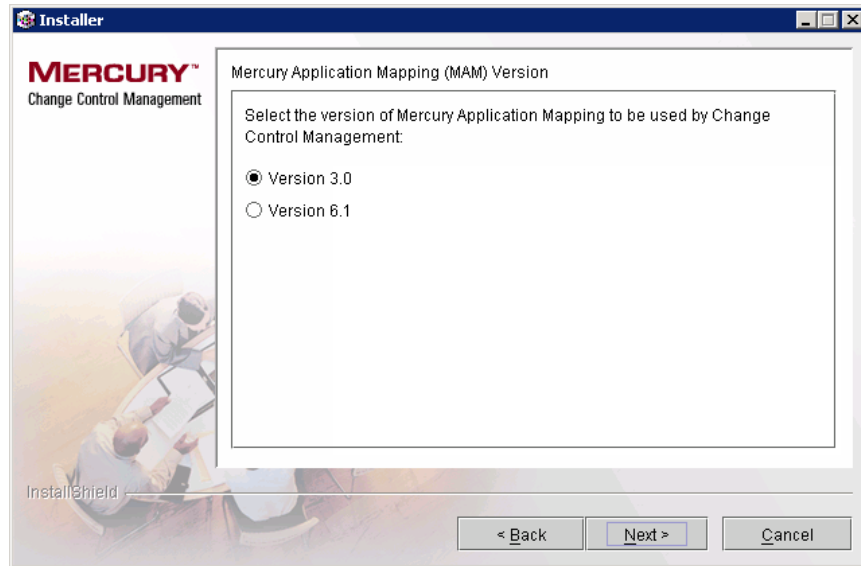
Select the required IIS Web site and click **Next**. Proceed to step 7.

- 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.



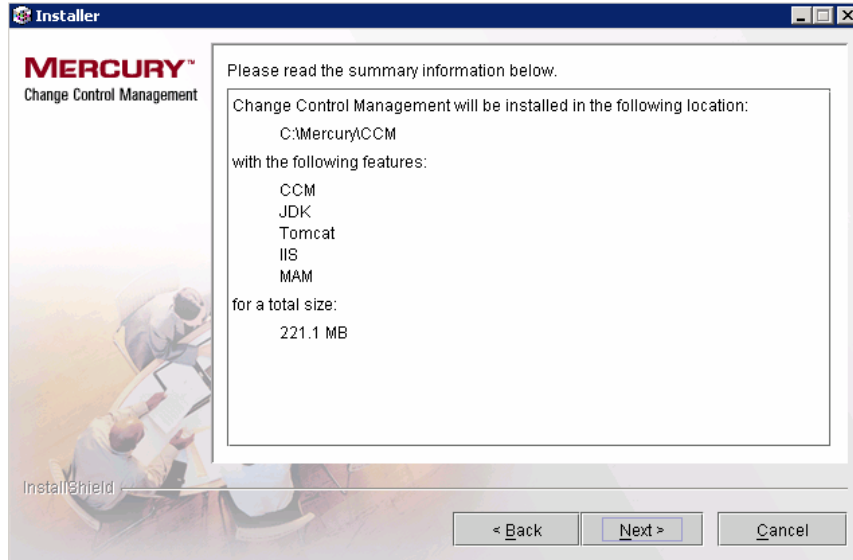
Click **Next**.

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



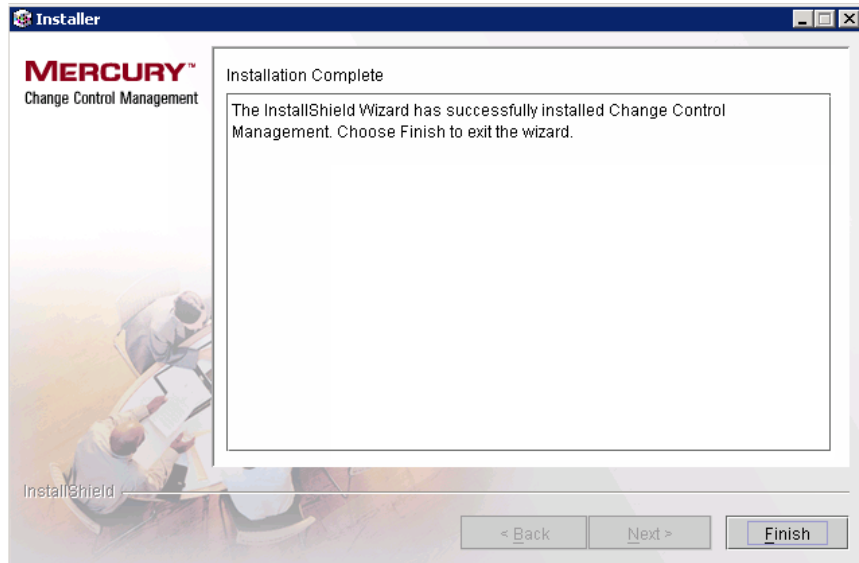
Click **Next**.

- 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 78.
- 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, deploy the **<Change Control Management installation directory>/MAM/6.1/extension/ccm_package.zip** package as described in “Configuring Settings for Mercury Application Mapping 6.1” on page 86.

- 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 84.
- 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
- ▶ the Change Control Management environment
- ▶ a Change Control Management-Mercury Application Mapping user
- ▶ Mercury Application Mapping settings (if you are working with Mercury Application Mapping 6.1)

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 cases in which Change Control Management calculates the impact of the identified CIs on the various components of your IT system.
- ▶ the sending of notifications as a result of an impact analysis calculation. You format notification content and configure the status and severity thresholds for which Change Control Management will send notifications.

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 the Change Control Management Environment

To work with Change Control Management, you must configure the following elements of your Change Control Management environment:

- ▶ 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 elements of your Change Control Management environment, see Chapter 6, “Configuring the Change Control Management Environment.”

Configuring a Change Control Management-Mercury Application Mapping User

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 the “Configuring Mercury Application Mapping Connection Properties for the Change Control Management User” section in Chapter 7.

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 6.1, 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 the “Configuring Settings for Mercury Application Mapping 6.1” section in Chapter 7.

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 the “Configuring Change Control Management-Mercury Application Mapping Integration Settings” section in Chapter 7.

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 8, “Configuring the Change Control Management Application.”

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.

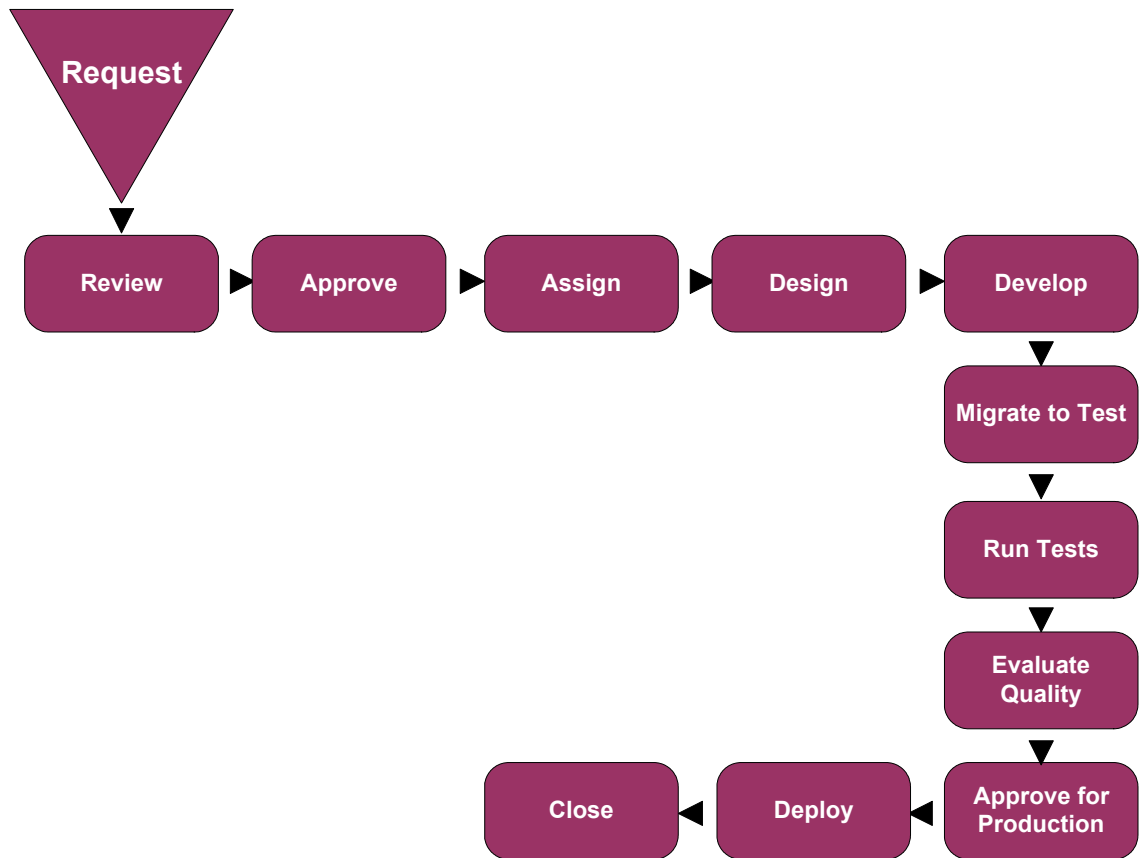
Your service desk application may contain a number of different types of change requests. For some of these change requests, such as a request from product marketing to modify a feature, impact analysis may be highly beneficial and you will want to ensure that Change Control Management performs an impact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

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

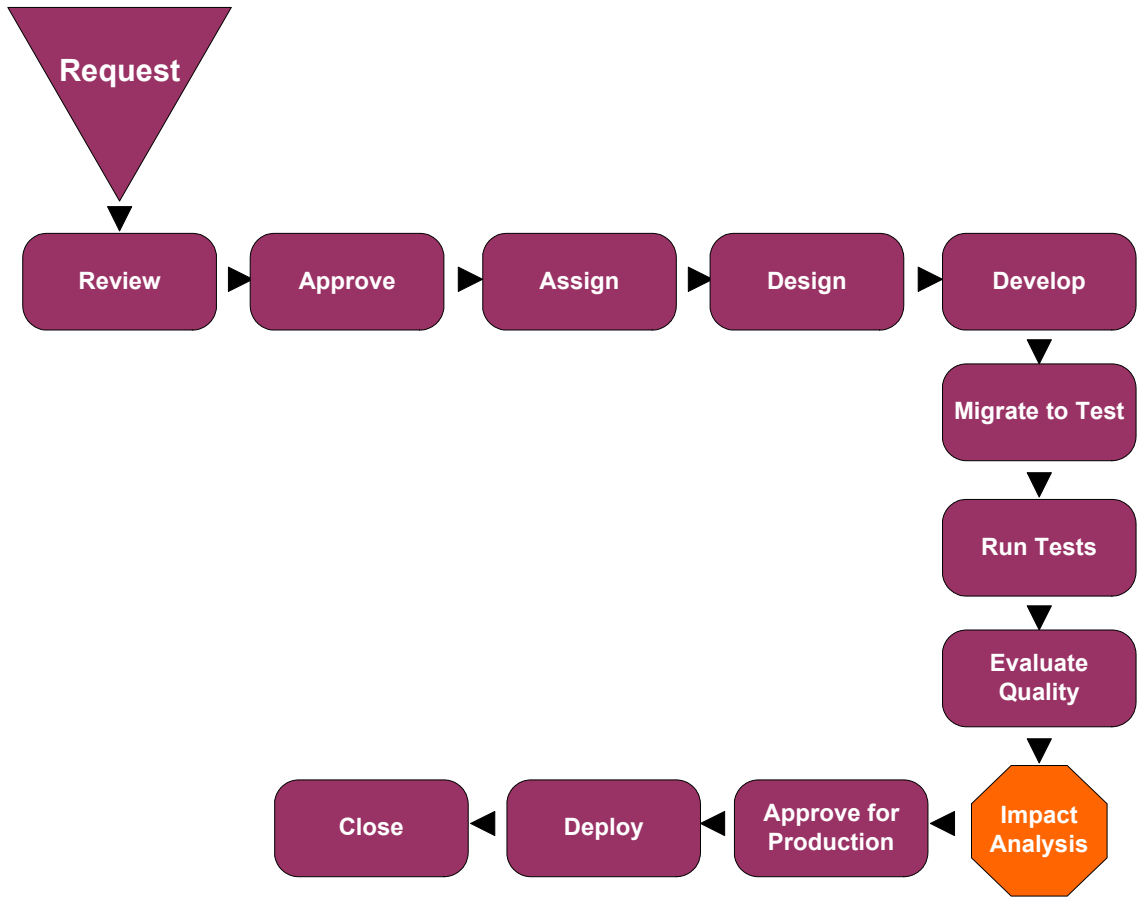
Once you have identified the types of change requests for which you want Change Control Management to perform impact analysis, it is important that you attend a Change Advisory Board meeting to gain a better understanding of the way in which change requests are managed in the organization.

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.

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

For each of the enumeration fields, determine which field value(s) in your service desk application requests should be mapped to each generic request 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.

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. You should also ensure that your Mercury Application Mapping correlation rules reflect your IT system.

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

9 Determine the thresholds for which notifications should be sent.

Change Control Management sends notifications for certain impact severity levels, 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,” for impact severity levels that are significant, such as a severity level of “High” or above.

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.

This chapter describes:	On page:
Customizing Change Control Management Fields	38
About Converting Service Desk Application-Specific Requests to Generic Requests	40
Overview of Adapter Configuration	42
Location and Naming Conventions of Service Desk Integration Files	43
Configuring the Common Adapter Attributes	45
Configuring the Connector Attributes	48
Configuring the Converter Attributes	64

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/field.settings` file. For details on customizing fields in the `field.settings` file, see “Configuring Change Request Field Settings” on page 95.

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>
```

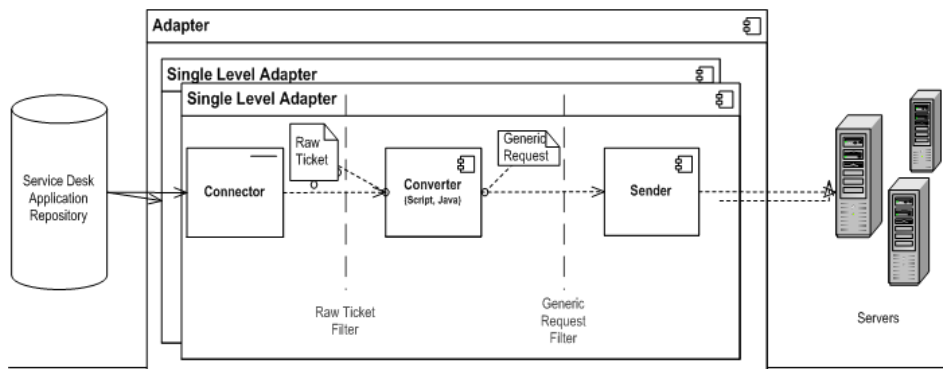
Notes:

- ▶ 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/enumerations-labels.properties** file. For details on configuring the **enumerations-labels.properties** file, see “Configuring Enumeration Field Display Settings” on page 112.
 - ▶ 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-integrations.settings** file. For details on configuring the impact severity level settings in the **mam-integrations.settings** file, see “Mapping Change Control Management-Mercury Application Mapping Severity Levels” on page 90.
-

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	<ul style="list-style-type: none"> ▶ 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	<ul style="list-style-type: none"> ▶ 6.1 Service Pack 1 – Web Services ▶ All versions that support Peregrine Connect-It, with XML target enabled.
Mercury Service Desk	9.1

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's attributes, such as the adapter's 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 45.

- ▶ 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 64.

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 65.

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.	—
service-desk-application (mandatory)	A unique, logical name for the service desk application that you are using. For example: Peregrine Service Center Note: This is the name that will be used for the service desk application within the Change Control Management application.	—

Property Name	Description	Default Value
number-of-tickets	<p>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.</p> <p>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.</p> <p>Note: To determine the number-of-tickets, consult with the people responsible for the service desk application(s) within your organization.</p>	50
polling-schedules	<p>A list of cron expressions separated by the new line character.</p> <p>Format: 30 * * * * <new line> 0 * * * *</p>	—
polling-frequency	<p>The frequency (in seconds) that the service desk application is polled for change requests.</p>	<p>If polling-schedules and polling-frequency are undefined, then the default is 30 seconds.</p>
use-xml-sender	<p>Specifies whether requests should be sent to XML files rather than the Change Control Management server.</p>	false

Property Name	Description	Default Value
initial-load-state	<p>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.</p> <p>Format: MM/dd/yy HH:mm:ss z</p>	null
request-types (mandatory)	<p>Lists all request types that the adapter collects, including all request type levels.</p> <pre data-bbox="551 579 1086 1171"><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></pre>	—

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 48
- ▶ “Peregrine ServiceCenter Connect-It Connector Settings” on page 50
- ▶ “Peregrine ServiceCenter Web Services Connector Settings” on page 51
- ▶ “IT Governance Web Services Connector Settings” on page 55
- ▶ “IT Governance RML Connector Settings” on page 56
- ▶ “Database Connector Settings” on page 59
- ▶ “Oracle Database Connector Settings” on page 62
- ▶ “Mercury Service Desk Connector Attributes” on page 63

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 **arutil50.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.”	—
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.	—
creationDatePropertyName (mandatory)	The property name of the request's creation-date value in the XML file.	—
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.	—

Property Name	Description	Default Value
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).	—
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	—

Property Name	Description	Default Value
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.	—
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: To return Peregrine ServiceCenter Web service requests that are sorted by the last modification or creation date, you must apply the following workaround:

In the Peregrine ServiceCenter Web service database table, under **System definition** > **Tables** > **<request table name>** > **Keys** > **New**, add a **not null:** **<last updated field name>** 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 Web Services Connector Settings

To connect to the IT Governance Web Services service desk application, you must first ensure that the necessary Web service proxy files reside in the **itgWsStubs.jar** file and that the **itgWsStubs.jar** file exists in the **<Change Control Management installation directory>/tomcat/webapps/ccm/WEB-INF/lib** directory. In addition, you must ensure that the Web service proxy version matches that of the IT Governance server. To do so, search for the IT Governance server version in the manifest files (**itgWsStubs.jar/META-INF/MANIFEST.MF**).

The following connector attributes must then be configured in the IT Governance 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 request type to be retrieved. Note that this field is case-sensitive.	—
parentRequestTypeName (mandatory, if the request is a task with a parent change)	The name of the IT Governance 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.	—

Property Name	Description	Default Value
password (mandatory)	The password with which Change Control Management connects to IT Governance. 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 Web service.	—

IT Governance RML Connector Settings

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

The following connector attributes must then be configured in the IT Governance 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 database.	—
userName (mandatory)	The user name with which Change Control Management connects to the IT Governance database.	—

Property Name	Description	Default Value
password (mandatory)	The password with which Change Control Management connects to the IT Governance 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
sqlQueryByLastUpdate (mandatory)	The SQL query that returns the change request set according to the requests’ last-update field value. 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 value. 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

Property Name	Description	Default Value
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
dbHelper-class-name	The class name used for the db helper.	com.mercury.onyx.sdi.sdk.db.DBHelperImpl
connectionProperties	The IT Governance database properties, in java.util.Properties format. For example: key1=value1; key 2=value2	oracle.jdbc.V8 Compatible=true
connectionPoolProperties	The IT Governance 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.	—
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.	—

Property Name	Description	Default Value
sqlQueryByLastUpdate (mandatory)	<p>The SQL query that returns the change request set according to the requests' last-update field value.</p> <p>To make use of a stored procedure, use the following syntax: { call <procedure_name> (?) }</p> <p>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.</p>	—
sqlQueryByCreationDate (mandatory)	<p>The SQL query that returns the change request set according to the requests' creation-date field value.</p> <p>To make use of a stored procedure, use the following syntax: { call <procedure_name> (?) }</p> <p>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.</p>	—
lastUpdatedFieldName (mandatory)	<p>The name of the column in the result set that contains the last-update field value.</p>	—
lastUpdatedFieldType (mandatory)	<p>One of the following values: time, timestamp, date, milliseconds, or seconds</p>	—

Property Name	Description	Default Value
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
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: <code>oracleDbConnector</code>	—
sqlQueryByLastUpdate (mandatory)	<p>The SQL query that returns the change request set according to the requests' last-update field value.</p> <p>To make use of a stored procedure, use the following syntax: <code>{ ? = call <procedure_name> (?) }</code></p> <p>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.</p>	—
sqlQueryByCreationDate (mandatory)	<p>The SQL query that returns the change request set according to the requests' creation-date field value.</p> <p>To make use of a stored procedure, use the following syntax: <code>{ ? = call <procedure_name> (?) }</code></p> <p>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.</p>	—

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 Attributes

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	—
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	—
idProperty (mandatory)	The property name of the ID field in the instance returned from the Web service.	—
serviceUrl (mandatory)	The Web service URL. This should be in the following format: http://<host name>/MSD-BIN/VTSSISA90.DLL/VTSS92/ITIL/svc?service=esql	—
userName (mandatory)	The user name with which Change Control Management connects to Mercury Service Desk.	—

Property Name	Description	Default Value
password (mandatory)	The password with which Change Control Management connects to Mercury Service Desk. Note that the password should be encrypted. For details on encrypting passwords, see Appendix A, “Password Encryption.”	—
fieldsToFetch	A comma-separated list of request fields to retrieve, or * to collect all request fields.	—

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. These files must reside in the adapter’s extension subdirectory (conf/<adapter name>.ext). For examples of conversion script files, see the sample scripts in the <Change Control Management installation directory>/examples directory.	—

Property Name	Description	Default Value
preFilterMethodName	The name of the pre-filter method in the script.	preFilter
postFilterMethodName	The name of the post-filter method in the script.	postFilter

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 value>

For example:

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

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, see 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)
```

- **preFilter.** This function filters the changes or tasks before they are converted, ensuring that no unnecessary requests are converted. 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. 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, IT Governance 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 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.

Predefined Generic Request Fields

Change Control Management generic requests contain the following set of predefined fields:

Field Name	Description
ActualEndTimeStamp (optional, but required for full Change Control Management functionality)	The time at which execution of the request was actually completed.
ActualStartTimeStamp (optional, but required for full Change Control Management functionality)	The time at which execution of the request actually began.
CreatedTimeStamp (mandatory)	The time at which the request was created.
Description	A detailed description of the request.
EstimatedRisk	Estimation of the risk level associated with the request (known as “impact” in some service desk applications).

Field Name	Description
<p>Link (optional, but required for full Change Control Management functionality)</p>	<p>A URL link to the original request in the service desk application. If the URL is simple (for example: http://labm1ccm01:18080/itg/web/knta/crt/RequestDetail.jsp?REQUEST_ID=30016), it can be easily created in the conversion script and associated with the Link field. If not, it is recommended that you get the URL from the service desk application.</p>
<p>ParentRefId (mandatory, if the request is a task with a parent change)</p>	<p>If the request is a task (meaning it has a parent change associated with it), this field must contain the service desk application ID number of the change.</p>
<p>PlannedEndTimeStamp (optional, but required for full Change Control Management functionality)</p>	<p>The time at which execution of the request is/was scheduled to be completed.</p>
<p>PlannedStartTimeStamp (optional, but required for full Change Control Management functionality)</p>	<p>The time at which execution of the request is/was scheduled to begin.</p>
<p>Priority</p>	<p>The request's priority level.</p>
<p>RefId (mandatory)</p>	<p>The reference ID number of the request in the service desk application.</p>
<p>ShortDescription</p>	<p>A summary of the request to be displayed, by default, in the Change Control Management application's Change Requests pane.</p>
<p>Status</p>	<p>The status of the request. In most cases, this field is generated by more than one field in the service desk application. (For example, a request can have an approval status and a workflow status.)</p>
<p>UpdatedTimeStamp (mandatory)</p>	<p>The time at which the request was last updated.</p>

Field Name	Description
Contact location	Geographic location of the contact person for the request.
Contact email	E-mail address of the contact person for the request.
Contact name	Name of the contact person for the request.
Contact phone	Phone number of the contact person for the request.

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.

This chapter describes:	On page:
Configuring the Collection of Converted Requests	72
Configuring the Analysis of Collected Requests	72
Configuring the Impact Analysis of Collected Requests	74
Configuring Notifications	74

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 from the **field.settings** file (for details, see “Analysis Rule Settings” on page 105). 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 defined pattern. You define a pattern using the following two elements:
 - ▶ **match-pattern.** Defines the pattern of the CI, 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>
 - ▶ **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.

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. These analysis rules may be referred to in the **field.settings** file. For details on specifying analysis rules in the **field.settings** file, see “Analysis Rule Settings” on page 105.

Configuring the Impact Analysis of Collected Requests

You use the `impact-calc-rule.js` script, located in the `<Change Control Management installation directory>/conf/impact-calculation.ext` directory and referenced from the `<Change Control Management installation directory>/conf/change-flow.settings` file, to configure the rules that determine the points at which Change Control Management calculates the impact of the CIs identified in the collected requests. For details on the API to be used in this script, see 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

Notifications are triggered as a result of an impact analysis calculation. Change Control Management sends notifications for certain impact severity levels, as a result of changes in the status of requests. You configure general notification properties, as well as the thresholds for which Change Control Management will send notifications, in the `<notifications>` section of the `<Change Control Management installation directory>/conf/change-flow.settings` file.

Configuring General Notification Properties

You can enable the notification mechanism and modify the notification sender and frequency in the top part of the `<notifications>` section.

To enable the Change Control Management notification mechanism:

Change the value of the `<notifications-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.

Note: For details on configuring the `mailSubject.ftl`, `mailbody-text.ftl`, `mailbody-html.ftl`, `user-mailbody-text.ftl`, `user-mailbody-html.ftl`, and `subject.ftl` files, located in the `notifications.ext` directory, refer to the `API_Reference.chm` file, located in the `docs/pdfs` directory of the Mercury Change Control Management CD-ROM.

Configuring Notification Rules

Under `<notification-rules>`, you configure the thresholds for which Change Control Management will send notifications.

Each notification rule contains the following elements:

- **summary.** Describes why the notification was sent. The notification summary is displayed in various places within a notification and appears as `notificationRuleSummary` within the notification templates.
- **status.** The status to which the request was changed. Change Control Management sends a notification for each request whose status changed to that specified in this element.
- **severity.** The bottom threshold for the impact severity level. Change Control Management sends a notification for a request with an impact severity of this level or above.

By default, Change Control Management sends notifications in the following cases:

- ▶ The status of a change request changed to “Assigned” and the impact severity level of the request is “High” or a level above “High.”
- ▶ The status of a change request changed to “Pending Approval” and the impact severity level of the request is “Low” or a level above “Low.”
- ▶ The status of a change request changed to “Approved” and the impact severity level of the request is “Medium” or a level above “Medium.”

Note: The statuses and severity levels used here must correspond to those defined in the <**Change Control Management installation directory**>/conf/enumerations.settings file. For details on configuring enumeration fields, see “Customizing Change Control Management Fields” on page 38.

6

Configuring the Change Control Management Environment

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 predefined Change Control Management log file properties, if required.

Note: The Change Control Management application server name and address are configured automatically during the Change Control Management installation process.

This chapter describes:	On page:
Configuring the Change Control Management Database or User Schema	78
Configuring the SMTP Mail Server	79
Configuring Log File Properties	80

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.

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
```

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 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. 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.”

7

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 6.1, and how to reconfigure the default Change Control Management-Mercury Application Mapping integration settings, if required.

Note: This chapter uses Mercury Application Mapping 6.1 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	84
Configuring Settings for Mercury Application Mapping 6.1	86
Configuring Change Control Management-Mercury Application Mapping Integration Settings	87

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 or 6.1—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 (version 6.1 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.
username	The user name required for the Change Control Management user to connect to Mercury Application Mapping.

Property	Description
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 (version 6.1 only)	<p>The type of Mercury Application Mapping installation you have. The following installation types exist:</p> <ul style="list-style-type: none"> ▶ 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 (version 6.1 only)	<p>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.</p> <p>Note: You define the view-refresh-schedule using cron expressions.</p>

Configuring Settings for Mercury Application Mapping 6.1

When working with Mercury Application Mapping 6.1, 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 6.1:

- 1 Copy the `<Change Control Management installation directory>/MAM/6.1/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. 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 the **appilogConfig.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 configuration settings discussed in the previous sections, 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)
- ▶ 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 in the `<cmdb-synchronizations>` section of the `mam-integration.settings` file:

```
<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 in the `<cmdb-synchronizations>` section of the `mam-integration.settings` file:

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

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>
```

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_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.

8

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	94
Configuring Change Request Field Settings	95
Configuring Default Change Requests Pane Display Settings	106
Configuring Default Request Details Tab Display Settings	107
Configuring Default Filter Display Settings	109
Configuring Dashboard Settings	110
Configuring Enumeration Field Display Settings	112

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

Each change request field for which you want to view data in the Change Control Management application must be defined in the `<Change Control Management installation directory>/conf/field.settings` file. By default, this file contains the required settings for all the standard change request fields and in general, it is recommended that these predefined settings not be modified. However, you can use the `field.settings` file to define additional customized fields for which you want to view data in the Change Control Management application.

Notes:

- ▶ Several examples of customized fields are provided at the bottom of the `field.settings` file.
- ▶ An XML schema, `fields_settings.xsd`, is available to assist you in the customization of the `field.settings` file. Using an XML editor that supports `.xsd` files to customize the `field.settings` file enables you to minimize the number of customization errors that can be made.

Below is an example of a change request field definition, which includes the following:

- ▶ a general definition section
- ▶ a section defining the way in which the field will appear in the Change Requests pane
- ▶ a section defining the way in which the field will appear in the Request Details tab
- ▶ a section defining the way in which the field will appear in the filter view
- ▶ a section defining the analysis rules that apply to the field

```

<request-field>
  <name>created</name>
  <type>date</type>
  <category/>
  <gridable>true</gridable>
  <sortable>true</sortable>
  <filterable>true</filterable>
  <predefined>true</predefined>
  <grid-display>
    <header>properties-file</header>
    <header-tip>properties-file</header-tip>
    <value-field>createdTimeStamp</value-field>
    <value-presentation>date</value-presentation>
    <tooltip-field/>
    <resizeable>true</resizeable>
    <preferred-width>70</preferred-width>
  </grid-display>
  <details-display>
    <label>properties-file</label>
    <label-tooltip>properties-file</label-tooltip>
    <value-field>changeVO.createdTimeStamp</value-field>
    <value-presentation>date</value-presentation>
  </details-display>
  <filter-display>
    <label>properties-file</label>
    <value-presentation>combo</value-presentation>
    <label-tooltip>properties-file</label-tooltip>
    <filter-values>
      <filter-value>
        <label>High</label>
        <value>1</value>
      </filter-value>
    </filter-values>
  </filter-display>
  <analysis-rules>
    <analysis-rule>
      <rule>ruleName</rule>
      <level>levelType</level>
    </analysis-rule>
  </analysis-rules>
</request-field>

```

The following tables explain each element within the change request field definition:

Element	Description
name	<p>The name of the change request field.</p> <p>The names of standard change request fields should not be changed. If you are defining a customized field, the name should be in the format <code>[a-zA-Z][a-zA-Z_]*</code>. Note that when you define a customized field, a new column is added to the Change Control Management database for this field.</p>
type	<p>The change request field's value type. The following three types can be used:</p> <ul style="list-style-type: none"> ▶ text. The request field's value is a simple text string. You can specify text format for this element, or parameters that contain the names of other fields from the <code>fields.settings</code> file, surrounded by two percentage signs on each side of the field. For example, you can use the parameter <code>%%contact-person%%</code> to return the name of the contact person for the request. ▶ bool. The request field's value is boolean (true/false; yes/no; 1/0).

Element	Description
<p>type (cont'd)</p>	<p>► date. The request field's value is a date. In specifying the way in which the date should be displayed, you can make use of letter patterns containing the following letters:</p> <ul style="list-style-type: none"> •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 <p>For example, to display Sat 04 Mar 2006 09:43AM, you would use the following date format: EEE DD MMM YYYY LL:NNA</p> <p>Note: Do not change the type of a standard change request field.</p>
<p>category</p>	<p>The user-defined filter category in which the customized change request field is to be included.</p> <p>Since the filter categories and the change request 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 create a new filter category for the customized field.</p>

Element	Description
gridable	<p>Indicates whether the change request field can be displayed in the Change Requests pane (true/false).</p> <p>Since the Change Requests pane incorporates many of the standard change request fields, it is strongly recommended that you not change the gridable value for standard change request fields.</p>
sortable	<p>Indicates whether you will be able to sort according to the change request field in the Change Control Management application (true/false).</p>
filterable	<p>Indicates whether you will be able to filter according to the change request field in the Change Control Management application (true/false).</p>
predefined	<p>Indicates whether the change request field is a standard request field (true/false). If you are defining a customized field, you must enter false for this element.</p>

Change Requests Pane Display Settings

Element	Description
header	<p>The text to appear in the header of the column in which the change request field value is to be displayed. You can enter text for this element, or properties-file if you want to reference the <Change Control Management installation directory>/conf/fields-labels.properties file for the column header. Note that if you reference the properties file, the property name in the file should be in the following format:</p> <p>changes.details.grid.REQUEST_FIELD_NAME.colHeader</p>
header-tip	<p>The tooltip for the column header, describing the column. You can enter text for this element, or properties-file if you want to reference the <Change Control Management installation directory>/conf/fields-labels.properties file for the column header tooltip. Note that if you reference the properties file, the property name in the file should be in the following format:</p> <p>changes.details.grid.REQUEST_FIELD_NAME.headerTip</p> <p>Note: If this element is left unspecified, the name of the header is displayed as the tooltip.</p>
value-field	<p>The change request sub-field whose value you want to display in the column defined above. This is generally applicable only to standard change request fields and not customized fields.</p> <p>A sub-field is indicated using the ChangeVO Java class for standard fields. For example, if several contact details are listed for each contact person (name, phone number, address), ChangeVO.contact.name is used to indicate that the name of the contact person should be displayed.</p>

Element	Description
value-presentation	<p>The type of value to be displayed for the change request field. The following options can be used:</p> <ul style="list-style-type: none"> ▶ text. The value is displayed as simple text. For details on the formats that can be used, see the explanation of the type element on page 97. ▶ date. The value is displayed as a date. For details on the formats that can be used, see the explanation of the type element on page 98. ▶ bool. The value is displayed as a check box (supports true/false, yes/no, and 1/0). ▶ severity. The value is displayed as an icon. ▶ priority. The value is displayed as text. ▶ status. The value is displayed as text. <p>Note that severity, priority, and status may not be used for customized fields.</p>
tooltip-field	<p>The name of the change request field whose value you want to display as the tooltip for the field.</p>
tooltip-presentation	<p>The format in which the tooltip is displayed. Possible values for this element are:</p> <ul style="list-style-type: none"> ▶ text. Simple text is displayed in the tooltip. For details on the formats that can be used, see the explanation of the type element on page 97. ▶ date. A date is displayed in the tooltip. For details on the formats that can be used, see the explanation of the type element on page 98.
resizeable	<p>Indicates whether the width of the column can be modified.</p>
preferred-width	<p>The default column width, in pixels.</p>

Request Details Tab Settings

Element	Description
label	<p>The text to appear as the label preceding the displayed change request field value. You can enter text for this element, or properties-file if you want to reference the <Change Control Management installation directory>/conf/fields-labels.properties file for the label. Note that if you reference the properties file, the property name in the file should be in the following format:</p> <p>changes.details.detailsTab.REQUEST_FIELD_NAME.label</p>
label-tooltip	<p>The tooltip for the label, describing the change request field. You can enter text for this element, or properties-file if you want to reference the <Change Control Management installation directory>/conf/fields-labels.properties file for the tooltip. Note that if you reference the properties file, the property name in the file should be in the following format:</p> <p>changes.details.detailsTab.REQUEST_FIELD_NAME.tooltip</p>
value-field	<p>The change request sub-field whose value you want to display for the label defined above. This is generally applicable only to standard change request fields and not customized fields.</p> <p>A sub-field is indicated using the ChangeVO Java class for standard fields. For example, if several contact details are listed for each contact person (name, phone number, address), ChangeVO.contact.name is used to indicate that the name of the contact person should be displayed.</p>

Element	Description
value-presentation	<p>The type of value to be displayed for the change request field. The following options can be used:</p> <ul style="list-style-type: none"> ▶ text. The value is displayed as simple text. For details on the formats that can be used, see the explanation of the type element on page 97. ▶ date. The value is displayed as a date whose format is set in a configuration file. For details on the formats that can be used, see the explanation of the type element on page 98. ▶ bool. The value is displayed as a check box (supports true/false, yes/no, and 1/0). ▶ long-text. The value is displayed within a text box, with the change request field's label appearing above the displayed value. ▶ link. The value is displayed as text which, when clicked, will open a page at a specific URL. Note that when you specify link, the value-field value is displayed as the URL.

Filter View Settings

Element	Description
label	<p>The text to appear as the label preceding the filter options available for the change request field. You can enter text for this element, or properties-file if you want to reference the <code><Change Control Management installation directory>/conf/fields-labels.properties</code> file for the label. Note that if you reference the properties file, the property name in the file should be in the following format:</p> <pre>filters.constraints.REQUEST_FIELD_CATEGORY.REQUEST_FIELD_NAME.label</pre>

Element	Description
label-tooltip	<p>The tooltip for the label, describing the change request field. You can enter text for this element, or properties-file if you want to reference the <code><Change Control Management installation directory>/conf/fields-labels.properties</code> file for the tooltip. Note that if you reference the properties file, the property name in the file should be in the following format: <code>filters.constraints.REQUEST_FIELD_CATEGORY.REQUEST_FIELD_NAME.tooltip</code></p>
value-presentation	<p>The way in which the change request field filter options are displayed. The following options can be used:</p> <ul style="list-style-type: none"> ▶ text. A simple text input box is provided for filtering. ▶ combo. A selection box with one or more options is provided for filtering. You set the options available in the selection box using the filter-values element. ▶ combo-editable. As in the combo option, a selection box with one or more options is provided for filtering. In addition, you can edit the values that appear in the selection box. ▶ bool. A check box (supporting true/false, yes/no, and 1/0) is provided for filtering.
filter-values	<p>The values to appear in the selector, if you set the value-presentation element to combo. These can be structured using either of the following options:</p> <ul style="list-style-type: none"> ▶ label. The text that will appear in the selection box. You can enter the text itself for this element, or properties-file if you want to reference the <code><Change Control Management installation directory>/conf/fields-labels.properties</code> file for the text. Note that if you reference the properties file, the property name in the file should be in the following format: <code>filters.constraints.REQUEST_FIELD_CATEGORY.REQUEST_FIELD_NAME.REQUEST_FIELD_VALUE.label</code> ▶ value. The actual value of the change request field. Note that this should be the same as the value stored in the database for the change request field.

Note: You cannot modify any of the settings for the predefined filter categories.

Analysis Rule Settings

Element	Description
rule	<p>The name of the analysis rule in the change-flow.settings file that is to be applied to the change request field. For details on analysis rules, see “Configuring the Analysis of Collected Requests” on page 72.</p> <p>To apply all the analysis rules listed in the change-flow.settings file to the change request field, enter everything as the value of the rule element. Note that the value everything does not include the mam-ticket or mam-object-id analysis rules. These must be explicitly specified in separate analysis rules.</p>
level	<p>The level—change or task—at which to apply the above rule. The following three values can be used for this element:</p> <ul style="list-style-type: none"> ▶ 1. The above rule applies to the change request field only if the request field belongs to a change. ▶ 2. The above rule applies to the change request field only if the request field belongs to a task. ▶ all. The above rule applies to all requests in which the change request field appears.

Configuring Default Change Requests Pane Display Settings

The `<default-grid-display>` section of the `<Change Control Management installation directory>/conf/field.settings` file contains a list of change request fields to be displayed in the Change Requests pane. It also defines the number of rows to be displayed in the pane.

Below is an example of the `<default-grid-display>` section of a `field.settings` file:

```
<default-grid-display>
  <number-of-rows>20</number-of-rows>
  <display-fields>
    <display-field>
      <name>summary</name>
    </display-field>
    <display-field>
      <name>severity</name>
    </display-field>
    <display-field>
      <name>origin-reference-id</name>
    </display-field>
    <display-field>
      <name>created</name>
    </display-field>
    <display-field>
      <name>priority</name>
    </display-field>
    <display-field>
      <name>status</name>
    </display-field>
    <display-field>
      <name>contact-person</name>
    </display-field>
  </display-fields>
</default-grid-display>
```

To add a field to the Change Requests pane display:

Add a `<display-field>` element whose `<name>` element contains the name of the change request field as defined in the `<request-fields>` section of the `field.settings` file. For example, to view the Project Name customized field, add the following `<display-field>` element:

```
<display-field>
  <name>project-name</name>
</display-field>
```

To reconfigure the number of rows to be displayed in the Change Requests pane:

In the `<number-of-rows>` element, change the value of 20 to the required value.

Note: This setting may be overridden by the user in the User Settings tab. For details on the User Settings tab, refer to the *Mercury Change Control Management User's Guide*.

Configuring Default Request Details Tab Display Settings

The `<default-details-display>` section of the `<Change Control Management installation directory>/conf/field.settings` file contains a list of change request fields to be displayed in the Request Details tab. It also defines the number of columns to be displayed in the tab and the change request fields to be included in each column.

Below is an example of the `<default-details-display>` section of a `field.settings` file:

```
<default-details-display>
  <columns>
    <column>
      <display-fields>
        <display-field>
          <name>service-desk</name>
        </display-field>
        <display-field>
          <name>contact-person</name>
        </display-field>
        <display-field>
          <name>priority</name>
        </display-field>
        <display-field>
          <name>estimated-risk</name>
        </display-field>
        <display-field>
          <name>created</name>
        </display-field>
        <display-field>
          <name>started</name>
        </display-field>
      </display-fields>
    </column>
    <column>
      <display-fields>
        <display-field>
          <name>description</name>
        </display-field>
      </display-fields>
    </column>
  </columns>
</default-details-display>
```


To add a field to the Request Details tab:

Add a `<display-field>` element whose `<name>` element contains the name of the change request field as defined in the `<request-fields>` section of the `field.settings` file. For example, to view the Project Name customized field, add the following `<display-field>` element:

```
<display-field>
  <name>project-name</name>
</display-field>
```

Ensure that you add the `<display-field>` element within the correct column element so that it is displayed in the required column in the Request Details tab.

To add a column to the Request Details tab:

Add a `<column>` element that includes the fields you want the column to display in the Request Details tab. The number of columns displayed in the tab is determined by the number of `<column>` elements defined in the `<default-details-display>` section of the `field.settings` file.

Configuring Default Filter Display Settings

The `<default-filter-display>` section of the `<Change Control Management installation directory>/conf/field.settings` file contains a list of all the change request fields to be displayed in the customized filter categories – that is, in all filter categories except for the three predefined categories (General, Applications, and Time Conditions).

By default, the `<default-filter-display>` section of a `field.settings` file is empty:

```
<default-filter-display>
  <display-fields/>
</default-filter-display>
```

To add a field to one of the customized filter categories:

Add a **<display-field>** element whose **<name>** element contains the name of the change request field as defined in the **<request-fields>** section of the **field.settings** file. For example, to add the Project Name field to a customized filter category, add the following **<display-field>** element:

```
<display-field>
  <name>project-name</name>
</display-field>
```

Note that each field you add will be displayed within the filter category defined for this field in the **<request-fields>** section of the **field.settings** file.

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 **Dashboar_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.settings** file. For details on configuring the **enumeration-labels.settings** file, see “Configuring Enumeration Field Display Settings” on page 112.

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.settings** file. For details on configuring the **enumeration-labels.settings** file, see “Configuring Enumeration Field Display Settings” on page 112.

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.settings` 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, requests are referred to as “changes” and sub-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.settings** file:

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


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) Pacific/Apia
(GMT -11) MIT	(GMT -11) Pacific/Pago_Pago
(GMT -10) Pacific/Tahiti	(GMT -10) Pacific/Fakaofu
(GMT -10) Pacific/Honolulu	(GMT -10) HST
(GMT -10) America/Adak	(GMT -10) Pacific/Rarotonga
(GMT -9) Pacific/Marquesas	(GMT -9) Pacific/Gambier
(GMT -9) America/Anchorage	(GMT -9) AST
(GMT -8) Pacific/Pitcairn	(GMT -8) America/Vancouver
(GMT -8) America/Tijuana	(GMT -8) America/Los_Angeles
(GMT -8) PST	(GMT -7) America/Dawson_Creek
(GMT -7) America/Phoenix	(GMT -7) PNT
(GMT -7) America/Edmonton	(GMT -7) America/Mazatlan
(GMT -7) America/Denver	(GMT -7) MST
(GMT -6) America/Belize	(GMT -6) America/Regina
(GMT -6) Pacific/Galapagos	(GMT -6) America/Guatemala
(GMT -6) America/Tegucigalpa	(GMT -6) America/El_Salvador
(GMT -6) America/Costa_Rica	(GMT -6) America/Winnipeg
(GMT -6) Pacific/Easter	(GMT -6) America/Mexico_City
(GMT -6) America/Chicago	(GMT -6) CST
(GMT -5) America/Porto_Acre	(GMT -5) America/Bogota
(GMT -5) America/Guayaquil	(GMT -5) America/Jamaica
(GMT -5) America/Cayman	(GMT -5) America/Managua
(GMT -5) America/Panama	(GMT -5) America/Lima
(GMT -5) America/Indianapolis	(GMT -5) IET
(GMT -5) America/Nassau	(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/Kuala_Lumpur
(GMT +8) Asia/Manila	(GMT +8) Asia/Singapore
(GMT +8) Asia/Taipei	(GMT +8) Asia/Shanghai
(GMT +8) CTT	(GMT +8) Asia/Ulan_Bator
(GMT +8) Asia/Irkutsk	(GMT +9) Asia/Jayapura
(GMT +9) Asia/Pyongyang	(GMT +9) Asia/Seoul
(GMT +9) Pacific/Palau	(GMT +9) Asia/Tokyo
(GMT +9) JST	(GMT +9) Asia/Yakutsk
(GMT +9) Australia/Darwin	(GMT +9) ACT
(GMT +9) Australia/Adelaide	(GMT +9) Australia/Broken_Hill
(GMT +10) Australia/Hobart	(GMT +10)
	Antarctica/DumontDURville
(GMT +10) Pacific/Truk	(GMT +10) Pacific/Guam
(GMT +10) Pacific/Saipan	(GMT +10) Pacific/Port_Moresby
(GMT +10) Australia/Brisbane	(GMT +10) Asia/Vladivostok
(GMT +10) Australia/Sydney	(GMT +10) AET
(GMT +10) Australia/Lord_Howe	(GMT +11) Pacific/Ponape
(GMT +11) Pacific/Efate	(GMT +11) Pacific/Guadalcanal
(GMT +11) SST	(GMT +11) Pacific/Noumea
(GMT +11) Asia/Magadan	(GMT +11) Pacific/Norfolk
(GMT +12) Pacific/Kosrae	(GMT +12) Pacific/Tarawa
(GMT +12) Pacific/Majuro	(GMT +12) Pacific/Nauru
(GMT +12) Pacific/Funafuti	(GMT +12) Pacific/Wake
(GMT +12) Pacific/Wallis	(GMT +12) Pacific/Fiji
(GMT +12) Antarctica/McMurdo	(GMT +12) Asia/Kamchatka
(GMT +12) Pacific/Auckland	(GMT +12) NST
(GMT +12) Pacific/Chatham	(GMT +13) Pacific/Enderbury
(GMT +13) Pacific/Tongatapu	(GMT +13) Asia/Anadyr
(GMT +14) Pacific/Kiritimati	

