OPTIMIZE

MERCURY BUSINESS AVAILABILITY CENTER™

Getting Started with Mercury Business Availability Center

MERCURY™

BUSINESS TECHNOLOGY OPTIMIZATION

Mercury Business Availability Center

Getting Started

Version 6.2

Document Release Date: June 20, 2006

MERCURY™

Mercury Business Availability Center, Version 6.2
Getting Started with Mercury Business Availability Center

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

© 2005-2006 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.

AMLIBGS6.2/01

Table of Contents

Welcome to Getting Started with Mercury Business Availability Center v
How This Guide Is Organized v
Who Should Read This Guide vi
Recommended Reading Lists vii
Typographical Conventions xi

Chapter 1: Introduction to Mercury Business Availability Center 1
About Mercury Business Availability Center 1
Alignment with ITIL 2

Chapter 2: Getting Started Roadmap 5

Chapter 3: Getting Help 9
Mercury Business Availability Center Readme File 10

Chapter 4: Understanding the Mercury Business Availability Center Platform and Components 11
The Mercury Business Availability Center Architecture 12
Overview of Applications 16

Chapter 5: Deployment Planning 21
Deployment Planning Checklist 22

Chapter 6: Quick Installation Guide 23
About the Quick Installation Guide 23
Prerequisites 25
Installation 28
After Installation 30

Chapter 7: Accessing and Navigating Mercury Business Availability Center 31
Accessing Mercury Business Availability Center 31
Navigating Mercury Business Availability Center 39
Troubleshooting Mercury Business Availability Center Login 42

Chapter 8: Basic Administration Checklists 47
Platform Administration Checklist 48
CMDB Administration Checklist 49
Monitor Administration Checklist 51
Application Administration Checklist 54

Chapter 9: How Do I...? A Task Reference for Administrators 55
How Do I Build and Maintain My Mercury Business Availability Center System? 57
How Do I Set Up Users and Permissions? 60
How Do I Reflect My IT Environment in Mercury Business Availability Center? 62
How Do I Collect Data on the Performance of a Specific Business Process? 65
How Do I Collect Data on the Performance of an IT Resource? 68
How Do I Collect Data on Real User Traffic Accessing a Specific Application? 70
How Do I Collect Data on the Performance of an Application Being Accessed by Specific Users? 72
How Do I Integrate Data from Third-Party Sources (EMS Data) into Mercury Business Availability Center? 74
How Do I View My Already Created Monitors in Dashboard? 78
How Do I Set Up SLAs and Track Their PNR KPIs in Dashboard? 80
How Do I Set Up a Report and Alert Delivery System? 82
How Do I Customize the Way Mercury Business Availability Center Displays My Views in Dashboard? 84
How Do I Customize Dashboard Repository Entities to Model My Business World? A Sample Scenario 86
Flowchart Legend 88

Chapter 10: Using the Mercury Business Availability Center Documentation Library 89
Working with the Documentation Library 90
Documentation Library Guides 93
Navigating the Documentation Library 98
Updating the Documentation Library 99
Accessing Additional Online Resources 101

Index 105

Welcome to Getting Started with Mercury Business Availability Center

Welcome to Mercury Business Availability Center. This guide helps you implement Mercury Business Availability Center in your organization by providing a roadmap, checklists, and other key information.

How This Guide Is Organized

The guide contains the following chapters:

Chapter 1 Introduction to Mercury Business Availability Center

Introduces the Mercury Business Availability Center platform and applications.

Chapter 2 Getting Started Roadmap

Provides a basic step-by-step roadmap for getting up and running with Mercury Business Availability Center.

Chapter 3 Getting Help

Describes help resources that are available to Mercury customers.

Chapter 4 Understanding the Mercury Business Availability Center Platform and Components

Provides an overview of the Mercury Business Availability Center platform and components.

Chapter 5 Deployment Planning

Describes, in checklist format, some of the basic issues that should be considered prior to Mercury Business Availability Center software installation.

Chapter 6 Quick Installation Guide

Describes, in checklist format, basic Mercury Business Availability Center server installation instructions.

Chapter 7 Accessing and Navigating Mercury Business Availability Center

Describes how to access and navigate Mercury Business Availability Center and how to troubleshoot login problems.

Chapter 8 Basic Administration Checklists

Describes, in checklist format, basic platform and monitoring configuration and administration tasks.

Chapter 9 How Do I...? A Task Reference for Administrators

Describes step-by-step process flows for common administrative tasks performed in Mercury Business Availability Center.

Chapter 10 Using the Mercury Business Availability Center Documentation Library

Describes how to use, navigate, and update the Mercury Business Availability Center Documentation Library.

Who Should Read This Guide

This guide is intended for the following users of Mercury Business Availability Center:

- Mercury Business Availability Center administrators

Readers of this guide should be knowledgeable and highly skilled in enterprise system administration.

Recommended Reading Lists

The lists below describe the guides in the Mercury Business Availability Center Documentation Library that are recommended reading for the different users of Mercury Business Availability Center. These lists can be distributed to staff as required. For a description of each guide, see "Documentation Library Guides" on page 93.

Reading lists for the following users are described below:

- Mercury Business Availability Center Administrators. See page vii.
- Database Administrators. See page vii.
- Security Administrators. See page vii.
- Data Collector Administrators. See page viii.
- Script Developers. See page ix.
- Platform Administrators. See page ix.
- Application Administrators. See page ix.
- End Users. See page x.

Mercury Business Availability Center Administrators

- All books in Documentation Library

Database Administrators

- Glossary
- Preparing the Database Environment
- Reference Information
- Working in an I18N Environment
- Troubleshooting Resources

Security Administrators

- Glossary
- Hardening the Platform

Data Collector Administrators

- Glossary
- Data Collector Overview
- Business Process Monitor Administration
- Client Monitor Administration
- SiteScope Administration
- Real User Monitor Administration
- Script Recording Tips
- Using Mercury Virtual User Generator
- Using Client Monitor Recorder
- Working with the CMDB
- IT Universe Manager Administration
- View Manager Administration
- Discovery Manager Administration
- Discovery Manager Tutorial
- Source Manager Administration
- CI Type Manager Administration
- Working with Monitor Administration
- End User Management Data Collector Configuration
- Managing SiteScope
- Configuring SiteScope Monitors
- Configuring SiteScope Alerts
- Configuring SiteScope Reports
- Advanced Monitor Options
- Application Administration
- Reference Information
- Integrating with Third-Party Applications

Script Developers

- Glossary
- Script Recording Tips
- Using Mercury Virtual User Generator
- Using Client Monitor Recorder
- Reference Information

Platform Administrators

- Glossary
- Platform Administration
- Working with the CMDB
- IT Universe Manager Administration
- View Manager Administration
- Discovery Manager Administration
- Discovery Manager Tutorial
- Source Manager Administration
- CI Type Manager Administration
- Application Administration
- Reference Information
- Integrating with Third-Party Applications

Application Administrators

- Glossary
- Working with the CMDB
- IT Universe Manager Administration
- View Manager Administration
- Discovery Manager Administration
- Discovery Manager Tutorial

- Source Manager Administration
- CI Type Manager Administration
- Application Administration
- Reference Information
- Integrating with Third-Party Applications

End Users

- Glossary
- Working with Applications
- Using Dashboard
- Using Service Level Management
- Using End User Management
- Using System Availability Management
- Using Application Performance Lifecycle

Typographical Conventions

The guides that comprise the Documentation Library use the following typographical conventions:

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

1

Introduction to Mercury Business Availability Center

Welcome to Mercury Business Availability Center. Before you install Mercury Business Availability Center or read any other Mercury Business Availability Center documentation, it is recommended that you read this short introduction to Mercury Business Availability Center, which includes a description of the new concepts that are a result of Mercury Business Availability Center's alignment with ITIL, starting from version 6.0.

About Mercury Business Availability Center

Mercury Business Availability Center helps companies to optimize the performance and availability of applications in production and proactively resolve problems when they arise, thus assisting critical production applications to perform as required and deliver business results.

Mercury Business Availability Center helps customers model their business processes and services by providing a framework for mapping the complex and dynamic dependencies between applications and their supporting infrastructure. Mercury Business Availability Center helps customers optimize business availability by proactively detecting problems in order to prioritize problem resolution based on business impact and service level compliance.

Mercury Business Availability Center consists of an integrated set of applications for real-time performance and availability monitoring from a business perspective, service level management, end-user management, system availability management, and custom reporting. Mercury Business Availability Center is based on a common foundation of shared workflow, administration and reporting services, shared assets, and expertise.

Mercury Business Availability Center helps customers to reduce mean time to detection (MTTD) and end-user downtime by proactively detecting application performance and availability problems—assisting in escalation of problems to the right department at the right priority, as well as isolation and resolution of performance problems before service-level objectives are breached. This helps organizations toward the goal of the maximization of value of IT operations and reduction of Total Cost of Ownership (TCO) of IT infrastructure.

Alignment with ITIL

Several new concepts in Mercury Business Availability Center come as a result of the alignment with the Information Technology Infrastructure Library (ITIL) methodology. ITIL is the most widely accepted methodology for IT service management in the world. In fact, it is quite possible that your organization is already following the ITIL methodology.

What is ITIL?

Originally developed by the Office of Government Commerce, a branch of the British Government, ITIL is a cohesive set of well-defined best practices for IT processes drawn from the public and private sectors internationally. ITIL best practices aim to provide the following benefits:

- Improved communications between IT, businesses, and customers
- Increased IT productivity
- Reduced IT costs
- Better management of risk
- Higher levels of customer satisfaction

For more information on ITIL, refer to the following Internet resources:

- http://www.itilpeople.com
- http://www.ogc.gov.uk (click Programmes & Projects and then click ITIL)

Note: The main ITIL concepts and terminology used in Mercury Business Availability Center are defined in the *Glossary*.

ITIL in Mercury Business Availability Center

Mercury Business Availability Center introduces the concept of the Mercury Universal Configuration Management Database (CMDB). The Mercury Universal CMDB stores information on services, their components or configuration items, details about configuration item attributes, the history of each configuration item, and details of the relationships between configuration items. A configuration item (CI) is a component that makes up a part of the IT environment. A CI can be a line of business, business process, application, server hardware, or a service that is provided by your IT organization. A CI can also be a logical container that includes multiple CIs. A CI Type (CIT) is the type of each CI within the IT environment.

The IT Universe Concept

If you provide an application to your company's employees to manage their own retirement accounts, then you are also providing a service. Let us call this service "Employee Self Help." To provide this service, you create an application that runs on a server and connects to a database. In your environment, you may provide many such services that depend on many applications and databases that utilize a variety of server and network hardware. All these services, applications, and hardware are interconnected to form what is called in Mercury Business Availability Center the IT universe.

In Mercury Business Availability Center, you start by defining a model of your company's IT Universe. To manage your company's IT Universe model, you create service views (views). Views enable you to divide up the IT Universe model into logical entities for monitoring. The IT universe model then becomes the foundation for the management functions provided by Mercury Business Availability Center applications.

Having a defined model of the organization's IT universe can then help you, for example, to see what application is being monitored by which Business Process Monitor, or to determine whether a server problem, detected by SiteScope, affects other CIs as well—for example, whether the Employee Self-Help service described above suffered service outages due to a problem with its database server.

Applying these new Mercury Business Availability Center concepts can help you to more efficiently and effectively manage and deliver IT services to your end users and customers.

2

Getting Started Roadmap

This chapter provides a basic step-by-step roadmap for getting up and running with Mercury Business Availability Center.

All guides referred to are located in the **Documentation\pdfs** directory on the Mercury Business Availability Center Documentation and Utilities CD-ROM and from the PDFs tab of the Mercury Business Availability Center Documentation Library.

Note to customers upgrading to Mercury Business Availability Center 6.2: For details on upgrading, see "Upgrading Mercury Business Availability Center" in *Deploying Servers*.

---

1 Register your copy of Mercury Business Availability Center.

Register your copy of Mercury Business Availability Center to gain access to technical support and information on all Mercury products. You will also be eligible for updates and upgrades. You can register your copy of Mercury Business Availability Center on Mercury's Customer Support Web site (support.mercury.com).

2 Read about where to get help.

Learn about the various sources of assistance, including Mercury Services and Mercury Customer Support, as well as the Mercury Business Availability Center Documentation Library. For details, see page 9.

3 Learn about the Mercury Business Availability Center platform and components.

Learn about the servers and components that power the Mercury Business Availability Center system. For details, see page 11.

4 Plan your Mercury Business Availability Center deployment.

Create a complete deployment plan prior to installing Mercury Business Availability Center software. Use the Deployment Planning checklist on page 22 to assist you. For in-depth deployment planning best practices, consult your Mercury Services representative.

5 Install Mercury Business Availability Center servers.

Use the Quick Installation Guide to gain a basic understanding of the steps involved in deploying Mercury Business Availability Center servers. For details, see page 23. When installing, it is recommended that you follow the instructions in *Deploying Servers*. If deploying Mercury Business Availability Center securely, see *Hardening the Platform*. You can also use the step-by-step process flow "How Do I Build and Maintain My Mercury Business Availability Center System?" to guide you through the deployment process. For details, see page 57.

6 Log in to Mercury Business Availability Center and initiate system administration.

Log into the Mercury Business Availability Center Web interface using a Web browser, as instructed on page 31. Use the Basic Administration Checklists to guide you through basic platform, CMDB, and monitor administration tasks. For details, see page 47. Use the step-by-step process flows to assist you in understanding the overall processes involved in performing key administrative tasks. For details, see page 55.

7 Configure Dashboard and other licensed applications to conform to your organization's monitoring and deployment plans.

Use the Application Administration Checklist to gain a basic understanding of the steps involved in configuring Mercury Business Availability Center applications. For details, see page 54. Use the step-by-step process flows to assist you in understanding the overall processes involved in performing key administrative tasks. For details, see page 55.

8 Roll out Mercury Business Availability Center to business and systems users.

Once the Mercury Business Availability Center system is up and running with defined users and incoming monitor data, begin the process of educating business and systems users on how to access and use Mercury Business Availability Center reporting and alerting functionality.

For complete details on using and administering Mercury Business Availability Center, use the guides that comprise the Documentation Library. For details on using the Documentation Library see "Using the Mercury Business Availability Center Documentation Library" on page 89.

3

Getting Help

To assist Mercury customers in the process of planning and deploying Mercury Business Availability Center, the following resources are available:

- **Documentation Library**. The Mercury Business Availability Center Documentation Library provides complete information on deploying, administering, and using the Mercury Business Availability Center platform and applications. For details on using and updating the Documentation Library, see "Using the Mercury Business Availability Center Documentation Library" on page 89.
- **Mercury Services**. Customers can acquire services through the Mercury Services organization that guide and assist in planning a Mercury Business Availability Center deployment and tailoring Mercury Business Availability Center to their specific environment. For details, contact your Mercury representative.
- **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.
- **Mercury Customer Support**. Registered customers can use the resources found on the Mercury Customer Support Web site (support.mercury.com), including the Mercury Customer Support Knowledge Base and user forums.

  For urgent issues (such as an inoperative production system), Mercury Customer Support can be contacted directly. Contact information is listed on the Mercury Customer Support Web site.

  Mercury Managed Services customers can click the **E-mail Managed Services Support** link from the Help menu to send an e-mail directly to Mercury Managed Services support.

Mercury Business Availability Center Readme File

The Mercury Business Availability Center readme file, readme62.html, provides a list of version limitations and last-minute updates. The readme file is included on the Mercury Business Availability Center CD-ROMs, in the following locations:

- the root directory of the Mercury Business Availability Center Setup CD-ROM.
- the **Documentation\readme** directory on the Mercury Business Availability Center Documentation and Utilities CD-ROM.

Note: You can also access the most updated readme file from the Mercury Business Availability Center Documentation area on the Mercury Customer Support Web site.

4

Understanding the Mercury Business Availability Center Platform and Components

The Mercury Business Availability Center platform consists of proprietary servers, data collectors, and scripting tools, as well as third-party servers such as database and mail servers. These components run the Mercury Business Availability Center business user and administrator applications. This chapter provides an overview of the Mercury Business Availability Center platform and components.

This chapter describes:	On page:
The Mercury Business Availability Center Architecture	12
Overview of Applications	16

The Mercury Business Availability Center Architecture

The Mercury Business Availability Center architecture is made up of servers, data collectors, scripting tools, and third-party servers and components that you set up in the enterprise network environment.

This section covers the following topics:

- Mercury Business Availability Center Servers. For details, see below.
- Mercury Business Availability Center Data Collectors. For details, see page 13.
- Third-Party Servers and Components. For details, see page 14.
- Architecture Diagram. For details, see page 15.

Mercury Business Availability Center Servers

Mercury Business Availability Center is powered by a set of servers that are responsible for facilitating system management, data handling, reporting, and alerting. You install the following Mercury Business Availability Center servers on one or more Microsoft Windows or Sun Solaris machines in your enterprise network environment:

- **Centers Server.** Responsible for running the Mercury Business Availability Center applications, reporting, and the Administration Console.
- **Core Server.** Responsible for receiving data samples from the data collectors, distributing the data to the relevant Mercury Business Availability Center components, and supporting the Bus.
- **Data Processing Server.** Responsible for aggregating data, running the Business Logic Engine, and controlling the Mercury Universal CMDB.

For more information on Mercury Business Availability Center servers, see *Deploying Servers*.

Mercury Business Availability Center Data Collectors

Mercury Business Availability Center data collectors are responsible for collecting performance data from various points throughout the infrastructure, as well as from external locations, and feeding it into a central repository. The data collected by Mercury Business Availability Center data collectors is used to monitor and analyze the performance of your business applications and IT infrastructure.

You install the following data collectors to machines in your enterprise network environment or remote locations:

- **Business Process Monitor.** Emulates the end-user experience by running transactions and collecting availability and response time data.
- **Client Monitor.** Tracks the user experience as perceived by key personnel or clients, as they use your application, and collects "last-mile" availability and response time data.
- **SiteScope.** Collects key performance measurements on a wide range of back-end infrastructure components, including Web, application, database, and firewall servers.
- **Real User Monitor.** Measures the end-user experience of real users from a network/server perspective, by monitoring real user traffic and collecting network and server performance data in real time.

For more information on Mercury Business Availability Center data collectors, see *Data Collector Overview*.

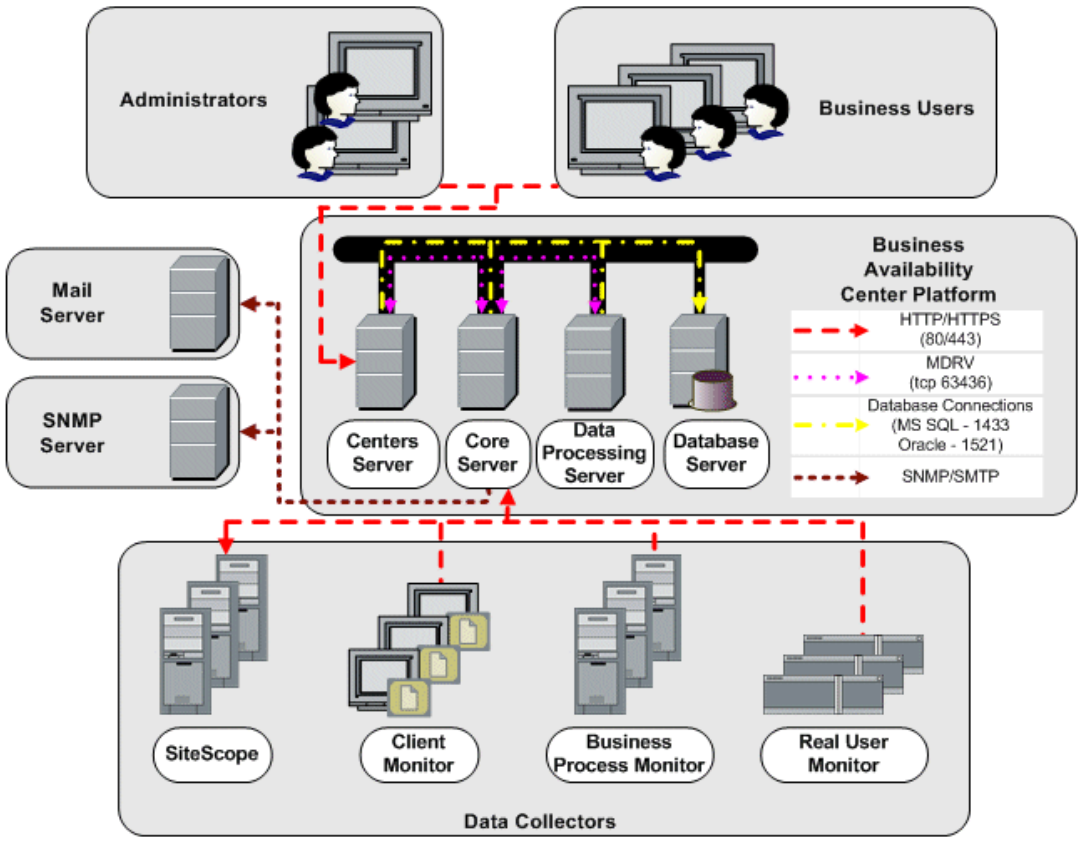
Third-Party Servers and Components

For full functionality, Mercury Business Availability Center requires connection to a database server and a mail server. The database server is used to store system-wide and management-related data, which includes administrative settings and customer-configured information, as well as profile data, which includes data collector settings and collected measurements. The mail server is used to send alerts and scheduled reports to designated recipients. Optionally, connection to an SNMP server might be implemented to receive SNMP traps sent by the Mercury Business Availability Center alerting mechanism.

In addition, Mercury Business Availability Center supports integration of data—to third-party Enterprise Management Software (EMS) tools using Mercury Business Availability Center's Generic Data Engine API and EMS adapters, and from EMS tools via SiteScope Integration Monitors.

For more information on using database servers in Mercury Business Availability Center, see *Preparing the Database Environment*. For more information on third-party integrations, see *Integrating with Third-Party Applications*.

Architecture Diagram



Overview of Applications

The applications that run on the Mercury Business Availability Center platform can be categorized as follows:

- **Business user applications.** Consist of applications used by managers, system administrators, support operators, and other business users to monitor and analyze the performance of critical business applications and IT infrastructure. For details, see below.
- **Administrator applications.** Consist of applications used by Mercury Business Availability Center administrators to manage and administer the Mercury Business Availability Center platform and components. For details, see page 18.

Business User Applications

Mercury Business Availability Center features the business user applications listed below. You access all applications from the Applications menu, except for the My BAC application which is accessed from the top level menu.

Menu Option	Description
My BAC	Select to open the My BAC application, a personalizable portal that individual users can customize to display key content relevant to them. For details, see *Using My BAC*.
Dashboard	Select to open the Dashboard application, a real-time dashboard for viewing performance and availability metrics from a business perspective. For details, see *Using Dashboard*.
Service Level Management	Select to open the Service Level Management application to proactively manage service levels from a business perspective. Service Level Management provides IT Operations teams and service providers with a tool to manage service levels and provide service level agreement (SLA) compliance reporting for complex business applications in distributed environments. For details, see *Using Service Level Management*.

Menu Option	Description
End User Management	Select to open the End User Management application, used to monitor applications from the end user perspective and analyze the most probable cause of performance issues. For details, see *Using End User Management*.
System Availability Management	Select to open the System Availability Management application, used for complete system and infrastructure monitoring as well as event management. For details, see *Using System Availability Management*.
Diagnostics	If a licensed version of Mercury Diagnostics is installed, select to open the Mercury Diagnostics application, to gain end-to-end visibility and comprehensive diagnostics for Java 2 Enterprise Edition (J2EE), .NET-connected, Siebel, SAP, Oracle, and other complex environments. For details, refer to the Mercury Diagnostics documentation accessed from the Help menu in Mercury Business Availability Center.
Application Performance Lifecycle	Select to open the Application Performance Lifecycle application, used to assist in constructing load tests based on real-user transaction data collected by the Real User Monitor. For details, see *Using Application Performance Lifecycle*.

Administrator Applications

Administrators use the Administration Console to administer the Mercury Business Availability Center platform and applications. In addition, administrators use Mercury scripting tools to create the scripts that are used by Business Process Monitor and Client Monitor to collect data for monitored applications.

➤ **Administration Console.** The Administration Console consists of several sections, organized by function. You access each functional area from the Admin menu. You select from the following menu options:

Menu Option	Description
Platform	Select to open the Platform Administration pages, which provide complete platform administration and configuration functionality. For details, see *Platform Administration*.
CMDB	Select to open the CMDB Administration pages, where you build and manage a model of your IT universe in the CMDB. From CMDB Administration, you manage the discovery process and the adapter sources that are used to populate the IT universe model with configuration items (CIs), the templates for creating CIs, and the viewing system for viewing the CIs in Mercury Business Availability Center applications. You can also manually create CIs to add to the model. For details, see *Working with the CMDB*.
Monitors	Select to open the Monitor Administration pages, where you configure and administer data collectors and their monitors. For details, see *Working with Monitor Administration*.
My BAC	Select to open the My BAC configuration pages, where you manage portal modules (including portlets), and set viewing permissions. For details, see *My BAC Administration*.

Menu Option	Description
Dashboard	Select to open the Dashboard Administration pages, where you attach Key Performance Indicators (KPIs) to CIs, define CI status alerts, define the custom and geographical maps, and customize the repositories. For details, see *Application Administration*.
Service Level Management	Select to open the Service Level Management Configuration pages, where you create service level agreements (SLAs) and build services that link to the data that Service Level Management collects. For details, see *Application Administration*.
End User Management	Select to open the End User Management Configuration pages, where you configure transaction order and color settings and report filters. For details, see *Application Administration*.
Diagnostics	Select to open the Mercury Diagnostics configuration page, where licensed Mercury Diagnostics users connect to an installed Diagnostics server and configure Mercury Diagnostics. For details, refer to the Mercury Diagnostics documentation installed with the product.
Personal Settings	Select to access the Personal Settings tab, which enables personalization of various aspects of Mercury Business Availability Center including menus and password. Note that Personal Settings are available to all users. For details, see *Platform Administration*.

➤ **Scripting tools.** Mercury Business Availability Center scripting tools enable you to record the end-user actions that represent the key business transactions whose performance you want to monitor using the Business Process Monitor or Client Monitor. You save the transactions in recorded scripts. The table below describes the scripting tools that are available. For additional information on Business Process Monitor scripting tools, including script recording tips, see *Script Recording Tips*.

Tool	Description
Mercury Virtual User Generator (VuGen)	Enables you to record scripts for a large variety of protocols. This is the recommended tool for recording Business Process Monitor scripts. You download VuGen from the Downloads page, accessed from the Setup and Maintenance tab in Platform Administration. For details on using VuGen, see *Using Mercury Virtual User Generator*. For information on using Mercury LoadRunner scripts in Mercury Business Availability Center, contact Mercury Customer Support.
Client Monitor Recorder	Enables you to record scripts for use with Client Monitor. For details on using the Client Monitor Recorder, see *Using Client Monitor Recorder*.
QuickTest Professional (for use with Windows-based Business Process Monitor only)	Enables you to record scripts for Web-based applications that include Java applets and ActiveX. For details on using QuickTest Professional, refer to the documentation installed with the product.

5

Deployment Planning

Deploying Mercury Business Availability Center in an enterprise network environment is a process that requires resource planning, system architecture design, and a well-planned deployment strategy. The checklist below describes some of the basic issues that should be considered prior to installation. For comprehensive best practices documentation on deployment planning, consult with Mercury Services.

Note to Mercury Managed Services customers: Although Mercury Managed Services customers do not deploy Mercury Business Availability Center software, most of the steps listed below are still relevant to optimally plan the best way to use Mercury Business Availability Center within the Mercury Managed Services framework.

Deployment Planning Checklist

Use this checklist to review the basic issues that your organization should consider when planning the Mercury Business Availability Center deployment.

✓	Step
	Analyze the IT processes and organizational structure and culture that can affect, or be affected by, the deployment.
	Map the customer environment.
	Analyze the organization's goals and identify the key IT-enabled business processes to achieve these goals.
	Identify the target users (those with a vested interest in the business processes), for example, executives, LOB managers, marketing managers, customer support personnel, support engineers, and so forth.
	Align the project with current performance management practices.
	Map the architecture of the monitored infrastructure, including identifying the processes, systems, system resources, and other infrastructure elements to monitor in each of the applications.
	Define the project deliverables, including setting expectations regarding measurements, features, the deployment scope, and maturity levels.
	Identify the appropriate Mercury Business Availability Center functionality.
	Build a deployment roadmap.
	Define success criteria for the project.
	Define performance and availability objectives for each monitored business process.
	Define measurement types to be supported at each deployment stage.
	Form Mercury Business Availability Center administration and operations team(s).
	Plan the practical aspects of the deployment, including system architecture and capacity planning, database environment considerations, security considerations, and so forth.

6

Quick Installation Guide

This chapter provides a quick overview of Mercury Business Availability Center deployment.

This chapter describes:	On page:
About the Quick Installation Guide	23
Prerequisites	25
Installation	28
After Installation	30

About the Quick Installation Guide

Use the checklists in the following sections to understand all the steps required to install Mercury Business Availability Center:

- **Prerequisites.** Includes the preparations you need to make before beginning installation
- **Installation.** Includes all the steps in the installation procedure
- **After Installation.** Includes information about procedures that you can perform following installation

The checklists refer to the following guides. They can be accessed in PDF format, as indicated in the table, from the **Documentation\pdfs** directory on the Mercury Business Availability Center Documentation and Utilities CD-ROM.

Guide Name	Description	PDF Filename
Getting Started with Mercury Business Availability Center (this guide)	Brief overview of Mercury Business Availability Center, providing basic installation information, and pointing to resources required to get up and running.	GettingStarted.pdf
Preparing the Database Environment	Description of the deployment and maintenance of MS SQL Server and Oracle Server databases for use with Mercury Business Availability Center.	PrepDatabase.pdf
Deploying Servers	Instructions on deploying the servers that run Mercury Business Availability Center.	Deploy.pdf
Hardening the Platform	Instructions on hardening the Mercury Business Availability Center platform.	Hardening.pdf

---

Note: Existing customers upgrading to Mercury Business Availability Center 6.2 should also refer to the appropriate *Upgrading Mercury Business Availability Center* guide, available from the **Deployment_Documentation** directory on the Mercury Business Availability Center Setup CD-ROM.

Prerequisites

This checklist includes the procedures you should perform before installing the Mercury Business Availability Center servers.

❑ Prepare the Database Environment

Set up the Mercury Business Availability Center management and profile databases:

- **Management database**. Have your DBA manually (recommended) set up the Mercury Business Availability Center management database (including the CMDB) from within MS SQL Server or Oracle Server. During installation, connect to this database.
  If you prefer, you can automatically set up and connect to the management database during installation.
- **Profile database**. Have your DBA manually (recommended) set up the profile database from within MS SQL Server or Oracle Server. After installation, connect to this database from within Mercury Business Availability Center.
  If you prefer, you can set up and connect to the profile database after installation from within Mercury Business Availability Center. For details, see "Database Management" in *Platform Administration*.

Manually set up databases on MS SQL Server	**Manually set up databases on Oracle Server**
🕮 Overview of MS SQL Server Deployment, in *Preparing the Database Environment*	🕮 Overview of Oracle Server Deployment, in *Preparing the Database Environment*

❑ Make Deployment Preparations

Verify that all information needed for the installation is at hand.

Microsoft Windows	**Solaris**
🕮 Preparing Information Required for Installation and Installation Prerequisites, in *Deploying Servers*	🕮 Preparing Information Required for Installation and Installing Mercury Business Availability Center Servers, in *Deploying Servers*

❑ Check the Mercury Business Availability Center Servers

Verify that the servers meet the minimum requirements for running Mercury Business Availability Center.

Verify that access to the servers is available, either through HTTP or HTTPS, from any standard Internet or intranet connection.

Do not have any other Mercury products installed on the machines on which you are installing Mercury Business Availability Center.

The servers must have a user account with administrative rights to the database server(s) upon which you set up the management database (and later, profile database).

To maximize the performance of machines on which you install servers, it is recommended that they be dedicated to Mercury Business Availability Center and not run other applications.

Microsoft Windows

📖 Reviewing System Requirements, in *Deploying Servers*

Tip: Verify that you have more than 50 MB free for installation needs on the system drive on which Windows is installed.

Solaris

📖 **Reviewing System Requirements**, in *Deploying Servers*

Tip: Verify that you have more than 50 MB free under **/tmp** and **/var/tmp** for installation needs.

❑ Check the Web Browser

Verify that your Web browser is set to accept all cookies.

Verify that your Web Browser does not block pop-up windows.

Verify that your Web Browser uses Java support for applets (JRE).

If you are using Microsoft Internet Explorer (IE), set the browser caching to automatically check for newer versions of stored pages, and to use the minimum amount of disk space.

📖 Browser Preparation, in *Deploying Servers*

❑ Deploy the Web Server

Install the Web server prior to installing Mercury Business Availability Center.

Note that if you wish to run the Apache HTTP Server with Mercury Business Availability Center, you choose this server during installation. No preliminary setup is required.

Microsoft Internet Information Server (IIS) (Windows only)

📖 Working with the Web Server, in *Deploying Servers*

Tip: Verify that the IIS services are up and running.

Sun Java System Web Server (Solaris only)

📖 Working with the Web Server, in *Deploying Servers*

Tip: Verify that the user root (used to run installation) has write privileges on the directory where the configuration files of Sun Java System Web Server reside.

❑ Check the Default Ports

Consult this section for an explanation of which ports are used by Mercury Business Availability Center:

📖 Port Management, in *Deploying Servers*.

Installation

This checklist includes the procedures you should perform during installation of the Mercury Business Availability Center servers.

❑ Install the Mercury Business Availability Center 6.1 Servers and 6.2 Add-on

Install the Mercury Business Availability Center 6.1 servers on a Windows or Solaris platform, using the Mercury Business Availability Center 6.1 Setup CD-ROM. Then install the 6.2 Add-on from the Mercury Business Availability Center 6.2 Add-on CD-ROM.

To run Mercury Business Availability Center on an Apache HTTP Server, you choose this server during installation. Note, however, that a port conflict may arise if another Web server is already installed on the machine.

📖 Apache HTTP Server (for Windows deployment) and Apache HTTP Server (for Solaris deployment), in *Deploying Servers*

Microsoft Windows	**Solaris**
📖 Installing Mercury Business Availability Center Servers on a Windows Platform, in *Deploying Servers*	📖 Installing Mercury Business Availability Center Servers on a Solaris Platform, in *Deploying Servers*

❑ Run the Set Management Database Procedure

If your DBA did not set up the management database before you installed Mercury Business Availability Center (for details, see "Prepare the Database Environment" on page 25), you must run the set management database utility—at the end of the installation procedure—to create and connect to the new management database.

If your DBA did set up the management database before you installed Mercury Business Availability Center, you must connect to the new database.

Microsoft Windows	**Solaris**
📖 Setting Management Database Parameters for a Windows Platform, in *Deploying Servers*	📖 Setting Management Database Parameters for a Solaris Platform, in *Deploying Servers*

❑ Install the Mercury Business Availability Center 6.2 Components

Install the Mercury Business Availability Center 6.2 components, including data collectors and scripting tools, using the Mercury Business Availability Center Components Setup CD-ROMs.

Until the components are installed, the Downloads page in the Mercury Business Availability Center Administration Console (a central location from where Mercury Business Availability Center administrators and users can download components) will be empty.

Microsoft Windows	Solaris
🕮 Installing Mercury Business Availability Center Servers on a Windows Platform, in *Deploying Servers*	🕮 Installing Mercury Business Availability Center Servers on a Solaris Platform, in *Deploying Servers*

After Installation

This checklist includes the procedures you should perform following installation of the Mercury Business Availability Center servers. To troubleshoot installation issues, see "Installation Troubleshooting" in *Deploying Servers*.

❑ Verify Successful Connectivity

Verify that the JBoss application server and Tomcat servlet engine connections are healthy.

Microsoft Windows	Solaris
🕮 Verifying JBoss and Tomcat Connectivity, in *Deploying Servers*	🕮 Verifying Jboss and Tomcat Connectivity:, in *Deploying Servers*

❑ Verify Ability to Log In to Mercury Business Availability Center

Verify that Mercury Business Availability Center is up and running: log in to Mercury Business Availability Center and navigate the application.

🕮 Chapter 7, "Accessing and Navigating Mercury Business Availability Center" in this guide

❑ Verify Support for I18N Environment (Optional)

If required, review information about deploying Mercury Business Availability Center in a non-English language environment.

🕮 *Working in an I18N Environment*

7

Accessing and Navigating Mercury Business Availability Center

This chapter provides details on how to access and navigate Mercury Business Availability Center.

This chapter describes:	On page:
Accessing Mercury Business Availability Center	31
Navigating Mercury Business Availability Center	39
Troubleshooting Mercury Business Availability Center Login	42

Accessing Mercury Business Availability Center

You access Mercury Business Availability Center using a supported Web browser, from any computer with a network connection (intranet or Internet) to the Mercury Business Availability Center servers. The level of access granted a user depends on the user's permissions. For details on granting user permissions, see "Configuring User Permissions" in *Platform Administration*.

For details on Web browser requirements, as well as minimum requirements to successfully view Mercury Business Availability Center, see "Reviewing System Requirements" in *Deploying Servers*.

Note to Mercury Managed Services customers: You access Mercury Business Availability Center via the Mercury Managed Services Web site (mms.mercury.com).

This section includes the following topics:

- "Logging In" on page 32
- "Logging Out" on page 33
- "Enabling Automatic Login in the Login Page" on page 34
- "Using the Automatic Login URL Mechanism" on page 35
- "Limiting Access by Different Machines Using the Same Login Name" on page 36
- "Using Direct Login to a Specific Page" on page 36

Logging In

You log into Mercury Business Availability Center from the login page.

To access the Mercury Business Availability Center login page and log in:

1 In the Web browser, enter the URL **http://<server_name>/MercuryAM** (**mercuryam** can also be used), where **server_name** is the name or IP address of the Mercury Business Availability Center server. If there are multiple servers or if Mercury Business Availability Center is deployed in a distributed architecture, specify the load balancer or Centers Server URL, as required.

Customers running previous versions of Mercury Business Availability Center (formerly Topaz) can still use bookmarks set to access the URL **http://<server_name>/topaz**.

2 Enter the login parameters (login name and password) of a user defined in the Mercury Business Availability Center system, and click **Log In**. After logging in, the user name appears at the top right, under the top menu bar.

Initial access can be gained using the default superuser login parameters: Login Name=**admin**, Password=**admin**. It is recommended that the system superuser change this password immediately to prevent unauthorized entry. For details on changing the password, see "Changing the User Password" in *Platform Administration*.

For details on creating users in the Mercury Business Availability Center system, see "User Management" in *Platform Administration*.

For details on login authentication strategies that can be used in Mercury Business Availability Center, see "Authentication Strategies" in *Platform Administration*.

For login troubleshooting information, see "Troubleshooting Mercury Business Availability Center Login" on page 42.

Note: For details on accessing Mercury Business Availability Center securely, see *Hardening the Platform*.

Logging Out

When you have completed your session, it is recommended that you log out of the Web site to prevent unauthorized entry.

To log out:

Click **Logout** at the top of the page.

Enabling Automatic Login in the Login Page

When automatic login is enabled from the login page, the next time the user enters the URL to access Mercury Business Availability Center, the login page does not open, the login name and password do not have to be entered, and the default page that is set to open for the user opens automatically.

To enable automatic login:

1. In the Mercury Business Availability Center login page, select the option to **Remember my login name and password for 14 days.**
2. When completing your session, do not click **Logout** at the top of the page, but simply close the browser window.

   Logging out disables the automatic login option and the login name and password must be entered when again accessing Mercury Business Availability Center.

Guidelines for Using Automatic Login

Keep the following in mind when using this option:

- Using the **Logout** option at the top of the Mercury Business Availability Center page cancels the option. If a user has logged out, the next time the user logs in, the Login page opens and the user must enter a login name and password. This can be useful if another user must log in on the same machine using a different user name and password.
- Automatic login can be enabled for a specific period of time (the default is 14 days). After that period of time has elapsed, the option must be selected again to enable it.
- This option could be considered a security risk and should be used with caution.

➤ You can configure this option and modify the default values in Infrastructure Settings. To access the relevant settings in Infrastructure Settings, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** > **Foundations** > **Security**. In this context, you can:

  ➤ Completely remove this option from appearing in the login page by setting the **Enable automatic login** value to false (true is the default value).

  ➤ Customize the number of days to enable the option by editing the **Days to remember login** value to the desired number of days (14 is the default value).

  For details on using the Infrastructure Settings page, see "Infrastructure Settings" in *Platform Administration*.

Using the Automatic Login URL Mechanism

You can use a special URL, containing several parameters including login name and password, to access Mercury Business Availability Center and automatically log in. Note that, though convenient, this method is not secure since the password is not encrypted in the URL.

To access Mercury Business Availability Center and log in using the automatic login mechanism:

In the Web browser, enter the URL **http://<server_name>/topaz/TopazSiteServlet?autologin=yes&strategyName=Topaz&requestType=login&userlogin=<loginname>&userpassword=<password>&createSession=true**, where **server_name** represents the name of the Mercury Business Availability Center server, and **loginname** and **password** represent the login name and password of a user defined in Mercury Business Availability Center.

To enable direct entry to Mercury Business Availability Center, bookmark this URL.

Limiting Access by Different Machines Using the Same Login Name

Mercury Business Availability Center can be accessed using the same login name from different machines. The number of machines accessing Mercury Business Availability Center using the same login name can be limited using the Infrastructure Settings page.

To modify the value in Infrastructure Settings, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** > **Foundations** > **Security**. Set the **Maximum machines per login name** value to the number of machines that can access Mercury Business Availability Center using the same login name. The default value is zero (0) which enables limitless logins.

If the maximum value has been reached when a user tries to log into Mercury Business Availability Center, the user receives a login error message and is unable to log in.

Feature Limitation

In certain network configurations where multiple clients are funneled through a default gateway or proxy server, the IP resolved to Mercury Business Availability Center is that of the gateway or proxy server and not the IP of the client. As a result Mercury Business Availability Center treats each client as coming from the same IP. Since this feature does not limit the number of logins from the same machine (IP), the feature enables all the clients to log into Mercury Business Availability Center, even though they originate from different IPs.

Using Direct Login to a Specific Page

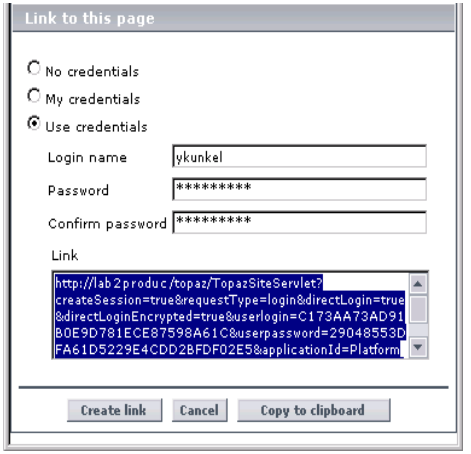
Direct Login is a mechanism to easily guide another user to a specific target page in Mercury Business Availability Center. Direct Login creates a URL with user name, password, and information about the target page. You can send this URL by e-mail, SMS, and so forth to another user.

Depending on how you configure Direct Login, the receiver accesses the page using his own user name and password, your user name and password, or another user's user name and password. The receiver bypasses the Mercury Business Availability Center login page because the URL supplies the user name and password information.

To configure direct login to a specific page:

1 Go to the page in Mercury Business Availability Center that you want to send to the receiver.

2 Select **Admin** > **Link to this page**. The **Link to this page** dialog box opens.



3 Select the method that the receiver uses to access the target page:

- Choose **No credentials** if the receiver should use his own user name and password to access the page.
- Choose **My credentials** if the receiver should use your user name and password to access the page.
- Choose **Use credentials** and fill in **Login name** and **Password** if the receiver should use the user name and password you supply here. There is no default user account, like guest in Microsoft Windows, so you must fill in both fields.

4 Click **Create link**. The URL is written in the Link box. The user name and password are encrypted so that no login information is revealed.

5 Click **Copy to clipboard**.

6 Click **Cancel** to close the **Link to this page** dialog box.

7 Open a new e-mail message and paste the clipboard contents into the message area. Publish the URL via e-mail, SMS, and so forth to the receiver with instructions to click the URL.

8 When the receiver clicks the URL, one of the following scenarios occurs:

- If **No credentials** was chosen in step 3, the receiver is first sent to the Mercury Business Availability Center login page. There is no limit to the number of login retries. After successfully logging in to his own account, he is automatically sent to the target page.
- If **My credentials** or **Use credentials** was chosen in step 3, the receiver is sent to the target page without logging in.

Limitations

- Direct Login is operational only in reports, Dashboard, and the configuration pages of specific views.
- The user name sent in the URL must be an account with sufficient privilege to access the target page. If the account does not have sufficient privilege, the receiver is sent to the page above the target page.

  For example, you want to direct the receiver to the Infrastructure Settings page. You configure Direct Login, however, with **Use Credentials** of a regular user. When the receiver uses this URL, he is sent to the Setup and Maintenance page and he cannot access Infrastructure Settings.
- Direct Login does not verify the user name and password sent in the URL. Verification is done only when the receiver tries to access the target page. If the user name and password are not correct, or the user account has been deleted, the receiver is sent to the Mercury Business Availability Center login page to log in normally. Once he is logged in, he does not proceed to the target page. There is no informational message about the reason for the Direct Login failure.

Security Notes and Precautions

- The user name and password in the URL are encrypted so that no login information is ever revealed.
- Sending encrypted information by e-mail still entails a security risk since the mail system can be breached. If the e-mail is intercepted, access to Mercury Business Availability Center is given to an unknown party.
- Do not use the URL from Direct Login as a link in any Web page.
- The receiver has all privileges of the user name he was given in the URL. Once the receiver accesses the target page, he can perform all actions permitted to that user name anywhere in Mercury Business Availability Center.

Navigating Mercury Business Availability Center

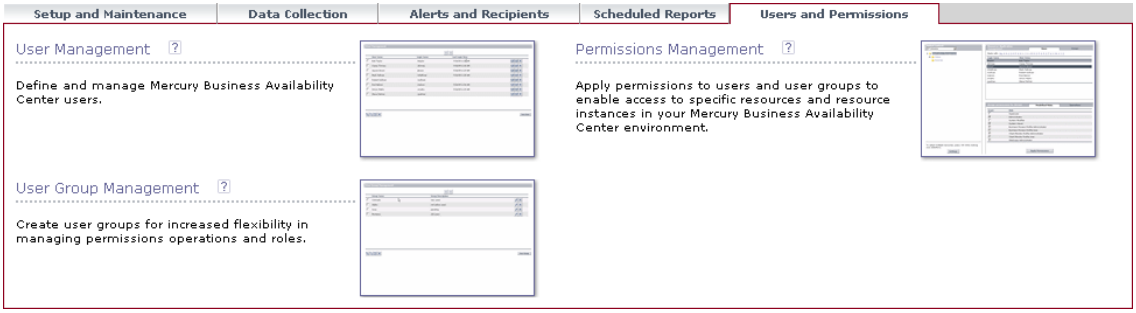
Mercury Business Availability Center runs in a Web browser. You move around Mercury Business Availability Center using the following navigation functions:

- **Site Map.** Enables quick access to all top-level contexts in the Applications menu or the Administration Console. The site map is the first page that opens, by default, after logging into Mercury Business Availability Center. If the default page after login is changed, you can access the site map by clicking the Site Map link, either in the top menu or from the Help menu.

- **Top menu bar.** Enables navigation to the applications, Administration Console pages, and help resources. The top menu bar also includes a link to the site map and the Logout button.



- **Tabs.** Enable navigation to various contexts within a particular area of Mercury Business Availability Center, for example to different types of reports within an application, different views within a report, or different administrative functions within the Administration Console. In certain contexts, tabs are used to distinguish between functions; in other contexts tabs are used to group logically similar functions or features together.
- **Tab main menus.** Enable navigation from a tab front page to various contexts related to the tab. Tab main menus appear when selecting a tab that represents a category containing several contexts, for example, report types or administrative settings. Tab main menus include a description and thumbnail image of each tab context.



➤ **Tab controls.** Assist in navigation from any context related to a tab to any other of the tab's contexts. To open the tab main menu, click the tab name.



To quickly jump to another context related to the tab, move your mouse pointer over the tab and click the down arrow that appears to open the tab dropdown menu. Click a tab menu option to move to that context.



➤ **Breadcrumbs.** Enable returning to previous pages within a multi-level context by clicking the appropriate page level. For example, in the following breadcrumb trail, you would click **Breakdown Summary** to return to the Breakdown Summary report:



Note: The Web browser **Back** function is not supported in Mercury Business Availability Center. Using the **Back** function does not always revert the current context to the previous context. To navigate to a previous context, use the breadcrumb function.

Troubleshooting Mercury Business Availability Center Login

Use the information below to troubleshoot possible causes of failure to log in to Mercury Business Availability Center. Reference the possible cause(s) using the error number shown in the error alert dialog box. For additional troubleshooting information, refer to the Mercury Business Availability Center Knowledge Base on the Mercury Customer Support Web site.

Error No.	Problem/Possible Cause(s)	Solution(s)
LI001	Mercury Business Availability Center failed to connect to the JBoss application server running on the Centers Server. This may be due to: ➤ JBoss server being down ➤ problems with the Mercury Business Availability Center service ➤ the port required by the application server being used by another application	**Solution 1:** Close all applications on the Centers Server machine and restart the machine. **Solution 2:** Ensure that there are no other running applications on the Centers Server machine that use this port (for example, applications that run from the Startup directory, another instance of JBoss, an MSDE or MS SQL Server, or any other process).
LI002	The JBoss application server running on the Centers Server is not responding or is not installed correctly.	Restart the Mercury Business Availability Center application.
LI003	The management database might be corrupted (for example, if a user record was accidentally deleted from the database).	Try logging in as a different user, or ask the Mercury Business Availability Center administrator to create a new user for you.
LI004	The connection between the Tomcat servlet engine and the JBoss application server failed due to an RMI exception. This may be due to problems in RMI calls to JBoss.	Ensure that none of the JBoss ports are in use by another process. Also, ensure that the RMI ports are bound. For details on port management, see “Port Management” in *Deploying Servers*.

Error No.	Problem/Possible Cause(s)	Solution(s)
LI005	The Mercury Business Availability Center login fails or hangs. This may be due to: ➤ an incorrect login name/password combination ➤ inability to connect to the management database ➤ current user does not have access rights to any profile ➤ authentication strategy has not been set/configured correctly	**Solution 1:** Ensure that you or the user enters a correct login name/password combination. **Solution 2:** Ensure that the connection to the management database is healthy. To do so: 1. In the Web browser, type **http://<Mercury Business Availability Center server name>:8080/web-console/index.html** to connect to the JMX management console. 2. Click the link **System** > **JMX MBeans** > **Topaz** > **Topaz:service=Connection Pool Information**. 3. Locate **java.lang.String showConfigurationSummary()** and click the **Invoke** button. 4. In **Active configurations in the Connection Factory**, find the appropriate row for the management database. 5. Verify that columns **Active Connection** and/or **Idle Connection** have a value greater than **0** for the management database. 6. If there is a problem with the connection to the database, verify that the database machine is up and running; if required rerun the Set Management Database utility. *...cont'd*

Error No.	Problem/Possible Cause(s)	Solution(s)
LI005 (*cont'd)*	The Mercury Business Availability Center login fails or hangs.	**Solution 3:** For details on granting permissions to users, see "Configuring User Permissions" in *Platform Administration*. **Solution 4:** For details on authentication strategies, see "Authentication Strategies" in *Platform Administration*.
LI006	The Mercury Business Availability Center login fails. This may be due to: ➤ incorrect cookie settings in the Web browser ➤ an unsupported character in the names of the machines running the Mercury Business Availability Center servers	**Solution 1:** Ensure that the client Web browser is set to accept cookies from Mercury Business Availability Center servers. **Solution 2:** Ensure that there are no underscore characters (_) in the names of the machines running the Mercury Business Availability Center servers. If this is the case, either rename the server or use the server's IP address when accessing the machine. For example, to access Mercury Business Availability Center, use http://111.222.33.44/MercuryAM instead of http://my_server/MercuryAM

Error No.	Problem/Possible Cause(s)	Solution(s)
LI007	The Mercury Business Availability Center login fails. This is because the maximum number has been reached of concurrent logins from different machines that access Mercury Business Availability Center using the same login name.	**Solution 1:** Log out of the instances of Mercury Business Availability Center that have logged in using the same login name from different machines. You can then retry logging in if the maximum number has not been reached. **Solution 2:** Log in using a different login name, if available. **Solution 3:** The administrator can edit the Infrastructure Settings to remove the limitation or increase the maximum number of concurrent logins using the same login name from different machines. To edit this setting, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, select **Security** and locate the **Maximum machines per login name** entry in the **Security - Login** table. Modify the value as required. The default value is 0, which enables limitless logins.

8

Basic Administration Checklists

This chapter provides checklists for basic platform, CMDB, monitor, and application administration and configuration tasks.

This chapter describes:	On page:
Platform Administration Checklist	48
CMDB Administration Checklist	49
Monitor Administration Checklist	51
Application Administration Checklist	54

Platform Administration Checklist

Use this checklist to review the basic platform administration tasks required to set up the Mercury Business Availability Center system.

✓	Step
	Configure the profile database, which holds monitor data collected by Mercury Business Availability Center. ➤ For details, see "Database Management" in *Platform Administration*.
	Define login names and passwords for users to whom you wish to provide access to Mercury Business Availability Center. If required, during user definition specify each user's user mode. For details, see: ➤ "User Management" in *Platform Administration*. ➤ "KPIs for User Modes"in *Application Administration*.
	Group users into logical groups to better facilitate applying permissions. ➤ For details, see "User Group Management" in *Platform Administration*.
	Define permissions for users and/or user groups. Permissions permit or deny users access to the various functions and features in the Mercury Business Availability Center Web interface. ➤ For details, see "Configuring User Permissions" in *Platform Administration*.
	Configure recipients of alerts and scheduled reports, including method of delivery (e-mail, SMS, pager). ➤ For details, see "Configuring and Selecting Recipients" in *Platform Administration*.
	If required, customize your Mercury Business Availability Center system using the Infrastructure Settings Manager. ➤ For details, see "Infrastructure Settings" in *Platform Administration*.

✓	Step
	If required, enable data partitioning on your profile database to facilitate the periodic purging of historical data. ➤ For details, see "Purging Historical Data from Profile Databases" in *Platform Administration*.
	If required, configure an alternate login authentication strategy. ➤ For details, see "Authentication Strategies" in *Platform Administration*.

CMDB Administration Checklist

Use this checklist to review the basic CMDB administration tasks required to set up the Mercury Business Availability Center IT universe model.

✓	Step
	Licensed Discovery Manager users can run the discovery process to identify IT resources in the network infrastructure. ➤ For details, see "Introduction to the Discovery Manager" in *Discovery Manager Administration*.
	If required, define custom data sources in Source Manager. If using SiteScope Integration Monitors, custom data sources must be defined. ➤ For details, see "Introduction to Source Manager" in *Source Manager Administration*.

✓	Step
	Manually build your IT universe model by defining configuration items (CIs) and CI relationships in the model. Divide the model into service views (views) that represent logical subsets of the overall model. Add CIs based on discovered network resources or manually define infrastructure components. Once you configure data collectors in Monitor Administration, you can attach monitor CIs to views. For details, see: ➤ "Introduction to IT Universe Manager Administration" in *IT Universe Manager Administration*. ➤ "Introduction to View Manager" in *View Manager Administration*.
	Define permissions for views. Permissions permit or deny users access to the defined views. ➤ For details, see "Configuring User Permissions" in *Platform Administration*.

Monitor Administration Checklist

Use this checklist to review the basic monitor administration tasks required to bring monitor data into Mercury Business Availability Center.

✓	Step
	Download script recorders to a central network location or directly to machines of administrators designated to create Business Process Monitor or Client Monitor scripts. ➤ For details, see "Downloads" in *Platform Administration*.
	Download data collectors to a central network location or directly to the machines designated to host data collector software. ➤ For details, see "Downloads" in *Platform Administration*.
	Record scripts for Business Process Monitor and Client Monitor data collectors based on business processes defined for monitoring. For details, see: ➤ "VuGen Recording Tips" in *Introduction to Creating Scripts*. ➤ Recording with VuGen in *Using Mercury Virtual User Generator*. ➤ "Script Creation Workflow" in *Using Client Monitor Recorder*.
	Deploy data collectors in the network environment or to remote hosts. For details, see: ➤ "Deploying Business Process Monitor" in *Business Process Monitor Administration*. ➤ "Installing Client Monitor" in *Client Monitor Administration*. ➤ "Introducing and Deploying SiteScope" in *SiteScope Administration*. ➤ "Introducing Real User Monitor Administration" in *Real User Monitor Administration*

✓	Step
	Upload scripts to the Script Repository. ➤ For details, see "Script Repository" (Mercury Managed Services customers, see "Mercury Managed Services Script Repository") in *Platform Administration*.
	Set up the enterprise tree in Monitor Administration to reflect the organization's monitoring strategy. ➤ For details, see "Using Monitor Administration" in *Working with Monitor Administration*.
	Configure data collectors in Monitor Administration to enable Mercury Business Availability Center to receive data. For details, see: ➤ "Creating Business Process Profiles" in *End User Management Data Collector Configuration*. ➤ "Managing Business Process Profiles and Creating Client Monitor Profiles" in *End User Management Data Collector Configuration*. ➤ "Working with Groups, Monitors, and Templates" in *Configuring SiteScope Monitors*. ➤ "Configuring the Real User Monitor" in *End User Management Data Collector Configuration*.
	If required, perform advanced monitor setup tasks, including setting views, defining categories, and using templates and solution sets. For details, see: ➤ "Setting Views and Defining Categories" in *Working with Monitor Administration*. ➤ "Using Templates to Deploy Monitors" in *Managing SiteScope*. ➤ "Introducing SiteScope Solution Templates" in *Managing SiteScope*.

✓	Step
	Define permissions for monitoring resources. Permissions permit or deny users access to the various resources. ➤ For details, see "Configuring User Permissions" in *Platform Administration*.
	If required, configure downtime or event schedules for defined data collectors. ➤ For details, see "Downtime/Event Scheduling" in *Platform Administration*.
	Define alerts based on trigger criteria related to monitoring, threshold, and service level priorities. ➤ For details, see "Creating Alert Schemes" in *Platform Administration*.
	If required, define scheduled reports, which are sent to predefined recipients. ➤ For details, see "Scheduled Reports" in *Platform Administration*.
	If required, set up third-party integrations. ➤ For details, see *Integrating with Third-Party Applications*.

Application Administration Checklist

Use this checklist to review the basic administration tasks required to get Mercury Business Availability Center applications up and running. For complete details on administering applications, see *Application Administration*.

✓	Step
	Configure and customize Dashboard, including customizing KPIs, configuring CI status alerts, or defining a custom and geographical map. ➤ For details, see: "Dashboard Administration" in *Application Administration*.
	Configure Service Level Management, including creating service level agreements (SLAs) and defining service objectives for availability and performance. ➤ For details, see "Setting Up Service Level Management" in *Application Administration*.
	If required, configure End User Management report options such as transaction order and color settings, and report filters. For details, see: ➤ "End User Management Report Configuration" in *Application Administration*.
	Licensed Mercury Diagnostics users must register their Diagnostics server in Mercury Business Availability Center. ➤ For details, see "Mercury Diagnostics and Mercury Business Availability Center Integration" in *Application Administration*.

9

How Do I...?
A Task Reference for Administrators

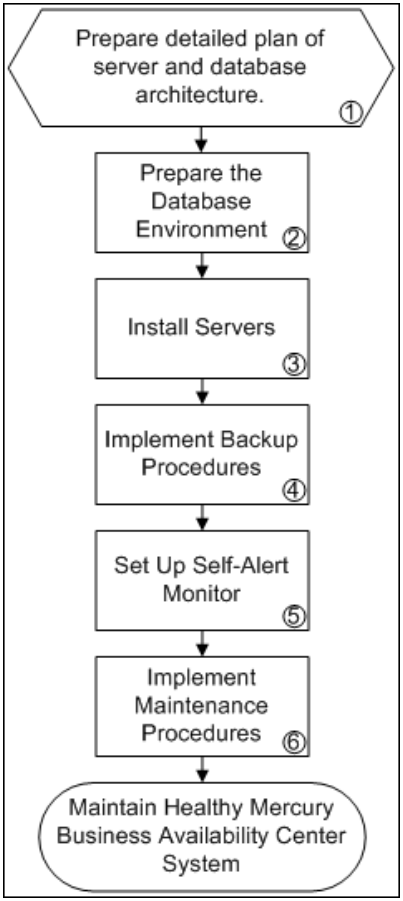
This chapter describes step-by-step process flows for the following common administrative tasks performed in Mercury Business Availability Center. A legend of shapes used by the flowcharts is located on page 88.

This chapter describes:	On page:
How Do I Build and Maintain My Mercury Business Availability Center System?	57
How Do I Set Up Users and Permissions?	60
How Do I Reflect My IT Environment in Mercury Business Availability Center?	62
How Do I Collect Data on the Performance of a Specific Business Process?	65
How Do I Collect Data on the Performance of an IT Resource?	68
How Do I Collect Data on Real User Traffic Accessing a Specific Application?	70
How Do I Collect Data on the Performance of an Application Being Accessed by Specific Users?	72
How Do I Integrate Data from Third-Party Sources (EMS Data) into Mercury Business Availability Center?	74

This chapter describes:	On page:
How Do I View My Already Created Monitors in Dashboard?	78
How Do I Set Up SLAs and Track Their PNR KPIs in Dashboard?	80
How Do I Set Up a Report and Alert Delivery System?	82
How Do I Customize the Way Mercury Business Availability Center Displays My Views in Dashboard?	84
How Do I Customize Dashboard Repository Entities to Model My Business World? A Sample Scenario	86
Flowchart Legend	88

How Do I Build and Maintain My Mercury Business Availability Center System?

The flowchart below describes the process recommended to set up and maintain a Mercury Business Availability Center system. Note that the term database in this section refers to both MS SQL Server databases and Oracle Server user schemas. The numbered elements are referenced in the table on the following page, which provides additional details about the steps and a reference to more information.

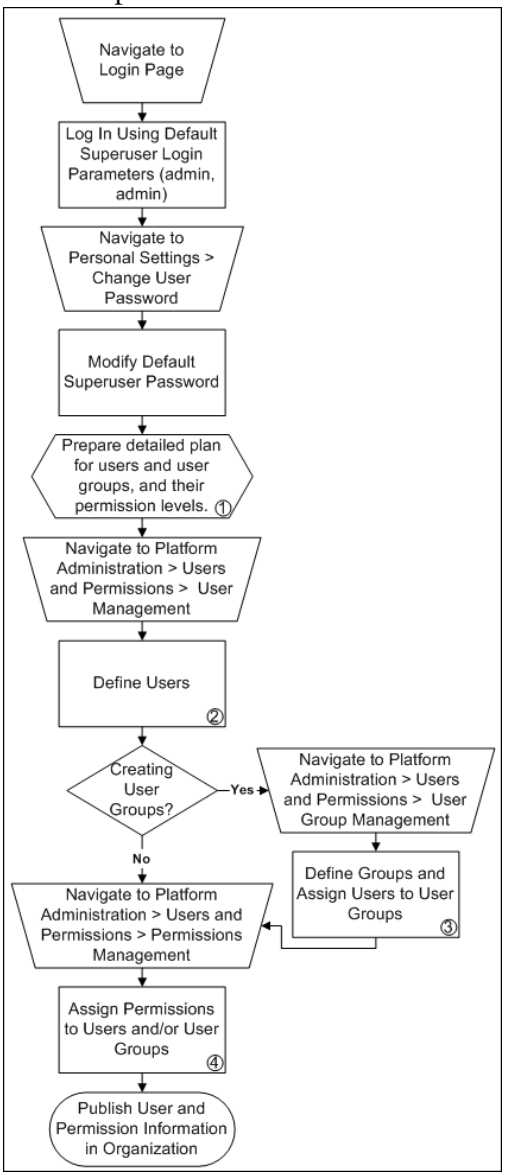


Ref. No.	Comment
1	Map out the Mercury Business Availability Center server and database architecture that will be required, based on organizational requirements, expected system capacity requirements (considering load factors such as data input and application usage), high availability and system failover requirements, and security requirements.
2	Set up the database server that will be used with Mercury Business Availability Center. Establish procedures for database backup and maintenance, including backup of management, profile, and LDAP databases and a data purging policy. Optionally, manually create the Mercury Business Availability Center management and profile databases. For more information, see *Preparing the Database Environment*
3	Install Mercury Business Availability Center servers and connect to the management database. Server installation must take into account planned high availability and failover strategies (including load balancing, backup servers, and so forth). Consider installing a separate staging system to use for testing configuration changes, patches, backup and restore procedures, and so forth. For more information, see *Deploying Servers*
4	Implement a backup process whereby key configuration files that contain data not stored in the database are automatically backed up daily (for more information, see "File Backup Recommendations" in *Deploying Servers*). In addition execute database backup plans. It is also recommended to create procedures for restoring resources and test those procedures on a staging system.

Ref. No.	Comment
5	Set up Mercury Self-Alert Monitor (via SiteScope) to monitor the health of Mercury Business Availability Center servers. For details, see "Mercury Self-Alert Monitor" in *SiteScope Administration*.
6	Implement ongoing maintenance procedures that will enable the system to run smoothly and will minimize issues during future upgrade. For example: ➤ Create run books that instruct personnel how to perform server maintenance procedures as well as how to proceed in the event of system failure or server downtime. ➤ Track customization and configuration changes that you make (such as those made in configuration files or in the Infrastructure Settings Manager), in case you need to roll back at a later time. ➤ If you install private patches keep track of them, and when upgrading make sure your Mercury representative knows about them and can confirm how the upgrade will affect their status. **Tip:** Private patches should be installed on a staging system before being deployed to production. ➤ Troubleshoot problems by accessing log files and searching for errors (for more information, see "Mercury Business Availability Center Logs" in *Reference Information*). Use the Knowledge Base on the Mercury Customer Support Web site (support.mercury.com) to search for answers to issues that may come up.

How Do I Set Up Users and Permissions?

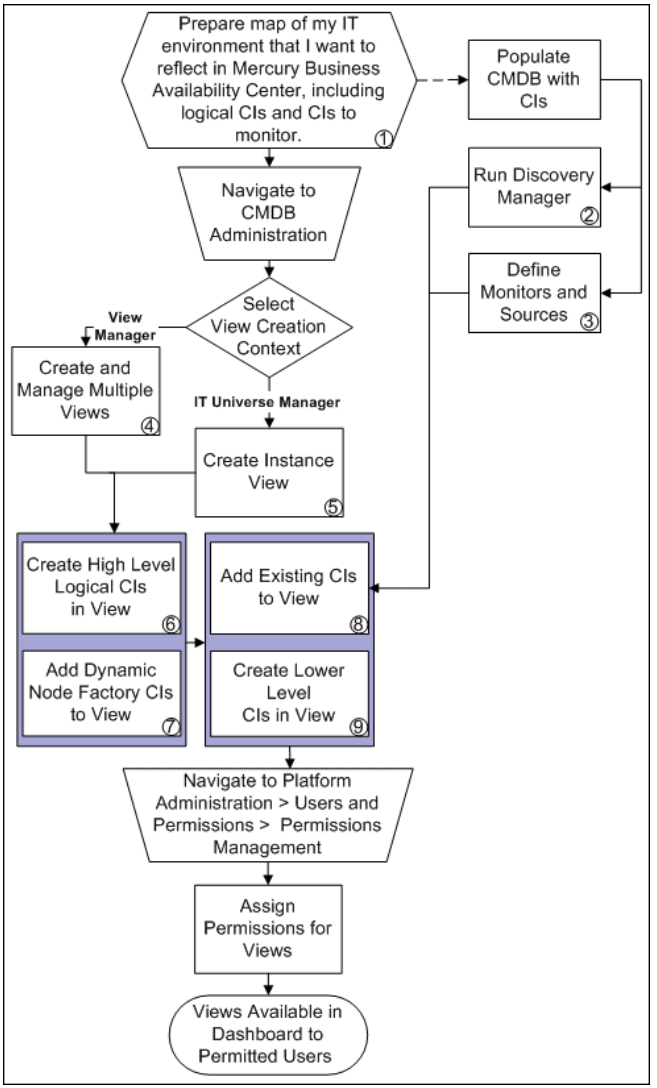
The flowchart below describes the process required to set up users and user groups and assign them system permissions. The numbered elements are referenced in the table on the following page, which provides additional details about the steps and a reference to more information.



Ref. No.	Comment
1	Map out the required users and user groups and their relevant permission levels before defining them in Mercury Business Availability Center. For example, in a spreadsheet enter the following information: ➤ a list of all staff who will be required to administer the system, as well as the end users who will be accessing Dashboard and reports. Gather appropriate user details such as user names, login names, initial passwords, and user time zones. Although not needed to define users, at this stage it might be useful to also collect user contact information such as telephone number, pager, or e-mail address (contact information is required for Mercury Managed Services customers). ➤ if categorization of users into modes (operations and business) is required, specify into which user mode to categorize each user. For more information, see "KPIs for User Modes" in *Platform Administration* ➤ if groups of users will require similar system permissions, a list of user groups and the users that should belong to each group. ➤ the permissions each user or user group will require. To aid in this process, review the Permissions Management page to learn about the different contexts and resources for which permissions can be granted. For more information, see "Configuring User Permissions" in *Platform Administration*
2	Define new users as per requirements or planned specifications. For more information, see "User Management" in *Platform Administration*
3	Define user groups (General tab) and assign users to them (Users tab) as per requirements or planned specifications. For more information, see "User Group Management" in *Platform Administration*
4	Assign role-level or operation-level permissions to individual users (Users tab) or user groups (Groups tab) as per requirements or planned specifications. Keep the following tips in mind: ➤ Superuser, Administrator, System Modifier, and System Viewer roles can only be applied to the Business Availability Center resource, which refers to the whole Mercury Business Availability Center system and appears at the top level in every context. ➤ Business Process Monitor, Client Monitor, and SiteScope roles can be applied to specific, related resources in the Monitors context. These roles are useful when assigning permissions to users and administrators responsible for specific data collectors. ➤ Operation-level permissions are applied, in any context, to resources below the Business Availability Center resource level. ➤ To assign a user permissions on a subresource, you must provide the user with at least View permissions on the selected resource's parent. For more information, see "Configuring User Permissions" in *Platform Administration*

How Do I Reflect My IT Environment in Mercury Business Availability Center?

The flowchart below describes the process required to create views that reflect your organization's IT environment in Mercury Business Availability Center. The numbered elements are referenced in the table on the following page, which provides additional details about the steps and a reference to more information.

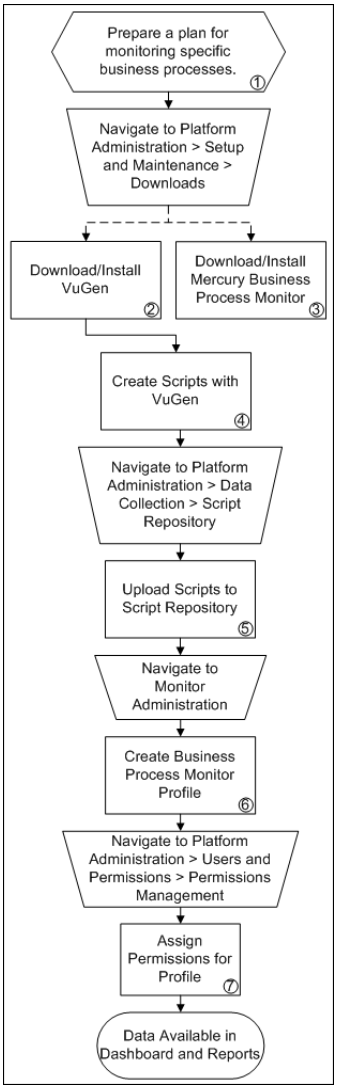


Ref. No.	Comment
1	Prepare this information before beginning work in Mercury Business Availability Center.
2	Use Discovery Manager (requires separate license) to populate the CMDB with physical CIs discovered in the IT environment. A view is automatically created for each Discovery Manager package that is run. For more information, see *Discovery Manager Administration* Apply monitors in Monitor Administration to discovered CIs using the Monitor Deployment Wizard. For more information, see "Monitor Deployment Wizard" in *Configuring SiteScope Monitors*
3	You configure monitors in Monitor Administration. Defined monitors based on default sources (Business Process Monitor/Client Monitor, Real User Monitor, SiteScope) are automatically added to the CMDB as monitor CIs and added to the Monitors View. For more information, see *Working with Monitor Administration* To include Business Process Monitor locations in the monitor hierarchy in views, you must set the Business Process Monitor model to use Transaction/Location hierarchy structure (in Source Manager). For more information, see "Business Process Monitoring" in *Source Manager Administration* Custom sources can be created to bring third-party EMS topology CIs or XML-defined topology CIs into the CMDB. A view is automatically created for each custom source type that is defined. For more information, see *Source Manager Administration*
4	Create instance views and store them in folders. Create and manage the folder hierarchy as per organizational requirements. For more information, see *View Manager Administration*
5	Create a view that represents a logical segment of the business or IT infrastructure that you want to monitor in Dashboard (for example, a line of business or a server farm). For more information, see "Getting Started with IT Universe Manager" in *IT Universe Manager Administration*

Ref. No.	Comment
6	Define CIs on both the root and subtree level that map the organizational structure you want to reflect in the view (for example, geographical locations or business groups). For more information, see "Working with CIs in IT Universe Manager" in *IT Universe Manager Administration*
7	Add Dynamic Node Factory CIs to the view. CIs generated via the Dynamic Node Factory are automatically added to the CMDB. The Dynamic Node Factory subtree is dynamically generated in the view. Once generated, Dynamic Node Factory CIs can be added to other views. For more information, see "Working with Dynamic Node Factory" in *IT Universe Manager Administration*
8	Populate your view with CIs that already exist in the CMDB and are attached to other views (for example, create a relationship between a geographical location, the database servers at that location, and the SiteScope monitors monitoring those servers). For more information, see "Working with CIs in IT Universe Manager" in *IT Universe Manager Administration*
9	Populate your view with additional logical or physical CIs that you define (for example, NT servers). For more information, see "Working with CIs in IT Universe Manager" in *IT Universe Manager Administration*

How Do I Collect Data on the Performance of a Specific Business Process?

The flowchart below describes the process required to set up and use Business Process Monitor to collect data on the performance of specific business processes. The numbered elements are referenced in the table on the following page, which provides additional details about the steps and a reference to more information.

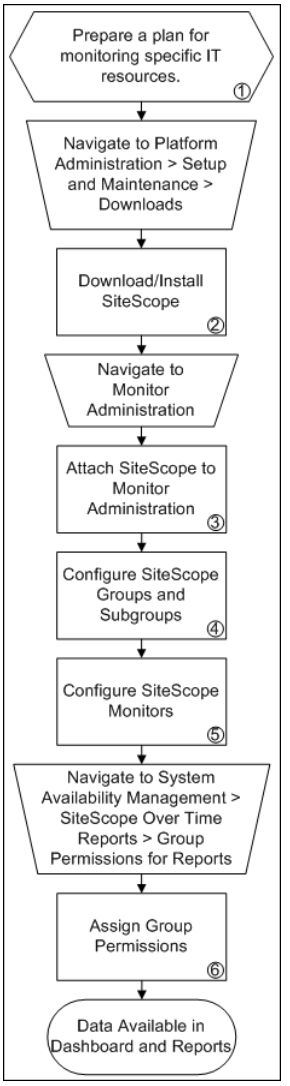


Ref. No.	Comment
1	Prepare a plan that maps out the specific applications and business processes for which you want to collect data. Consider the locations from where you want to emulate end users accessing the application. Include information about the monitored IT infrastructure components associated with the applications (for example, servers being monitored by SiteScope that are running a Web-based application against which you plan to run Business Process Monitor scripts).
2	Download Mercury Virtual User Generator (VuGen), the primary recording tool for use with Business Process Monitor, and install on machines of administrators responsible for script recording. For more information, see *Using Mercury Virtual User Generator* In certain circumstances you may need to record scripts with another Mercury recording tool such as QuickTest Professional. For more information, see "Scripting tools" on page 20
3	Download and save the Business Process Monitor installation file (for Windows or Solaris) to a local or network drive. Install Business Process Monitor on machines designated to run scripts recorded with Mercury script recording tools such as Mercury Virtual User Generator. You can run multiple Business Process Monitors from multiple platforms. For more information, see "Deploying Business Process Monitor" in *Business Process Monitor Administration*
4	Create scripts that include transactions that reflect the business processes for which you planned to collect data, and save them to a local or network drive. For more information, see *Script Recording Tips* and *Using Mercury Virtual User Generator*

Ref. No.	Comment
5	In the Script Repository, organize your uploaded scripts into folders. Scripts can also be uploaded to the Script Repository while creating a profile in Monitor Administration. For more information, see "Script Repository" in *Platform Administration*
6	Once defined, the profile and its monitors are added as CIs to the CMDB and are automatically attached to the Monitors View, from where they can be added to other views (if Monitors View is not updated, perform a synchronization in Source Manager). During profile creation, you can associate the profile or its monitors with existing CIs using Configuration Item Attachment Settings (for example you can associate the profile with an existing logical CI representing an application whose business processes are being monitored by Business Process Monitor). For more information, see "Creating Business Process Profiles" in *End User Management Data Collector Configuration*
7	Profile permissions set in the Monitors context in the Permissions Manager do not affect the permissions to view that profile in views defined in IT Universe Manager. Permissions for views must be set separately. For more information, see "Configuring User Permissions" in *Platform Administration*

How Do I Collect Data on the Performance of an IT Resource?

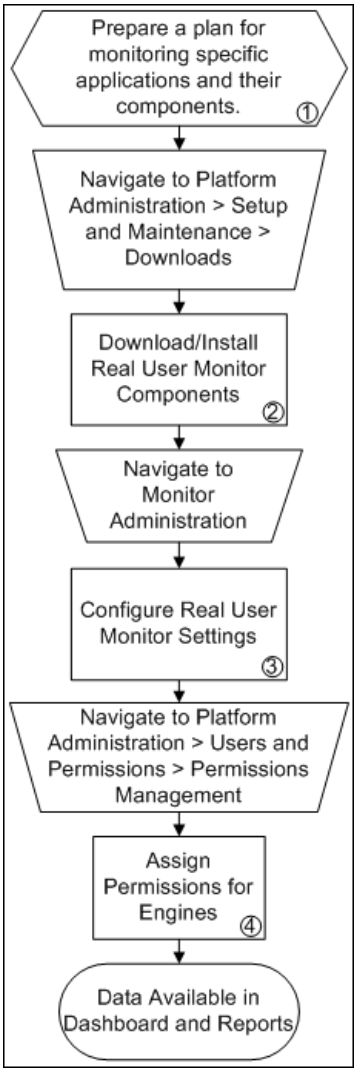
The flowchart below describes the process required to set up and use SiteScope to collect data on the performance of IT infrastructure components. The numbered elements are referenced in the table on the following page, which provides additional details about the steps and a reference to more information.



Ref. No.	Comment
1	Prepare a plan that maps out the specific IT infrastructure resources about which you want to collect data. Include information about the business process that are affected by the specified infrastructure components (for example, business processes—being monitored by Business Process Monitor—that are running on an application server against which you plan to run SiteScope monitors).
2	Download and save the SiteScope installation files (for Windows or Solaris) to a local or network drive. Install SiteScope on machines designated to run the SiteScope data collector. You can run multiple SiteScopes from multiple platforms. For more information, see *SiteScope Administration*
3	Attach SiteScope instances to Monitor Administration to be able to fully control and manage SiteScope from with Mercury Business Availability Center. It is also possible to configure SiteScope to be controlled in, but not report data to, Mercury Business Availability Center, or to remain as a standalone tool but report data to Mercury Business Availability Center for viewing in reports. For more information, see "Managing SiteScope in the Monitor Tree" in *Managing SiteScope*
4	Create groups and subgroups to organize the monitors to be deployed. For example, you can create groups of locations, server types, network resources, and so forth. For more information, see "Working with SiteScope Groups" in *Configuring SiteScope Monitors*
5	When configuring monitors, verify that Mercury BAC Logging settings are set as required. You can use the Monitor Deployment Wizard to deploy monitors onto existing CIs in the CMDB. You can also use Solution Sets to configure predefined sets of monitors on specific systems. For more information, see *Configuring SiteScope Monitors* Once defined, the SiteScope and its groups and monitors are added as CIs to the CMDB and are automatically attached to the Monitors View, from where they can be added to other views (if Monitors View is not updated, perform a synchronization in Source Manager). During monitor configuration, you can associate the monitor with existing CIs using Configuration Item Attachment Settings (for example you can attach the CPU monitor to an existing logical CI representing all machines whose CPU is being monitored).
6	For each defined user, assign permissions to view SiteScope groups and their subgroups in System Availability Management reports and custom reports. For more information, see "Group Permissions for Reports" in *Using System Availability Management*

How Do I Collect Data on Real User Traffic Accessing a Specific Application?

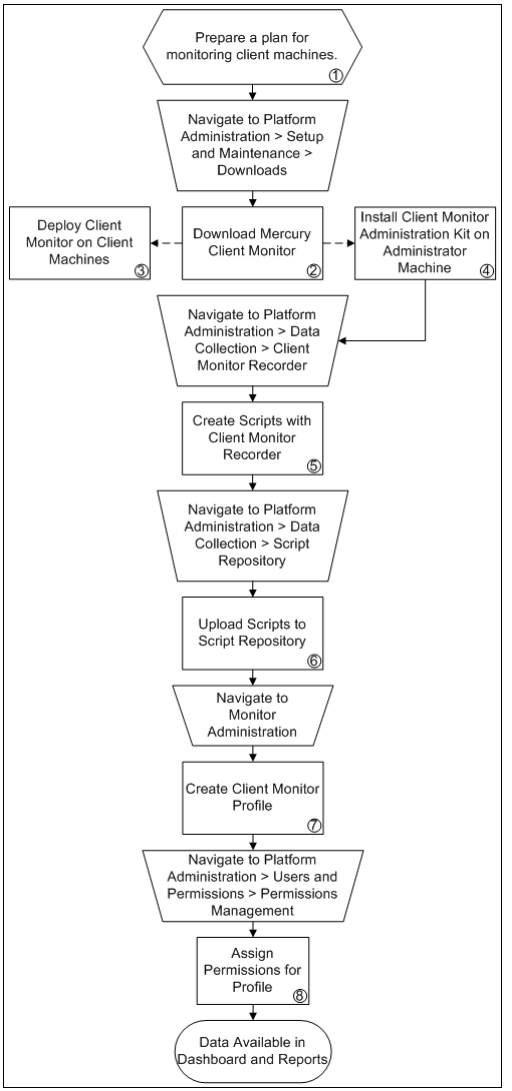
The flowchart below describes the process required to set up and use Real User Monitor to collect data on the performance of real users accessing defined applications. The numbered elements are referenced in the table on the following page, which provides additional details about the steps and a reference to more information.



Ref. No.	Comment
1	Prepare a plan that maps out the applications about which you want to collect data, and any specific pages, transactions, and end users on which you want to focus. Keep in mind that the Real User Monitor collects large quantities of data so it is recommended to focus only on the components considered critical for monitoring. Include information about the monitored IT infrastructure components associated with the applications (for example, servers being monitored by SiteScope that are running a Web-based application against which you plan to monitor real user traffic).
2	Install the Real User Monitor engine, probe, and MySQL database. Use the Real User Monitor Engine Web Console to administer connection parameters between Real User Monitor and Mercury Business Availability Center and for other engine administration tasks. For more information, see "Installing and Administering Real User Monitor" in *Real User Monitor Administration*
3	In Monitor Administration, you add the Real User Monitor engine you installed to the monitor tree. You then add one or more probes to the engine and configure the probe(s) to collect data from specific Web servers. In addition, you configure applications to monitor, and the pages, transactions, events and end users for which you want to collect specific data. For more information, see "Configuring the Real User Monitor" in *End User Management Data Collector Configuration* Once defined, the applications, pages, events, and end users are added as CIs to the CMDB and are automatically attached to the Monitors View and the various Real User Views (applications, end users, locations, and servers) from where they can be added to other views (if the views are not updated, perform a synchronization in Source Manager). When configuring new pages and transactions to monitor, you can associate the page or transaction with existing CIs using Configuration Item Attachment Settings. For more information, see "Real User Monitor Views in Dashboard" in *Using Dashboard*
4	Engine permissions set in the Monitors context in the Permissions Manager do not affect the permissions to view that engine in views defined in IT Universe Manager. Permissions for views must be set separately. For more information, see "Configuring User Permissions" in *Platform Administration*

How Do I Collect Data on the Performance of an Application Being Accessed by Specific Users?

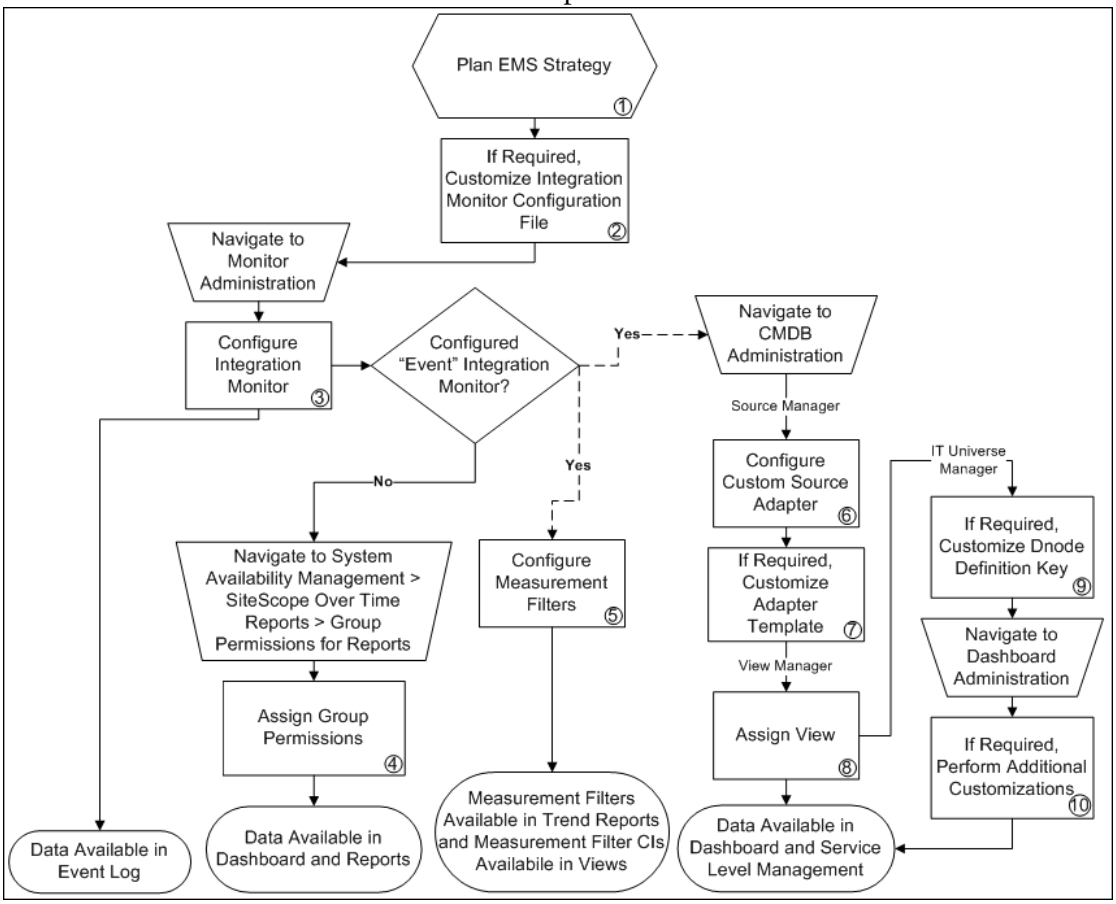
The flowchart below describes the process required to set up and use Client Monitor to collect data on the performance of an application being used by specific users. The numbered elements are referenced in the table on the following page, which provides additional details about the steps and a reference to more information.



Ref. No.	Comment
1	Prepare a plan that maps out the specific clients/customers, applications, and business processes for which you want to collect data. Include information about the monitored IT infrastructure components associated with the clients and applications (for example, servers being monitored by SiteScope that are running a Web-based application being accessed by a key customer on whose desktop Client Monitor will be installed).
2	Download and save the MCMSetup.exe file to a local or network drive. It is required for both installing the Client Monitor Administration Kit and instances of Client Monitor for distribution to desktops of clients/customers. For more information, see "Installing Client Monitor" in *Client Monitor Administration*
3	Select the method of Client Monitor distribution suitable for your organization: single-machine installation, multiple-machine installation, or silent installation. For more information, see "Installing Client Monitor" in *Client Monitor Administration*
4	Install the Client Monitor Administration Kit on machines from which the administrator will access the Client Monitor Recorder in Mercury Business Availability Center. For more information, see "Installing Client Monitor" in *Client Monitor Administration*
5	The Client Monitor Administration Kit must be installed on the machine from which the administrator accesses the Client Monitor Recorder in Mercury Business Availability Center. For more information, see *Using Client Monitor Recorder*
6	In the Script Repository, organize your uploaded scripts into folders. Scripts can also be uploaded to the Script Repository while adding them to a profile in Monitor Administration. For more information, see "Script Repository" in *Platform Administration*
7	Once defined, the profile and its monitors are added as CIs to the CMDB and are automatically attached to the Monitors View, from where they can be added to other views (if Monitors View is not updated, perform a synchronization in Source Manager). During profile creation, you can associate the profile or its monitors with existing CIs using Configuration Item Attachment Settings (for example you can associate the profile with an existing logical CI representing a group of clients whose desktops are being monitored using Client Monitor). For more information, see "Managing Business Process Profiles and Creating Client Monitor Profiles" in *End User Management Data Collector Configuration*
8	Profile permissions set in the Monitors context in the Permissions Manager do not affect the permissions to view that profile in views defined in IT Universe Manager. Permissions for views must be set separately. For more information, see "Configuring User Permissions" in *Platform Administration*

How Do I Integrate Data from Third-Party Sources (EMS Data) into Mercury Business Availability Center?

The flowchart below describes the process required to integrate data from third-party enterprise management systems (EMS data) into Mercury Business Availability Center using SiteScope Integration Monitors. The numbered elements are referenced in the table on page 75, which provides additional details about the steps and a reference to more information.



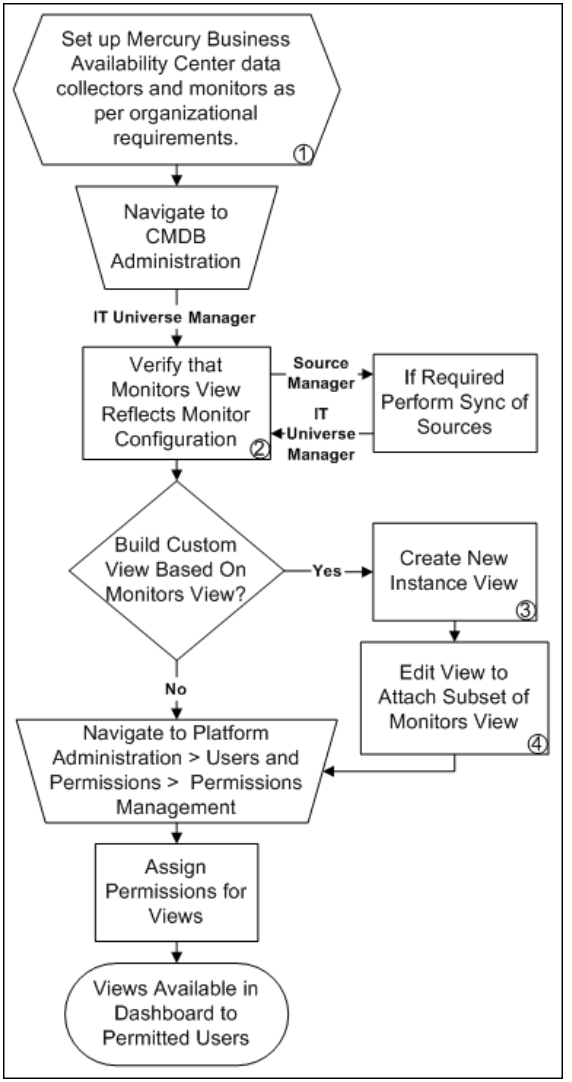
Ref. No.	Comment
1	Review the Integration Monitor types. Consider the type of information you want to see in Mercury Business Availability Center from your EMS system. Determine whether one of the specific Integration Monitors meets your organization's needs or whether a generic Integration Monitor (Technology Log File, Database, SNMP, Web Service) is required. For more information, see "Working with SiteScope Integration Monitors" in *Configuring SiteScope Monitors* Review the Event and Metrics samples and fields to understand how the incoming EMS metadata maps to Mercury Business Availability Center metadata. For more information, see "Integration Monitor Configuration Files" in *Configuring SiteScope Monitors*
2	You customize Integration Monitor configuration files to correctly map the data Integration Monitors collect to a format recognizable by Mercury Business Availability Center. For Technology Integration Monitors, you must create an appropriate configuration file using one of the generic configuration file templates. Integration Monitors designed for use with specific EMS applications only require modification if specific customizations are required. For more information, see "Integration Monitor Configuration Files" in *Configuring SiteScope Monitors*
3	After monitors are defined in Monitor Administration, data can be seen in the Event Log. Depending on whether you configure Integration Monitors that use the metrics data template or Integration Monitors that use the event data template, you proceed differently to enable the data to be viewed in Mercury Business Availability Center. For the step-by-step process of setting up and using SiteScope monitors, see "How Do I Collect Data on the Performance of an IT Resource?" on page 68.
4	For each defined user, assign permissions to view SiteScope groups and their subgroups in System Availability Management reports and custom reports. For more information, see "Group Permissions for Reports" in *Using System Availability Management*

Ref. No.	Comment
5	You must create measurement filters to enable viewing Integration Monitor event data in trend reports. In addition, each measurement filter created gets added to the UDX Measurement Filters view as a CI. These CIs can be added to Dashboard views and SLAs. For more information, see "Working with Measurement Filters" in *Platform Administration*
6	If you configured a specific Integration Monitor that has a corresponding custom source adapter, configure and start the relevant source adapter in Source Manager. If you configured a specific Integration Monitor that does not have a corresponding custom source adapter, or if you configured a (generic) Technology Integration Monitor, configure and start the Generic EMS source adapter. For more information, see "Custom Source Adapter Details" in *Source Manager Administration* If using the Generic EMS source adapter, you may want to customize (in IT Universe Manager) the Generic EMS DNode Definition Key or the selector for the Generic EMS Dynamic Node Factory CI (to refine the filter so that it picks up only relevant samples from the Bus). For more information, see "Working with Dynamic Node Factory" in *Source Manager Administration*
7	In certain cases it may be required to edit the custom source adapter template, for example to modify the KPIs or rules used by the custom source. For more information, see "Working with Templates" in *Source Manager Administration*
8	In View Manager, select the Integrations folder and edit the properties for the relevant view to assign the view to IT Universe Manager and/or Dashboard and Service Level Management. This enables you to administer the view in IT Universe Manager and see it in the Dashboard and Service Level Management applications. For more information, see "Creating and Editing Views" in *View Manager Administration*

Ref. No.	Comment
9	For Integration Monitor views that use Dynamic Node Factory, a Dynamic Node Factory CI is automatically added to the view once the custom source adapter is defined. If required, you can customize the Dynamic Node Factory CI by editing the DNode Definition Key or other Dynamic Node Factory CI properties in IT Universe Manager. For more information, see "Working with Dynamic Node Factory" in *IT Universe Manager Administration* You may need to customize the DNode Definition Key, for example, if you added the Generic EMS adapter and want to filter part of the incoming data, or if you made certain types of customizations to the configuration file for one of the predefined Integration Monitors such as modifying data fields that also appear in the DNode Definition Key. For more information, see "DNode Definition Key Property" in *IT Universe Manager Administration*
10	In Dashboard Administration, customize the views for your Integration Monitor and/or related repository elements as required. For the step-by-step process of customizing the way a view is displayed in Dashboard to reflect your organizational requirements, see "How Do I Customize the Way Mercury Business Availability Center Displays My Views in Dashboard?" on page 84. For a sample scenario that describes how to customize repository entities so that unique terminology and elements of the business can be seen in Dashboard, see "How Do I Customize Dashboard Repository Entities to Model My Business World? A Sample Scenario" on page 86.

How Do I View My Already Created Monitors in Dashboard?

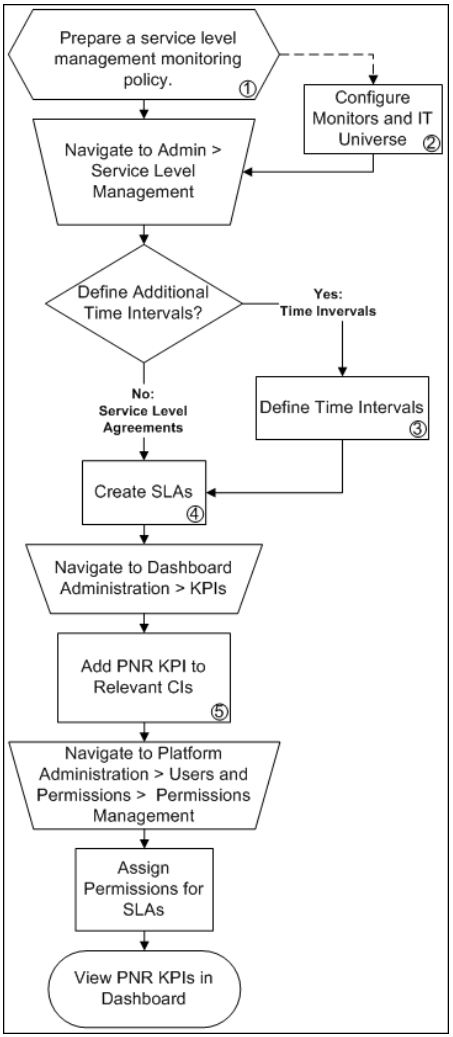
The flowchart below describes the process required to view, in Dashboard, monitors that have already been created in Monitor Administration, including viewing all monitors or a monitor subset (in default or custom views). The numbered elements are referenced in the table on the following page, which provides additional details about the steps and a reference to more information.



Ref. No.	Comment
1	Business Process Monitor, Real User Monitor, Client Monitor, and SiteScope monitor CIs defined in Monitor Administration automatically populate the CMDB and can be seen in the Monitors View.
2	Monitors View is updated once per hour. If Monitors View is not updated, perform a synchronization in Source Manager. For more information, see "Using Source Manager" in *Source Manager Administration*
3	Create a top level logical view that represents the segment of the Monitors View to see in Dashboard. (For example, choose one specific line of business on which to focus.) For more information, see "Working with CIs in IT Universe Manager" in *IT Universe Manager Administration*
4	Using the Quick Edit function on the new view, select Monitors View, and choose the CIs to add to the new view. (For example, attach one specific geographical location on which to focus.) For more information, see "Working with CIs in IT Universe Manager" in *IT Universe Manager Administration*

How Do I Set Up SLAs and Track Their PNR KPIs in Dashboard?

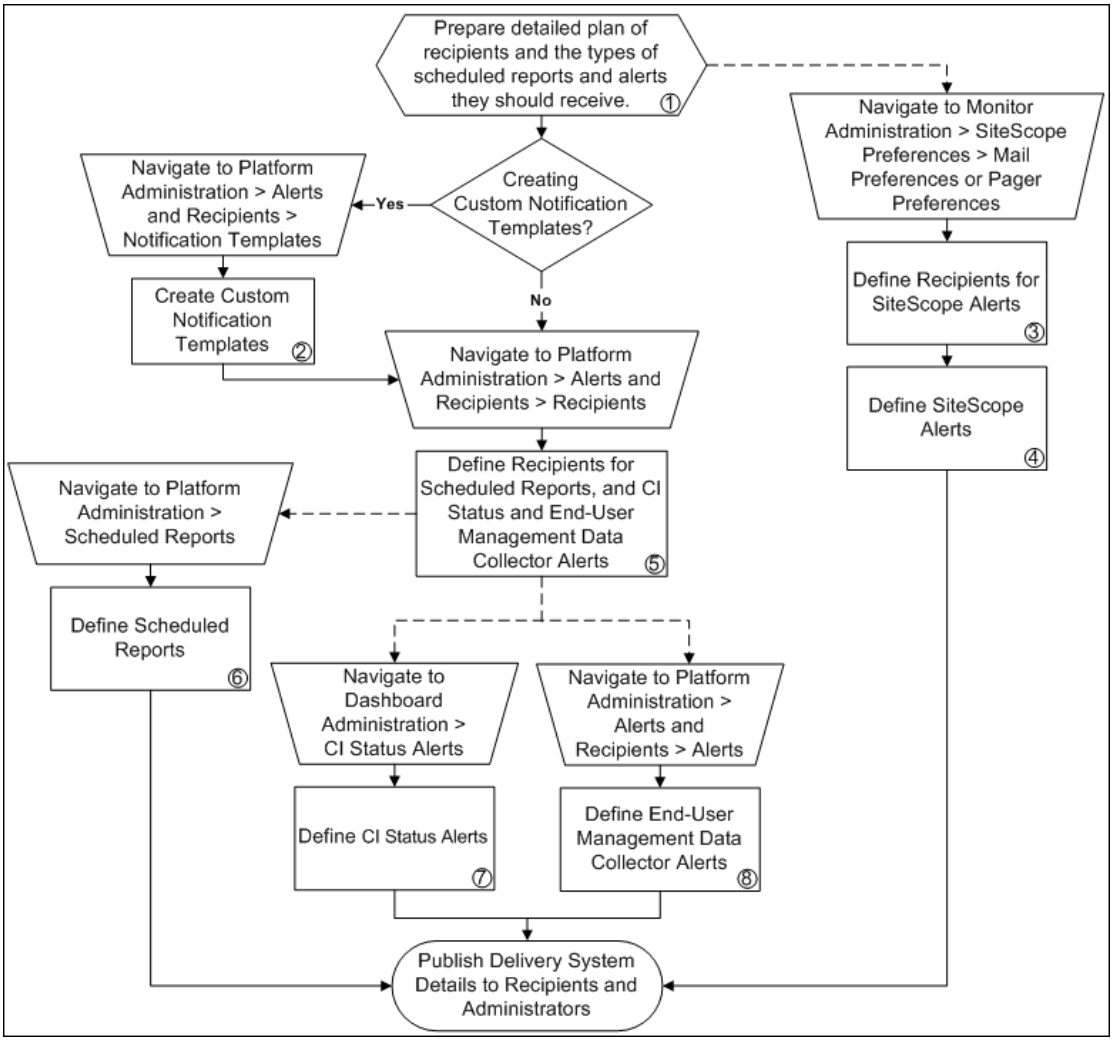
The flowchart below describes the process required to set up SLAs and track their PNR KPIs in Dashboard. The numbered elements are referenced in the table on the following page, which provides additional details about the steps and a reference to more information.



Ref. No.	Comment
1	Create a service level management monitoring plan by establishing which of the organization's written service level agreements are to be monitored using Mercury Business Availability Center, and by mapping out the IT infrastructure and business processes covered by those service level agreements.
2	Ensure that monitor configuration and IT Universe model setup reflect the service level management plan.
3	If time intervals other than the defaults (24x7, business hours) are required, define them. For more information, see "Time Intervals" in *Application Administration*
4	Define SLAs that reflect the organization's written service level agreements that are to be monitored (as per the service level management plan). When defining SLAs, ensure that the following conditions exist so that PNR KPIs will later display properly in Dashboard: ➤ The SLA must include the CIs whose PNR you want to track in Dashboard. ➤ The SLA must include the Availability KPI for each CI to which you plan to add the PNR KPI. Examples of SLAs follow: ➤ Ensure that users can access the finance site within eight seconds for 98.5% of the time during West Coast business hours. After business hours (that is, 5:00 PM to 9:00 AM), ensure that users can access the site within 10 seconds for 95% of the time. ➤ Ensure that the average round-trip transmission between a UUNET-designated Hub Router in the IT department and a UUNET-designated Hub Router in the finance office in the Chicago metropolitan area will take 120 milliseconds or less during business hours and 150 milliseconds or less after business hours. For more information, see "Service Level Agreements (SLAs)" in *Application Administration*
5	Add a PNR KPI to each CI whose PNR you want to track in Dashboard. For more information, see "Attaching a PNR KPI to a CI" in *Application Administration*

How Do I Set Up a Report and Alert Delivery System?

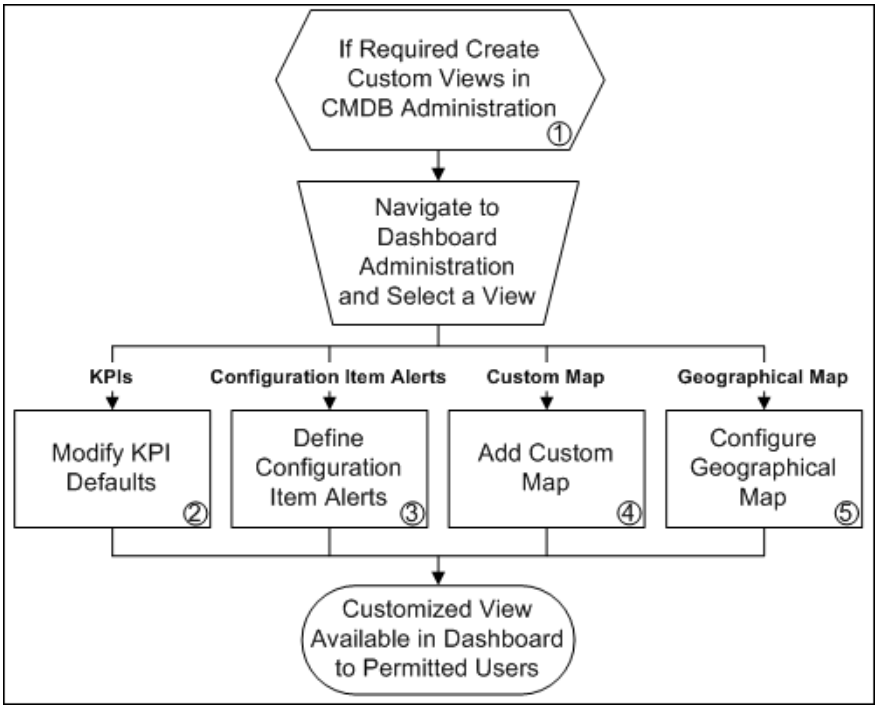
The flowchart below describes the process required to set up a system for delivering scheduled reports and alerts to defined recipients. The numbered elements are referenced in the table on the following page, which provides additional details about the steps and a reference to more information.



Ref. No.	Comment
1	List required recipients of scheduled reports and alerts, including contact information and required delivery method for alerts (e-mail, SMS, pager). Map out the types of scheduled reports and alerts you plan to deliver: ➤ Scheduled Reports include the Performance Update report, an out-of-the-box report on the performance of Business Process Monitor transactions, and user reports, which can include performance data collected by all data collectors. ➤ Alerts include CI status alerts (alert you to status changes in KPIs associated with configuration items), End-User Management data collector alerts (alert you to performance issues related to data collected by Business Process Monitor, Client Monitor, and Real User Monitor), and SiteScope alerts (alert you to performance issues related to data collected by SiteScope).
2	If required, create custom notification templates for End-User Management data collector alerts to customize the format and information included in alert e-mails. For more information, see "Alert Notification Templates" in *Platform Administration*
3	In Monitor Administration, you define alert recipients for SiteScope alerts. You can specify recipients for e-mail or pager delivery. For more information, see "Working with E-mail Recipient Profiles" and "Working with Pager Recipient Profiles" in *Managing SiteScope*
4	Define SiteScope alerts as required to alert recipients to SiteScope monitor status changes. For more information, see *Configuring SiteScope Alerts*
5	On the Recipients page, you define system recipients for scheduled reports and alerts (except SiteScope alerts). For alerts you can specify e-mail, SMS, or pager delivery methods. If required, enter specific alert delivery schedules (for example, recipients who receive alerts during business hours versus evenings and weekends). For more information, see "Configuring and Selecting Recipients" in *Platform Administration*
6	Define scheduled reports as required. You can select the Performance Update report for delivery, as well as user reports (custom reports and trend reports) if they are defined in the system. For more information, see "Scheduled Reports" in *Platform Administration*
7	Define CI Status alerts as required to alert recipients to KPI status changes for specific CIs and KPIs being monitored in Dashboard. For more information, see "Configuring CI Status Alerts" in *Application Administration*
8	Define End-User Management data collector alerts as required to alert recipients to performance variance of Real User Monitor entities or Business Process Monitor/Client Monitor transactions. For more information, see "Creating Alert Schemes" in *Platform Administration*

How Do I Customize the Way Mercury Business Availability Center Displays My Views in Dashboard?

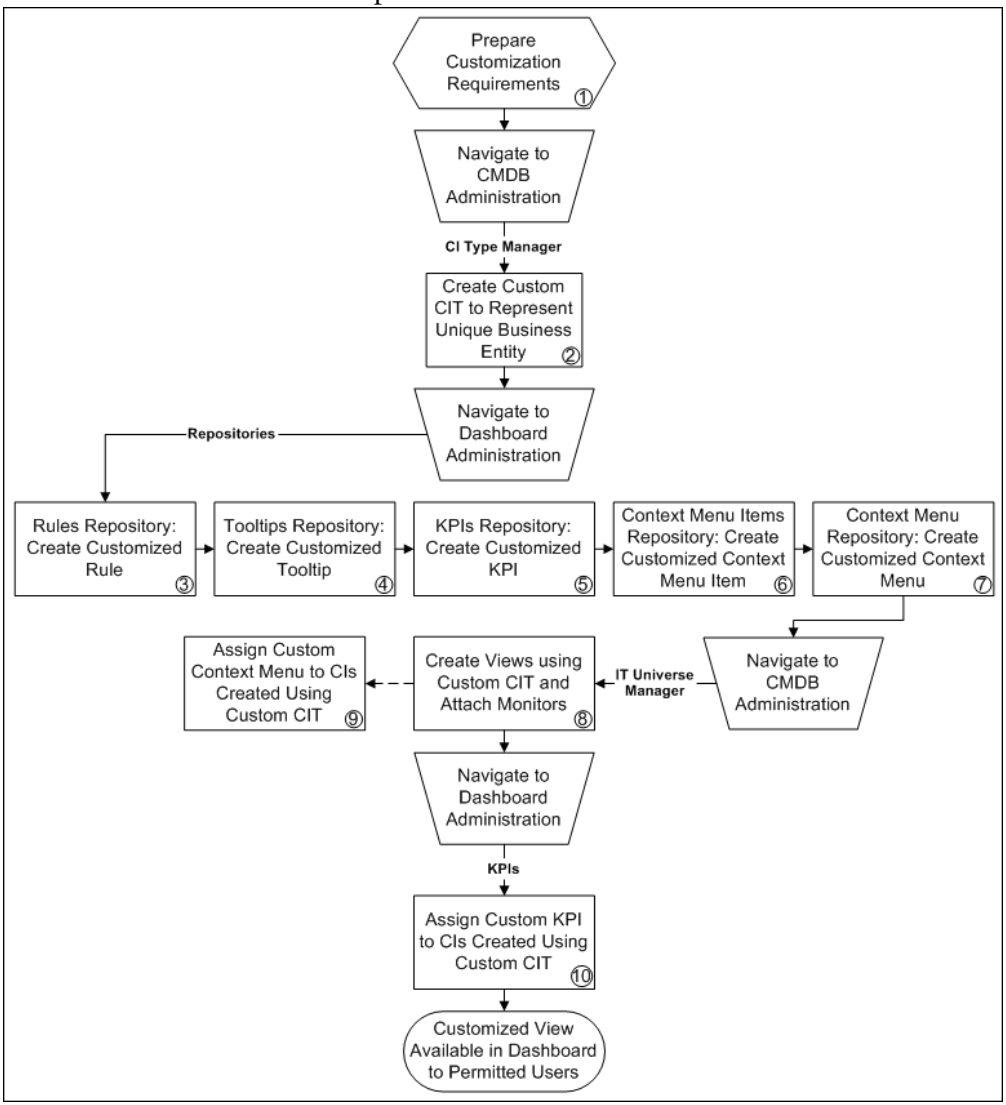
The flowchart below describes the process of customizing the way a view is displayed in Dashboard to reflect your organizational requirements. The numbered elements are referenced in the table on the following page, which provides additional details about the steps and a reference to more information.



Ref. No.	Comment
1	Mercury Business Availability Center provides several default views. If required, you can create custom views in CMDB Administration. For the step-by-step process of creating views to reflect your IT environment, see "How Do I Reflect My IT Environment in Mercury Business Availability Center?" on page 62.
2	Monitor CIs associated with default sources generally have default KPIs. For example, Business Process Monitor, Real User Monitor, Client Monitor, and SiteScope monitor CIs that you configure in Monitor Administration all have default KPIs. Note that CIs with default KPIs that are placed under other CIs in a view generally propagate their KPIs upward to the parent CIs. You may want to modify the business rule (or its properties) used by a KPI. Alternatively, you may want to modify or delete a KPI associated with a higher level CI in a view if the KPI originated from a lower level CI, was propagated upward, and is not appropriate for the higher lever CI (for example, if you want to only see performance and not availability). You may also want to add a new KPI to a higher level CI. You can also choose to save historical data for a KPI if you want to see the associated data in the KPI over Time report. For more information, see "Configuring KPIs" in *Application Administration*
3	Define CI Status Alerts to alert defined recipients to status changes in KPIs for specified CIs. For more information, see "Configuring CI Status Alerts" in *Application Administration*
4	You can add a custom image upon which you place status indicators that display the real time status for specified CIs. Each status indicator displays the worst status from all KPIs associated with that CI. For example, if you place on the image a status indicator for a Line of Business CI, the status indicator will display the worst status of all KPIs associated with the Line of Business CI. The custom image can be useful for representing data centers, geographical distribution of IT resources, and so forth. For more information, see "Configuring the Custom Map" in *Application Administration*
5	The geographical map displays status indicators showing real time status for CIs at different locations. When location parameters are defined for a CI in CMDB Administration, a status indicator automatically appears on the geographical map at the defined location. When there are multiple CIs with the same defined location, one status indicator is displayed for the location, showing the worst status for all KPIs associated with all CIs at that location. Use the geographical map's zoom and center functions to focus on the parts of the map relevant to the defined locations. For more information, see "Configuring the Geographical Map" in *Application Administration*

How Do I Customize Dashboard Repository Entities to Model My Business World? A Sample Scenario

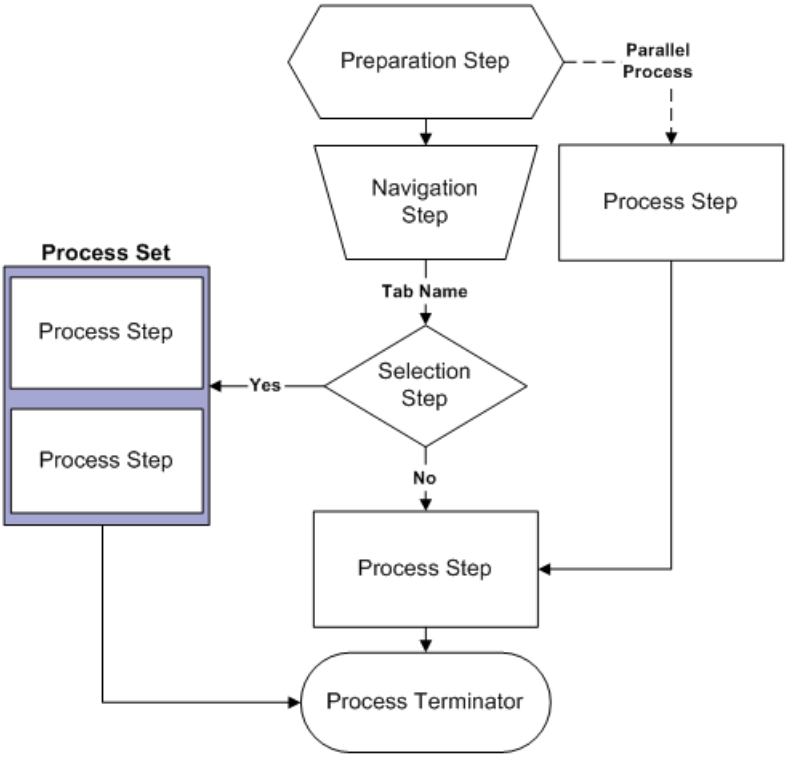
The flowchart below describes a sample scenario for a company that wishes to customize repository entities so that unique terminology and elements of the business can be seen in Dashboard. The numbered elements are referenced in the table on the following page, which provides additional details about the steps.



Ref. No.	Comments
1	A cruise ship company wishes to define the following unique business elements to see in Dashboard: a logical CI called Cruise Ship to add to views; a custom KPI to monitor the dollar impact of down time of monitored ship systems; a customized context menu for Cruise Ship CIs that includes a URL link to its fleet intranet site.
2	In the CI Type Manager, the company's Mercury Business Availability Center administrator adds a new logical CI type called Cruise Ship to the Business folder. In the Attributes page, she adds a new editable attribute, ship_serial_number, and marks the data_name attribute as the key attribute (since it serves as a unique identifier for each ship).
3	In the Business Rules repository, the administrator creates a customized rule to deal with the dollar impact of ship system non-availability by cloning the Impact Over Time Rule, renaming the cloned rule to Ship Impact Over Time Rule, and editing the DollarImpactFactor parameter to 1000 (to represent a dollar loss of $1,000 per hour).
4	In the Tooltips repository, the administrator edits the description of the new tooltip associated with newly created Ship Impact Over Time Rule that appears in the Custom Tooltips section to say: Dollar loss due to no availability on ship system
5	In the KPIs repository, the administrator creates a customized KPI to monitor the dollar impact of ship system non-availability by cloning the OT Impact KPI, renaming the cloned KPI to Ship OT Impact, and modifying the selected applicable rules—clearing Impact Over Time Rule and selecting Ship Impact Over Time Rule.
6	In the Context Menu Items repository, the administrator clones the Go to Report item, renames the cloned item Go to Ship, selects the Dashboard generic URL pre-processor class, edits the value of the URL parameter to the desired URL address, and selects the Open window post-processor class.
7	In the Context Menus repository, the administrator clones the Group Menu, renames the cloned item Ship Group Menu, and edits Ship Group Menu to add Go to Ship as a new item in the Go to Report menu item list.
8	In IT Universe Manager, the administrator creates a new instance view called Cruise Ship Fleet, and adds a Cruise Ship CI for each ship in the fleet. She attaches relevant SiteScope and Business Process Monitors that were previously configured to monitor ship systems.
9	When adding Cruise Ship CIs to views, the administrator assigns the Ship Group Menu as the context menu for the CIs. The menu will then be visible in Dashboard views.
10	After creating views that include the Cruise Ship CIs, in the Dashboard Administration KPIs tab the administrator assigns the new KPI Ship OT Impact to the Cruise Ship CIs. This KPI will then be visible in Dashboard views to users with appropriate permissions on the views.

Flowchart Legend

The following legend describes the shapes used in the flowcharts.



10

Using the Mercury Business Availability Center Documentation Library

This chapter provides instructions and recommendations on using, navigating, and updating the Mercury Business Availability Center Documentation Library.

This chapter describes:	On page:
Working with the Documentation Library	90
Documentation Library Guides	93
Navigating the Documentation Library	98
Updating the Documentation Library	99
Accessing Additional Online Resources	101

Working with the Documentation Library

The Documentation Library is an online help system that describes how to deploy, administer, and use Mercury Business Availability Center. You access the Documentation Library using a Web browser. For a list of supported Web browsers, see "Viewing Mercury Business Availability Center Site" in *Deploying Servers*.

The Documentation Library is best viewed from a browser with Java support. If you do not have Java support on your browser, download the Sun Java plug in from the Sun Java Web site (http://java.com/en/index.jsp). Note that if Java support is not available, the Documentation Library automatically opens using the JavaScript implementation. The JavaScript implementation provides the same basic functionality as the Java implementation, however does not allow use of the Favorites tab within the navigation pane (for details on the navigation pane, see "Navigating the Documentation Library" on page 98).

All major guides in the Documentation Library are available in PDF format for printing or on-screen reading in Adobe Acrobat Reader.

Post-release updates to documentation are posted to the Mercury Documentation Portal on a periodic basis. For details on downloading updates, see "Updating the Documentation Library" on page 99.

This section covers the following topics:

- Accessing the Documentation Library. For details, see below.
- Accessing Guides in PDF Format. For details, see page 91.
- Documentation Library Functionality. For details, see page 92.

Accessing the Documentation Library

You can access the Documentation Library in the following ways:

- Click **Documentation Library** in the Mercury Business Availability Center Help menu to open the Documentation Library home page. The home page provides quick links to the main help topics.
- Click **Help on this page** in the Mercury Business Availability Center Help menu, click the **Help** button in a dialog box, or click the help icon within a specific context, to open the Documentation Library to the topic that describes the current page or context.



- Double-click **index.htm** in the **Documentation\doc_lib** directory on the Mercury Business Availability Center Documentation and Utilities CD-ROM.
- Access the Documentation Library from the Mercury Business Availability Center Documentation Portal area on the Mercury Customer Support Web site (support.mercury.com).

Accessing Guides in PDF Format

To open guides in PDF format, make sure you have Acrobat Reader 4.0 or later installed on the machine.

You can access guides in PDF format from the following locations:

- From the Printer-Friendly Documentation page in the Documentation Library. You can access this page from the PDFs tab on the Documentation Library home page.
- From the **Documentation\pdfs** directory on the Mercury Business Availability Center Documentation and Utilities CD-ROM. Open the **PDF_Index.html** file to select from a menu of available PDF files.
- From the Mercury Business Availability Center Documentation Portal area on the Mercury Customer Support Web site (support.mercury.com).

Documentation Library Functionality

The following functionality is available from the top frame in the Documentation Library main pane.



➤ **Show Navigation** button. Click to display the navigation pane, which includes the Contents, Index, Search, and Favorites tabs. For details on the Navigation pane, see "Navigating the Documentation Library" on page 98. Note that this button is only displayed when the navigation pane is closed.



➤ **Show in Contents** button. Click to highlight, in the Contents tab, the entry corresponding to the currently displayed page. Note that this button is only displayed when the navigation pane is open.



➤ **Previous** and **Next** buttons. Click to move forward or backward in the guide currently displayed.



➤ **Send Feedback** button. Click to open your e-mail client and send feedback to Mercury. An e-mail message opens with the **To** and **Subject** fields already completed and a link to the current page in the message body. Make sure to complete the e-mail by entering your feedback. Note that you must have an e-mail client configured on the machine for this function to operate correctly.



➤ **Print** button. Click to print the currently displayed page.



➤ **Bookmark** button. Click to save a browser bookmark for the currently displayed page.

Documentation Library Guides

The Documentation Library consists of the following guides:

Name	Description
Getting Started with Mercury Business Availability Center (this guide)	Helps you get Mercury Business Availability Center up and running in your organization by providing a roadmap, process checklists and flowcharts, and other key information.
Glossary	Defines key terms used in Mercury Business Availability Center.
Preparing the Database Environment	Describes how to prepare and configure the enterprise database infrastructure to work optimally with Mercury Business Availability Center, including how to set up a recommended database configuration.
Deploying Servers	Describes how to deploy Mercury Business Availability Center servers in the enterprise network environment.
Hardening the Platform	Describes how to harden the Mercury Business Availability Center platform to provide a secure environment for the Mercury Business Availability Center software and hardware.
Data Collector Overview	Provides an overview of the various data collectors available in Mercury Business Availability Center and how they work with their various monitored environments.
Business Process Monitor Administration	Describes how to deploy and administer the Business Process Monitor data collector.
Client Monitor Administration	Describes how to deploy and administer the Client Monitor data collector.
SiteScope Administration	Describes how to install and administer the SiteScope data collector.
Real User Monitor Administration	Describes how to deploy and administer the Real User Monitor data collector.

Name	Description
Script Recording Tips	Provides tips on recording Business Process Monitor scripts for use in Mercury Business Availability Center.
Using Mercury Virtual User Generator	Describes how to work with the Mercury Virtual User Generator (VuGen) to create scripts for Business Process profiles.
Using Client Monitor Recorder	Describes how to use the Client Monitor recorder to record business process to be monitored on client machines.
Platform Administration	Describes how to configure and administer the Mercury Business Availability Center platform, including database management, alert configuration, and user permission and security administration.
Working with the CMDB	Provides an introduction to working with the CMDB and describes how to work with the View Explorer.
IT Universe Manager Administration	Provides detailed instructions on how to configure and administer the Mercury Business Availability Center IT Universe.
View Manager Administration	Describes how to create, and navigate through, the views in the CMDB.
Discovery Manager Administration	Describes how to activate the discovery patterns needed to run the discovery process.
Discovery Manager Tutorial	Teaches how to run the discovery process in Mercury Business Availability Center.
Source Manager Administration	Describes how to work with the CMDB Administration Source Manager. The Source Manager's predefined definitions provide all the tools required to harness data from the data sources used by Dashboard, and enable using the received information to build views for the Dashboard application.

Name	Description
CI Type Manager Administration	Describes how to work with the different types of configuration items.
Working with Monitor Administration	Provides information on working with the enterprise tree, navigating the tabs, creating filters that customize monitoring information, and changing and updating configurations across the entire monitoring infrastructure.
End User Management Data Collector Configuration	Describes how to configure Business Process Monitor and Client Monitor profiles and monitors, and the Real User Monitor, within Monitor Administration.
Managing SiteScope	Provides information about managing a SiteScope server within Monitor Administration, including defining preferences and ensuring the health of the SiteScope server and its running monitors.
Configuring SiteScope Monitors	Describes how to configure within Monitor Administration each of the SiteScope monitors.
Configuring SiteScope Alerts	Provides instructions on how to configure SiteScope alerts.
Configuring SiteScope Reports	Provides instructions on how to configure SiteScope reports.
Advanced Monitor Options	Provides details on advanced SiteScope topics, including working with SSH and using regular expressions.
Application Administration	Describes how to configure and administer Mercury Business Availability Center applications, including Dashboard, Service Level Management, and End User Management.
Repositories Administration	Describes how to configure and customize the repositories.

Name	Description
Using My BAC	Describes how to work with the My BAC application, a real-time personalizable portal that individual users can customize to display key content relevant to them.
My BAC Administration	Describes how to work with the My BAC configuration pages, where you manage portal modules (including portlets), and set viewing permissions.
Working with Applications	Provides general information on working with Mercury Business Availability Center applications, including working with reports and configuring user reports.
Using Dashboard	Describes how to work with the Mercury Business Availability Center Dashboard.
Using Service Level Management	Describes how to work with the Service Level Management application.
Using End User Management	Describes how to work with the End User Management application.
Using System Availability Management	Describes how to work with the System Availability Management application.
Using Application Performance Lifecycle	Describes how to work with the Application Performance Lifecycle application.
Reference Information	Provides general reference information (for example, allowed names and time zones) as well as details on working with Mercury Business Availability Center log files and samples.

Name	Description
Integrating with Third-Party Applications	Describes how to work with Mercury Business Availability Center third-party integration tools, including the Generic Data Engine API (used to extract data from Mercury Business Availability Center for use with third-party or custom tools) and EMS adapters (used to integrate alerts generated by Mercury Business Availability Center into your enterprise management console).
Working in an I18N Environment	Describes various considerations and limitations when working in a non-English or multi-language environment.
Troubleshooting Resources	Lists resources that are available to aid in troubleshooting problems that arise while working with or administering Mercury Business Availability Center.
Documentation Library Updates	Lists details of updates to the Documentation Library.

Navigating the Documentation Library

The Documentation Library is an integrated help system that can be navigated in the following ways:

- **From the home page.** To access the home page, select **Documentation Library** in the Mercury Business Availability Center Help menu. The home page can also be accessed from the Contents tab.

  The home page is divided into the following tabs:

  - **Main Topics tab.** The Main Topics tab organizes the various guides contained in the Documentation Library into logical sections.
  - **How Do I...? tab.** The How Do I...? tab provides direct links to the step-by-step process flows, which appear in the chapter "How Do I...? A Task Reference for Administrators" in this guide.
  - **PDFs tab**. The PDFs tab is organized similar to the Main Topics tab, but provides links to the guides in PDF format.

- **From the Navigation pane.** To access the navigation pane if it is not being displayed, click the **Show Navigation** button.

  The navigation pane is divided into the following tabs:

  - **Contents tab.** The Contents tab organizes the various guides in a hierarchical tree, enabling direct navigation to a specific guide or topic.
  - **Index tab.** The Index tab enables you to select a specific topic to display. Double-click the index entry to display the corresponding page. If your selection occurs in multiple documents, a dialog box is displayed enabling you to select a context.
  - **Search tab.** The Search tab enables you to search for specific topics or keywords. Results are returned in ranked order.
  - **Favorites tab.** The Favorites tab enables bookmarking specific pages for quick reference. Note that the Favorites tab is only available when using the Java implementation of the Documentation Library. If your browser does not support Java, the JavaScript implementation is automatically used and the Favorites tab is not displayed.

Updating the Documentation Library

Note to Mercury Managed Services customers: This section is not relevant to Mercury Managed Services customers, who always have access to the latest documentation via Mercury Managed Services servers.

Mercury may periodically update its product documentation with new information. Mercury Business Availability Center administrators can choose from the following options to gain access to the latest version of the Documentation Library:

- manually download files. For details, see below.
- configure Web access. For details, see page 101.

Manually Download Files

Manually download files from the Mercury Documentation Portal, and update the Documentation Library files located on the local Mercury Business Availability Center server. This option is required if access to the Documentation Library is set to local access (default setting).

To update local Documentation Library files:

1. Click the **Mercury Documentation Portal** link from the Mercury Business Availability Center Help menu, or in the Customer Support Web site click the **Documentation** link.
2. Select the product name.

   Note that if the 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 Mercury Documentation Portal opens to the Downloads page.

   The Downloads page lists documentation updates and provides further instructions on how to update the files on your local Mercury Business Availability Center server.

4 Click a document link to download the required documentation. Save the files to a temporary location.

5 Replace the older files on the local Mercury Business Availability Center server with the newer ones you downloaded. It is recommended that you back up files that you plan to delete to a temporary location until verifying that the newer files can be accessed.

Documentation resources are located in the following directory on the Mercury Business Availability Center server (or Centers server if installed separately):
<server_name>\MercuryAM\AppServer\webapps\site.war\amdocs\<version>\<language>\<resource file>

For example:

my_am_server\MercuryAM\AppServer\webapps\site.war\amdocs\6.1.0.0\eng\doc_lib

The following resource file directories exist:

- **doc_lib.** Contains the complete set of Mercury Business Availability Center Documentation Library files. To update the complete Documentation Library, delete all contents of this directory and then copy the new Documentation Library files into the directory.
- **pdfs.** Contains Mercury Business Availability Center Documentation Library files in PDF format. To update a PDF file, replace it.
- **whatsnew.** Contains the What's New file. To update, replace the file.

Configure Web Access

Configure Web access to the Documentation Library. When this option is chosen, the Documentation Library is served via the Web, from Mercury servers. When access via the Web is chosen, the most updated version of the Documentation Library is always displayed.

To configure Web access to the Documentation Library:

1. In the Mercury Business Availability Center Administration Console, open the Infrastructure Settings Manager from **Admin** > **Platform** > **Setup and Maintenance**.
2. Select the **Foundation** > **Business Availability Center Interface** context.
3. Change the value of the **Enable Access to Web-based Documentation Library** setting in the **Business Availability Center Interface - Documentation Access** table to **True**.
4. Restart the Mercury Business Availability Center servers (Centers Servers in a distributed architecture).

Accessing Additional Online Resources

You can access additional online resources from the following locations:

- Mercury Business Availability Center Help Menu. For details, see below.
- Mercury Business Availability Center CD-ROMs. For details, see page 102.

Mercury Business Availability Center Help Menu

You can access the following online resources from the Mercury Business Availability Center Help menu:

- **Mercury Documentation Portal.** Opens the Customer Support Web Site directly to the Mercury Documentation Portal landing page.
- **Troubleshooting & Knowledge Base.** Opens the Customer Support Web Site directly to the Knowledge Base landing page.

- **Customer Support Web Site.** opens the Customer Support Web Site. This site enables you to browse the knowledge base and add your own articles, 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 Web Site.** opens the Mercury home page. 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.
- **What's New?.** Opens the What's New document, which describes the new features and enhancements of the version.
- **About Mercury Business Availability Center.** Opens the About Mercury Business Availability Center dialog box, which provides version, patch, and third-party license information.

Mercury Business Availability Center CD-ROMs

You can access the following online resources from the Mercury Business Availability Center CD-ROMs:

- the *Getting Started with Mercury Business Availability Center*, *Deploying Servers*, and *Upgrading Mercury Business Availability Center* guides, from the **Deployment_Documentation** directory on the Mercury Business Availability Center Setup CD-ROM.
- the Mercury Business Availability Center What's New file, **whatsnew.html**, from the root directory on the Mercury Business Availability Center Setup CD-ROM, and from the **Documentation\whatsnew** directory on the Mercury Business Availability Center Documentation and Utilities CD-ROM.
- the Mercury Business Availability Center readme file, **readme62.html**, from the root directory on the Mercury Business Availability Center Setup CD-ROM, and from the **Documentation\readme** directory on the Mercury Business Availability Center Documentation and Utilities CD-ROM.

Note: You can access the most updated readme file from the Mercury Business Availability Center Documentation area on the Mercury Customer Support Web site.

➤ You can access various tools and utilities from the **tools_and_utilities** directory on the Mercury Business Availability Center Documentation and Utilities CD-ROM. References to use of these items are located in the relevant contexts within the Documentation Library.

Index

A

administration checklists 47
    applications 54
    CMDB 49
    monitors 51
    platform 48
administration tasks 55
alerts
    process flowchart 82

B

Business Process Monitor
    process flowchart 65

C

checklists
    administration 47
    application administration 54
    CMDB administration 49
    installation 23
    Monitor Administration 51
    platform administration 48
Client Monitor
    process flowchart 72
components, understanding 11
customer support 9

D

Dashboard
    customization scenario, process flowchart 86
    customization, process flowchart 84
    view monitors, process flowchart 78
data collection process
    Business Process Monitor 65
    Client Monitor 72
    EMS 74
    SiteScope 68
    third-party data 74
deployment
    planning 5, 21
    process flowchart 57
documentation
    typographical conventions xi
    updating 99
Documentation Library
    accessing 91
    guides, list of 93
    navigating 98
    PDF files 91
    updating 99
    Web access for 101
    working with 90

E

EMS
    process flowchart 74

G

getting started 5

H

Help menu resources 101
help, getting from Mercury 9

I

installation
checklist 23
See also Quick Installation Guide

L

LI001 error 42
LI002 error 42
LI003 error 42
LI004 error 42
LI005 error 43
LI006 error 44
LI007 error 45
logging in 32
automatic login 34
automatic login URL mechanism 35
direct login to specific page 36
limiting access by different machines 36
logging out 33
login error
LI001 42
LI002 42
LI003 42
LI004 42
LI005 43
LI006 44
LI007 45
login failure
troubleshooting 42

M

Mercury Business Availability Center
applications, overview 16
architecture 12
platform, understanding 11
Mercury Business Availability Center Documentation Library, *See* Documentation Library

P

PDF files, accessing 91
planning work with Mercury Business Availability Center 5, 21
platform, understanding 11
process flowcharts 55
legend 88

Q

Quick Installation Guide 23
after installation 30
checking servers 26
checking Web browser 26
deploying the Web server 27
installation 28
installing Mercury Business Availability Center data components 29
installing Mercury Business Availability Center servers 28
making deployment preparations 25
preparing database environment 25
prerequisites 25
running Set Management Database procedure 28
verifying ability to log in to Mercury Business Availability Center 30
verifying successful connectivity 30
verifying support for multilingual environment 30

R

readme file
accessing 10, 102
recipients
process flowchart 82
roadmap 5

S

scheduled reports
    process flowchart 82
service level agreements
    tracking PNR KPIs, process flowchart 80
services 9
SiteScope
    process flowchart 68
system maintenance
    process flowchart 57

T

task reference 55
third-party data
    process flowchart 74
troubleshooting
    login failure 42
typographical conventions xi

U

user groups
    defining, process flowchart 60
user permissions
    process flowchart 60
users
    defining, process flowchart 60

V

views
    defining, process flowchart 62

W

What's New file, accessing 102