OPTIMIZE

MERCURY BUSINESS AVAILABILITY CENTER™

Upgrading Mercury Business Availability Center 6.0-6.1

MERCURY™

BUSINESS TECHNOLOGY OPTIMIZATION

Mercury Business Availability Center

Upgrading Mercury Business Availability Center

Version 6.0 to Version 6.1

Document Release Date: March 5, 2006

MERCURY™

Mercury Business Availability Center, Version 6.1
Upgrading Mercury Business Availability Center 6.0-6.1

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

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

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

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

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

© 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.

AMLIB_UPG6.0_6.1/01

Table of Contents

Welcome to Upgrading Mercury Business Availability Center.....v
Using this Guide.....v
Getting More Information vi

Chapter 1: Introduction to Upgrade.....1
Important Information About the Upgrade Procedure 2
Major Upgrade Steps 2

Chapter 2: Upgrade Checklists.....3
Before You Begin 3
Upgrade Checklist 4

Chapter 3: Upgrading the Servers 7
Server Architecture for Mercury Business Availability Center 7
Upgrading Considerations 8
Installing Mercury Business Availability Center 6.1 on a Windows Platform.....9

Chapter 4: Verifying and Upgrading the Database Schema 13
Introducing Upgrade Methodology 14
Using the Verify and Upgrade Utility 14
Verifying the Database Schema.....17
Upgrading the Database Schema.....21
Creating Database Users for the Upgrade Procedure 24
Troubleshooting Database Schema Verify and Upgrade Errors 25

Chapter 5: Configuration Upgrade.....27
Upgrading Configuration Data 27

Chapter 6: Upgrading the Components to Work with Mercury Business Availability Center 6.1 33
Switching Mercury Business Availability Center URL on the Data Collectors 33
Upgrading the Components to Mercury Business Availability Center 6.1 37

Index 45

Welcome to Upgrading Mercury Business Availability Center

This guide provides detailed instructions on how to upgrade Mercury Business Availability Center 6.0 to Mercury Business Availability Center 6.1.

Note to Mercury Managed Services customers: The information in this guide is not relevant to Mercury Managed Services customers.

Before starting the upgrade, refer to "Important Information About the Upgrade Procedure" on page 2.

Using this Guide

The guide contains the following chapters:

Introduction to Upgrade

Introduces the methodology for upgrading your servers and database to Mercury Business Availability Center 6.1.

Upgrade Checklists

Describes what actions to perform before and during the upgrade to Mercury Business Availability Center 6.1.

Upgrading the Servers

Describes how to upgrade your servers to Mercury Business Availability Center 6.1.

Verifying and Upgrading the Database Schema

Describes the methodology for upgrading your database schema to Mercury Business Availability Center 6.1.

Configuration Upgrade

Describes how to upgrade your data to Mercury Business Availability Center 6.1.

Upgrading the Components to Work with Mercury Business Availability Center 6.1

Describes how to upgrade your components for Mercury Business Availability Center 6.1.

Getting More Information

For information on using and updating the Mercury Business Availability Center Documentation Library, reference information on additional documentation resources, typographical conventions used in the Documentation Library, and quick reference information on deploying, administering, and using Mercury Business Availability Center, refer to *Getting Started with Mercury Business Availability Center*.

1

Introduction to Upgrade

This guide describes the methodology for upgrading your servers and database to Mercury Business Availability Center 6.1. Mercury Business Availability Center supports direct schema and data upgrade from Mercury Business Availability Center 6.0.

The aim of the procedures and recommendations provided in this guide is to enable you to upgrade your platform to Mercury Business Availability Center 6.1 with the minimum possible interruption to your system operation.

You can access this guide in PDF format (make sure you have Acrobat Reader 4.0 or later installed on the machine) from the following locations:

- From the **Deployment_Documentation** directory on the **Mercury Business Availability Center 6.1 Setup** CD-ROM.
- From the **Documentation\pdfs** directory on the **Mercury Business Availability Center 6.1 Documentation and Utilities** CD-ROM.
- From the Mercury Business Availability Center Documentation Portal area on the Mercury Customer Support Web site (support.mercury.com).

Important Information About the Upgrade Procedure

Mercury Business Availability Center can be installed in a variety of configurations. The upgrade procedure will depend on how Mercury Business Availability Center is configured in your environment. The steps detailed in this book are intended as a guide only.

If upgrading from Mercury Business Availability Center 6.0, you must contact your Mercury representative to arrange assistance with the upgrade process.

Major Upgrade Steps

Upgrading your platform to Mercury Business Availability Center 6.1 requires the following major activities:

- Upgrading servers
- Upgrading the database schema
- Upgrading the data and completing the upgrade
- Upgrading Mercury Business Availability Center components

The complete upgrade process is described in Chapter 2, "Upgrade Checklists." For each part of the upgrade process, the upgrade checklist directs you to the section of this guide that contains the relevant steps.

2

Upgrade Checklists

This chapter describes what actions to perform before and during the upgrade to Mercury Business Availability Center 6.1.

This chapter describes:	On page:
Before You Begin	3
Upgrade Checklist	4

Before You Begin

You should be aware of the following information before you begin the upgrade.

General Information

- Rollback to Mercury Business Availability Center 6.0 after upgrading to Mercury Business Availability Center 6.1 is not supported.
- If you are upgrading from Mercury Business Availability Center 6.0 and want to perform a "clean" installation and lose all existing data, uninstall all previous Topaz server installations and then install Mercury Business Availability Center 6.1, as for a first-time installation. For details, refer to *Deploying Servers*. (You may want to make a list of your customized configuration settings before uninstalling, so that you can redefine them after the clean installation of Mercury Business Availability Center 6.1.
- Do not create any new databases between the database schema upgrade and the end of the full upgrade procedure. If you do so by mistake, please contact Mercury Customer Support.

➤ If you have any private patches for your current installation, you will lose them when you upgrade. If you have private patches that you want to continue to use, you should coordinate with Mercury Customer Support before beginning the upgrade process.

Upgrade Checklist

The following checklist should be used when upgrading from Mercury Business Availability Center 6.0 to Mercury Business Availability Center 6.1:

Mercury Business Availability Center 6.0 to Mercury Business Availability Center 6.1 Upgrade Checklist

Step	Description	Details
1 Backup files	Backup various files and directories that are required during the upgrade process, or as a precautionary measure.	Backup any files you may wish to keep for historical or precautionary reasons.
2 Shut down existing Mercury Business Availability Center 6.0 servers	Stop the Mercury Business Availability Center service on each of the old Mercury Business Availability Center servers. Make sure there are no open connections to Mercury Business Availability Center databases.	Select **Start** > **Programs** > **Mercury Business Availability Center** > **Administration** > **Disable Business Availability Center**.
3 If upgrading to Mercury Business Availability Center 6.1 using the existing Mercury Business Availability Center 6.0 servers, uninstall Mercury Business Availability Center 6.0	Uninstall Mercury Business Availability Center 6.0 from all machines.	Select **Start** > **Settings** > **Control Panel** > **Add/Remove Programs** > **Mercury Business Availability Center**.

Step	Description	Details
4 Install Mercury Business Availability Center 6.1 on all machines	Install Mercury Business Availability Center 6.1 on all machines, but do not connect to the database as part of the installation process. After installation, do not start (enable) Mercury Business Availability Center 6.1.	For details on installing Mercury Business Availability Center 6.1, see *Deploying Servers*.
5 Connect each Mercury Business Availability Center 6.1 machine to the Management database	On each Mercury Business Availability Center 6.1 machine, run Connect to Database to connect to the upgraded Management database. The first server to be connected should be the Mercury Business Availability Center 6.1 Centers Server designated for running LDAP. For information on LDAP, refer to *Preparing the Database Environment*.	Select **Start Menu** > **Programs** > **Mercury Business Availability Center** > **Administration** > **Connect to Database**.
6 Start Mercury Business Availability Center 6.1 on all machines	Enable Mercury Business Availability Center 6.1 on all machines. In a distributed environment, you must enable Mercury Business Availability Center 6.1 on the machines in the following order: ➤ Core Servers ➤ Data Processing Servers ➤ Centers Servers Only proceed to the next server when the previous one has successfully started.	Select **Start** > **Programs** > **Mercury Business Availability Center** > **Administration** > **Enable Business Availability Center.** To verify that a server has successfully started – On the server in question, look in **MercuryAM\log\jboss_boot.log** file for a line that includes **INFO - JBoss** and **Started in**.

Step	Description	Details
7 Reenter the Mercury Business Availability Center 6.1 license key	After starting Mercury Business Availability Center for the first time, reenter the Mercury Business Availability Center 6.1 license key.	Select **Admin** > **Platform** > **Setup and Maintenance** > **License Management** and click **New License Key**. For information on updating the license key, see *Platform Administration*.
8 Check that data has been inserted into CMDB	A few minutes after Mercury Business Availability Center 6.1 has been restarted, check that Adapters has inserted data in the CMDB.	From **CMDB Administration**, in the **Source Manager** tab, make sure that the **Last Update** column has a date for all the sources listed.
9 Switch URLs on data collectors (only if upgrading to Mercury Business Availability Center 6.1 on new servers)	If you installed the Mercury Business Availability Center 6.1 on new machines with different URLs, switch the URLs on your data collectors to report to Mercury Business Availability Center 6.1 servers.	See "Switching Mercury Business Availability Center URL on the Data Collectors" on page 33.
10 Upgrade Mercury Business Availability Center components	To benefit from the latest features, upgrade your Mercury Business Availability Center components to the most current version for Mercury Business Availability Center 6.1.	See "Upgrading the Components to Mercury Business Availability Center 6.1" on page 37.

3

Upgrading the Servers

This chapter describes how to upgrade your servers to Mercury Business Availability Center 6.1. You upgrade your servers after performing the previous steps in the upgrade checklists (as described on page 3).

This chapter describes:	On page:
Server Architecture for Mercury Business Availability Center	7
Upgrading Considerations	8
Installing Mercury Business Availability Center 6.1 on a Windows Platform	9

Server Architecture for Mercury Business Availability Center

In Mercury Business Availability Center 6.1, an additional server type has been added to those used in versions prior to Mercury Business Availability Center 6.0. The three server types are:

- **Centers Server** – This server is mainly responsible for running the Mercury Business Availability Center applications, reporting and the Administration Console.
- **Core Server** – This server is mainly responsible for receiving data samples from the data collectors and distributing the data to the various Mercury Business Availability Center components.
- **Data Processing Server** – This server is mainly responsible for processing the data received from the data collectors.

The Mercury Business Availability Center servers can be deployed on a single machine, or in a distributed environment where each server (or multiple instances of each server) are deployed on separate machines.

When upgrading, you must consider how you want to migrate your existing architecture to suit the new server structure, keeping in mind requirements for a load balanced and/or high availability system. For more information, refer to *Deploying Servers*.

Upgrading Considerations

You can install Mercury Business Availability Center 6.1 on new machines or on the same machine(s) on which your current system is running.

If installing Mercury Business Availability Center 6.1 on existing servers, part of the upgrade process requires uninstalling your current system from all the servers. For details on uninstalling your current system, refer to the relevant system documentation. In addition, make sure your old machine(s) meet all system requirements for Mercury Business Availability Center 6.1.

If installing Mercury Business Availability Center 6.1 on new machines, bear in mind that the Data Processing Server is a new server as of Mercury Business Availability Center 6.0 and you may require an additional machine (for distributed environments). In addition, make sure your new machine(s) meet all system requirements for Mercury Business Availability Center 6.1.

Note: During downtime, data collectors will continue to collect data, but it will not be sent to the database; alerts will not be generated.

Installing Mercury Business Availability Center 6.1 on a Windows Platform

If you are installing on a machine previously used for a Topaz or Mercury Business Availability Center server, make sure that the previous installation has been fully removed. Refer to your system documentation for uninstall procedures.

For more information on installing Mercury Business Availability Center servers, refer to the chapters on installing servers on a Windows platform in *Deploying Servers*.

You install Mercury Business Availability Center 6.1 servers—the Centers Server, Core Server, and Data Processing Server—from the Mercury Business Availability Center 6.1 Setup CD-ROM provided with the Mercury Business Availability Center distribution package. Unless you install on a machine running IIS, Mercury Business Availability Center installs Apache HTTP Server (adapted for Mercury Business Availability Center) during the installation process.

You need administrative privileges for the machine(s) on which you are installing Mercury Business Availability Center servers.

Note: For installation troubleshooting, refer to the Mercury Customer Support Knowledge Base, which can be accessed from the Mercury Business Availability Center Help menu or from the Mercury Customer Support Web site.

In addition, refer to the Mercury Business Availability Center readme file (located in the Mercury Business Availability Center 6.1 Setup CD-ROM root directory) for last-minute technical and troubleshooting information.

To install Mercury Business Availability Center servers on a Windows platform:

1 Insert the Mercury Business Availability Center 6.1 Setup CD-ROM into the drive from which you want to install. If you are installing from a network drive, connect to it.

2 From the **Start** menu, select **Run**.

3 Type the location from which you are installing, followed by setup.exe. Note that the setup file for Mercury Business Availability Center servers is located in the CD-ROM root directory. For example, type d:\setup.exe.

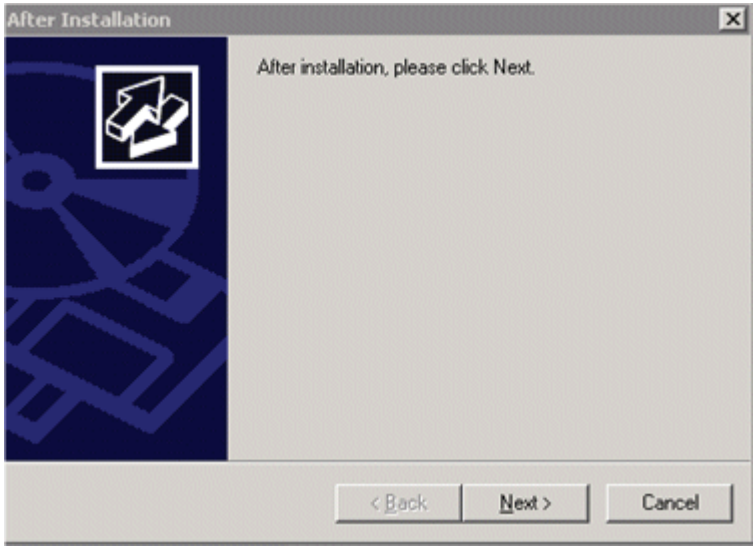
4 Click **OK**. If Mercury Business Availability Center detects a previous Topaz or Mercury Business Availability Center installation on the machine, a message is displayed warning that any customized configuration data will be overwritten.

5 Setup begins. Follow the on-screen instructions for server installation.

Note the following during the server installation stage:

➤ **Installing on a Windows platform with remote services running in application server mode:**

➤ The following window will appear if Windows detects a wrong user mode for the installation:



Click **Next** when the installation is complete and follow any other instructions that may appear in the window.

For more information on this subject, refer to Microsoft Knowledge Base Article – 252330.

- **Selecting the setup type:**
  - Select **Typical** setup type for a standard (Mercury Business Availability Center box) installation that installs the Core Server, Centers Server, and Data Processing Server on the machine, as well as MDAC.
  - Select **Custom** setup type to select the Mercury Business Availability Center features to be installed on the machine. For more information, refer to *Deploying Servers*.
- **Selecting the Web server type:**
  - If Mercury Business Availability Center does not detect an installation of Microsoft IIS on the machine, you are offered the **Apache HTTP Server** option only. If you want to run Mercury Business Availability Center with Microsoft IIS, click **Cancel** to exit Mercury Business Availability Center Setup. Install IIS and rerun the Mercury Business Availability Center installation.
- **Configuring connection settings:**
  - For Apache HTTP Server – if port 80 (default port) is already in use by the existing Web server, Mercury Business Availability Center notifies you of this. Resolve the conflict by either entering a different port number (in which case, Mercury Business Availability Center configures Apache HTTP Server to use the defined port), or exiting Setup and changing the port number of the existing Web server, then rerunning the installation procedure. For more information, refer to *Deploying Servers*.
  - For Microsoft IIS – if IIS is using a port other than port 80, enter the IIS port.
- **Specifying the SMTP mail server:**
  - It is recommended that you specify the complete Internet address of your SMTP server. Use only alphanumeric characters.
  - In the Sender name box, specify the name to appear in scheduled reports and on alert notices that Mercury Business Availability Center sends. Accept the default name (“MercuryAM_Alert_Manager”) or type another sender name.

6 When Setup has completed the installation of the Mercury Business Availability Center server files, you are prompted as to whether you want to continue with the set management database stage immediately, or finish the server installation and set database parameters later. Do not set the Management database at this stage. Refer to the checklist on page 4 for the correct sequence for connecting to the Management database.

For information on completing Mercury Business Availability Center server installation, refer to the chapter on completing server installation and launching Mercury Business Availability Center in *Deploying Servers*.

Tip: When you have installed all the servers, proceed with the next step in the checklist.

4

Verifying and Upgrading the Database Schema

This chapter describes the methodology for upgrading your database schema to Mercury Business Availability Center 6.1.

This chapter describes:	On page:
Introducing Upgrade Methodology	14
Using the Verify and Upgrade Utility	14
Verifying the Database Schema	17
Upgrading the Database Schema	21
Creating Database Users for the Upgrade Procedure	24
Troubleshooting Database Schema Verify and Upgrade Errors	25

Introducing Upgrade Methodology

It is recommended that you upgrade the database schema in the correct sequence according to the upgrade and staging checklists.

To access the database schema verify and upgrade utility in Mercury Business Availability Center 6.1, select **Start** > **Programs** > **Mercury Business Availability Center** > **Administration** > **Upgrade Database Schema**.

Important: Ensure that you have backed up your management and profile databases before running the database schema upgrade stage. Once you run the database upgrade process, it is not possible to restore the databases to their pre-upgrade state. For details, refer to *Preparing the Database Environment*.

Note: Check that your current database server version is supported for Mercury Business Availability Center 6.1. For details on supported and recommended database servers, refer to *Preparing the Database Environment*.

Using the Verify and Upgrade Utility

The database schema verify and upgrade utility runs the verify program and the upgrade program in two separate stages: the verify stage (for details, see "Verify Stage" on page 15) and the upgrade stage (for details, see "Upgrade Stage" on page 16).

If errors occur during either stage, you troubleshoot them, and then rerun the utility. For details, see "Troubleshooting Database Schema Verify and Upgrade Errors" on page 25.

Note: If you are running the database verify program on Oracle 10g schemas and use Oracle datapump utilities to import or export the target schemas, ensure that you do not have any active datapump jobs running against the target schemas.

If you have datapump tables in the target schemas, they should be dropped prior to running the database schema verification program.

It is recommended to assign an administrator schema to perform datapump operations and not to use Mercury Business Availability Center schemas as the login. By assigning an administrator schema to perform datapump operations, you do not have to grant additional permissions to Mercury Business Availability Center schemas and the datapump tables will be created in the administrator schema.

Note: If you want to verify the database after upgrading to Mercury Business Availability Center 6.1 (for example, to debug database upgrade problems), refer to the Database Schema Verification chapter in *Preparing the Database Environment*.

Verify Stage

The utility first runs the database verify stage. This stage does not involve downtime for your system. The verify program checks that there are no problems with the existing databases, and that they can be upgraded; for example, the program checks that there is no corruption and that there is sufficient storage space. The program will also check for possible lengthy operations that could slow down the upgrade process and will notify you of the estimated time they may take.

The verify program will ask you for a user name and password that can access the master database; this is required for certain (read-only) tests to be performed. If you do not want to supply your DBA account user name and password, you can create a user name with the minimum privileges required for dbverify to operate. For details on how to create this user, see "Creating Database Users for the Upgrade Procedure" on page 24.

Note: During the verify stage, you must browse to the **TopazInfra.ini** file (**<root directory>\conf\TopazInfra.ini**) from the previous version from which you are upgrading. Make sure you have a copy of this file accessible to the Mercury Business Availability Center 6.1 machine on which you will be running the database verify utility.

Note: You will be prompted for a user name and password for each database server on which the management and profile databases reside.

Upgrade Stage

If the verification is successful, you are asked if you want to continue with the database schema upgrade program, which upgrades the management database and the profile databases to the latest version schema.

The upgrade stage necessitates a short amount of downtime for the Mercury Business Availability Center servers, unless lengthy operations have been detected. The verify stage preceding the upgrade will inform you of the estimated time required for any lengthy operations it detects.

Important: There must be no open connections to the databases during the database schema upgrade.

Verifying the Database Schema

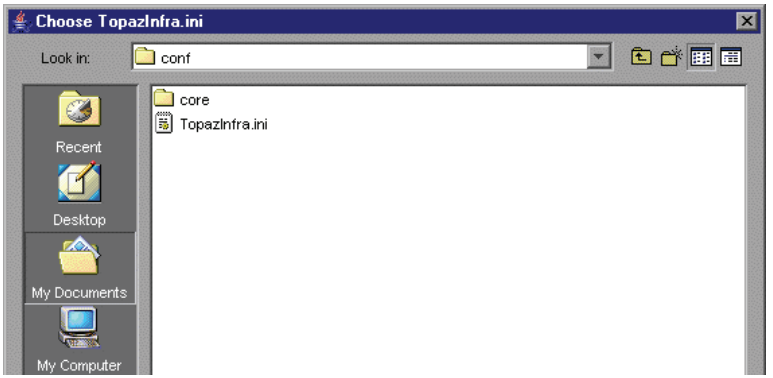
You run the database schema verify utility from a Mercury Business Availability Center 6.1 server machine.

To verify databases:

1 From any of the Mercury Business Availability Center 6.1 servers, select **Start > Programs > Mercury Business Availability Center > Administration > Upgrade Database Schema**.

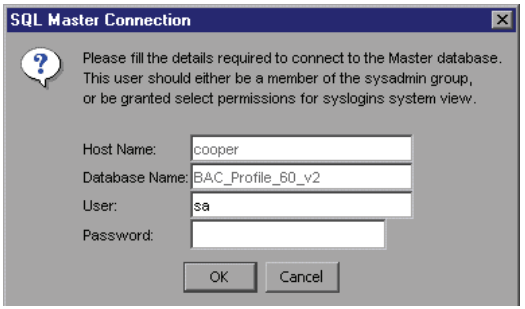
The database verify program starts.

2 In the Choose TopazInfra.ini dialog box, browse to the **TopazInfra.ini** file that you copied from your previous version.



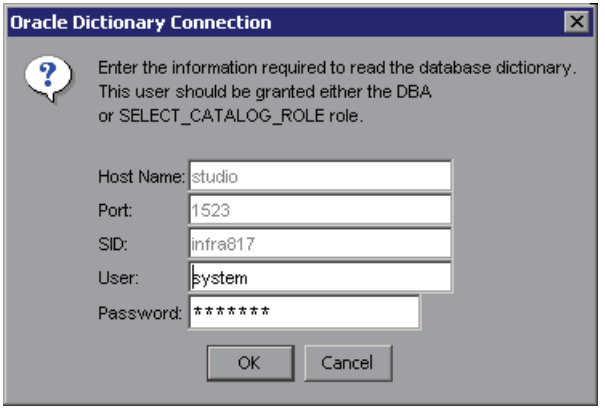
3 Specify the details required to connect to the appropriate database:

➤ In the SQL Master Connection dialog box, specify the details required to connect to the Master database.



In the **User** and **Password** boxes, type the user name and password of a user with permissions for the database. (The User box displays the default MS SQL Server administrator user name, **sa**; by default, there is no password.) Click **OK**.

➤ In the Oracle Dictionary Connection dialog box, specify the details required to connect to the Oracle database.



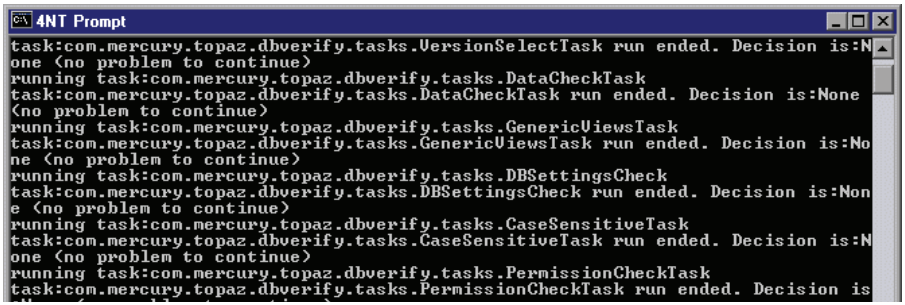
In the **User** and **Password** boxes, type the user name and password of a user with permissions for the database, and click **OK**.

Note: You will be prompted for connection data for each different server on which your management and profile databases reside.

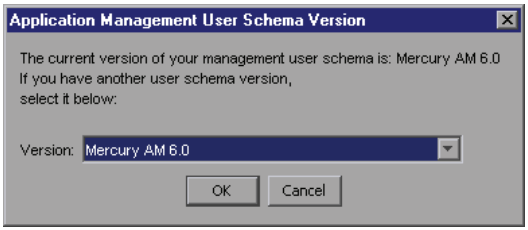
Note: If you do not want to supply your database administrator account user name and password, you can create a user name with the minimum privileges required for the verify program to operate. For details on how to create this user, see "Creating Database Users for the Upgrade Procedure" on page 24.

---

4 The database verify program performs database verification. You can view the progress of the verify process in a command prompt window.

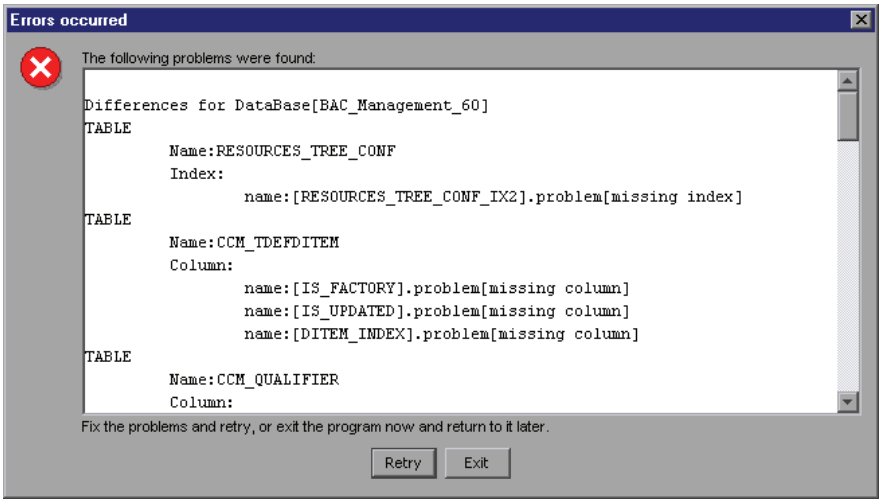


5 Check that your schema version is displayed in the Application Management User Schema Version dialog box.



Click **OK**.

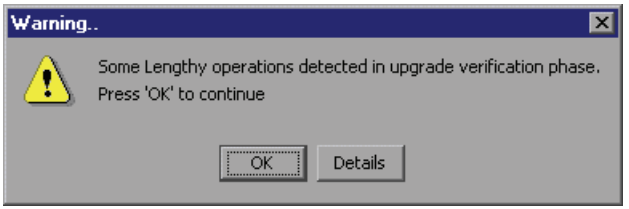
6 If problems occur during the database verification, a dialog box is displayed listing the errors.



Either fix the problems found and click **Retry**, or click **Exit** and rerun the database schema verify program at a later date. If you are unable to fix the problems, contact Mercury Customer Support for assistance.

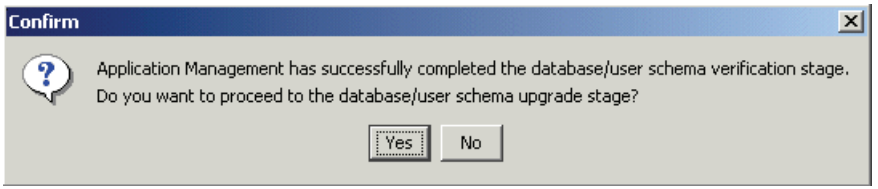
You can view a log file of the errors located in the **<Mercury Business Availability Center server root directory>\dbverify\log** directory.

7 If the verification process detects lengthy operations that could slow down the upgrade process, resulting in longer downtime, a dialog box is displayed.



Click **OK** to continue, or **Details** to display the estimated times that the lengthy operations detected could take during an upgrade.

8 If the database verification is successful, a confirmation message is displayed asking if you want to proceed with the database schema upgrade. Before proceeding, you should back up existing databases and shut down existing servers (see the checklist for details).



When this is done, proceed with the upgrade as described in "Upgrading the Database Schema" on page 21.

Note: During the database verification, the verify utility checks if the databases have sufficient disk space for a database rollback. If there is insufficient disk space, it does not continue with the verification.

Upgrading the Database Schema

After successfully verifying the database (for details, see "Verifying the Database Schema" on page 17), you can continue with the database upgrade stage.

Before proceeding with the upgrade, ensure that your management and profile databases are backed up.

Announce system downtime, then stop all Mercury Business Availability Center servers by stopping the Mercury Application Management service on each of the server machines. If you have any additional open connections to the databases (for example, additional connections that are not part of usual functioning), close them.

Note: Check that all processes have actually stopped after stopping the service. Stopping may take a few minutes. If necessary, stop the processes manually. There must be no open connections to the databases during the database schema upgrade.

To upgrade databases:

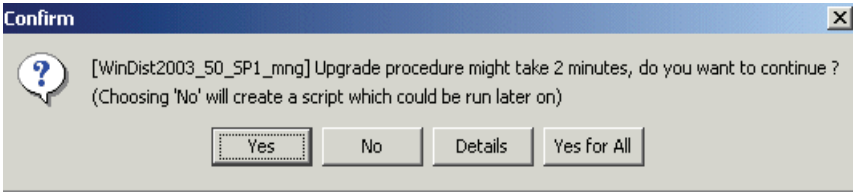
1 If you left the dbverify program open at the end of the database verification stage, click **Yes** to proceed with the database schema upgrade.

If you closed dbverify, rerun it according to the instructions on page 17. Note that the dbverify program will run through the verification stage again.

2 If there are still open connections to the database, a message is displayed giving details of the open connections. Make sure to close all connections.

3 The database schema upgrade program reviews all existing databases (management and profiles), and begins performing the required upgrade procedures for each database.

4 If lengthy operations are detected for a specific database, a message is displayed showing the estimated time that the upgrade will take, together with different options for continuing:



The options for continuing are:

- **Yes**–continues with the upgrade for the specific database, including lengthy operations.
- **No**–aborts the upgrade for the specific database, but creates a script for upgrading the database that can be run at a later time.

Note: This script is only valid while Mercury Business Availability Center is disabled. Once Mercury Business Availability Center has been restarted, the script is no longer valid.

- **Details**–displays details of the individual lengthy operations detected.
- **Yes for All**–continues with the upgrade for all the databases, including lengthy operations.

5 The database schema upgrade program runs until all existing MS SQL Server or Oracle Server databases are upgraded to Mercury Business Availability Center 6.1 format.

Note: During database upgrade, you can view log files in **<Mercury Business Availability Center_server_directory>\log\dbupgrade.log**. If errors occur, examine the dbupgrade.log file and troubleshoot the errors. For details, see "Troubleshooting Database Schema Verify and Upgrade Errors" on page 25.

---

6 Click **OK** to close the database schema upgrade utility.

7 Restart the Mercury Business Availability Center servers and processes (to work with the upgraded databases).

Tip: When you are done, proceed with the next step in the checklist.

Creating Database Users for the Upgrade Procedure

When running the database schema verify and upgrade utility, you are prompted to supply a user name and password that can access the master database. You can create users with minimum privileges by running one of the following scripts.

For MS SQL Server

```
set nocount on
use master
GO
sp_addlogin @loginame ='dbv_read',@passwd = '<pass>'
GO
sp_adduser @loginame = 'dbv_read', @name_in_db = 'dbv_read'
go
grant select on syslogins to dbv_read
go
set nocount off
```

Note: You must run this script as an **sa** user.

For Oracle Server

```
CREATE USER dbv_read IDENTIFIED BY admin

GRANT SELECT_CATALOG_ROLE TO dbv_read;

GRANT CONNECT TO dbv_read;
```

Note: You must run this script as a system user.

Troubleshooting Database Schema Verify and Upgrade Errors

If errors occur during the database verify program, troubleshoot them by examining the log file located at **<Mercury Business Availability Center server root directory>\dbverify\log**. If errors occur during the database schema upgrade program, troubleshoot them by examining the dbupgrade.log file, located in the **<Mercury Business Availability Center server root directory>\log** directory.

After correcting errors, rerun the database schema verify and upgrade utility. If further errors occur, correct them as required, and rerun the utility.

For details on troubleshooting known issues, refer to the Mercury Business Availability Center Knowledge Base, accessed from the Mercury Customer Support Web site (support.mercury.com). (Only registered customers can access the resources on the Mercury Customer Support Web site. Customers who have not yet registered can do so from the site.)

Note: While running the database verify utility, if you receive an error that indexes are missing, this may be as a result of exporting and reimporting a profile database. For details, refer to the Mercury Business Availability Center Knowledge Base.

Modifying the mx Java Run-Time Parameter

If the database schema verify and upgrade utility (dbverify) fails, displaying a **java.lang.OutOfMemoryError** error, you need to modify the default value of the **mx** Java run-time parameter used by the dbverify Java application. The default value is approximately 64 MB, varying according to the platform and the Java virtual machine (JVM) version used.

When running a JVM using java <app>, the JVM extends a certain HEAP_SIZE. The HEAP_SIZE that is used grows and shrinks automatically according to the application code, varying between ms (minimum size) and mx (maximum size).

You change the default **mx** value to match your implementation size.

To change the mx value:

1. On the machine on which you are running the database schema verify and upgrade utility, open the **\MercuryAM\dbverify\bin\run_schema_upgrade.bat file** in a text editor.
2. Add the **mx** parameter to the Java command. The value of the parameter should be the upper limit of the memory size for your machine (frequently, this may mean a value as large as 200m). For example, the modified line may read as follows:

   ```
   %JAVA_CMD% %OPTS% -Xmx200m -jar %TOPAZ_HOME%/lib/dbverifier.jar
   ```

3. Save the file and rerun the database schema verify and upgrade utility.

5

Configuration Upgrade

This chapter describes how to upgrade your configuration data.

Upgrading Configuration Data

You upgrade all your configuration data to Mercury Business Availability Center 6.1 from the Manual Configuration Upgrade page in the Mercury Business Availability Center site. Each of the entities listed below is upgraded independently.

The following entities are listed on the Manual Data Upgrade page:

User Upgrade	Upgrades user and user roles to Mercury Business Availability Center 6.1.
Custom Reports Upgrade	Upgrades custom and trend reports to Mercury Business Availability Center 6.1. There are two phases to the upgrade: ➤ Phase 1 – The custom report (in 4.5) had a public flag. During upgrade the permissions are set according to this flag. If the flag is set to Private report, the owner gets full permissions and all the other users get no permission; if the flag is set to Public report, the owner gets full permissions and all other users get view permission on this report. ➤ Phase 2 – Custom reports keep their JSPs in the database. During the upgrade these JSPs are cleared so the next user who enters a report automatically creates a new JSP.

Downtime Event Schedule Upgrade	Moves all downtime events for profiles to CMDB.
RUM MA Upgrade (5.1 to 6.1)	Removes Real User Monitor Monitor entries from the Mercury Business Availability Center 6.1 LDAP.
Monitoring Upgrade	Upgrades the monitoring administration. It includes: ➤ Monitor Permissions Upgrade (this includes updating all the LDAP data) ➤ Licensing Upgrade
Repositories Upgrade	Upgrades all the custom repositories definitions to Mercury Business Availability Center 6.1.
Dashboard Filters Upgrade	Upgrades filter persistency to Mercury Business Availability Center 6.1. Also adds support for filter sharing between users and wildcards.

The system automatically upgrades global data and configures new data types for Mercury Business Availability Center 6.1 the first time that you access the Manual Configuration Upgrade page.

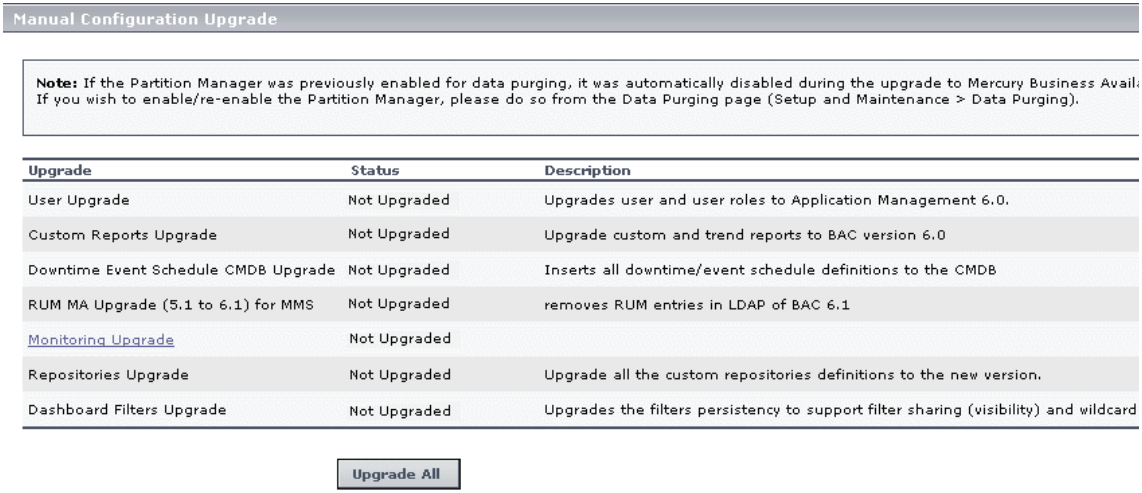
For a detailed explanation of the effects of the data upgrade on certain components, see "Upgrading the Components to Mercury Business Availability Center 6.1" on page 37.

To run a configuration upgrade:

1 Log into Mercury Business Availability Center 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 a 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.

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.

3 Click the **Admin** button in the top menu, then select **Platform** > **Setup and Maintenance** > **Configuration Upgrade**. The Manual Configuration Upgrade page opens.

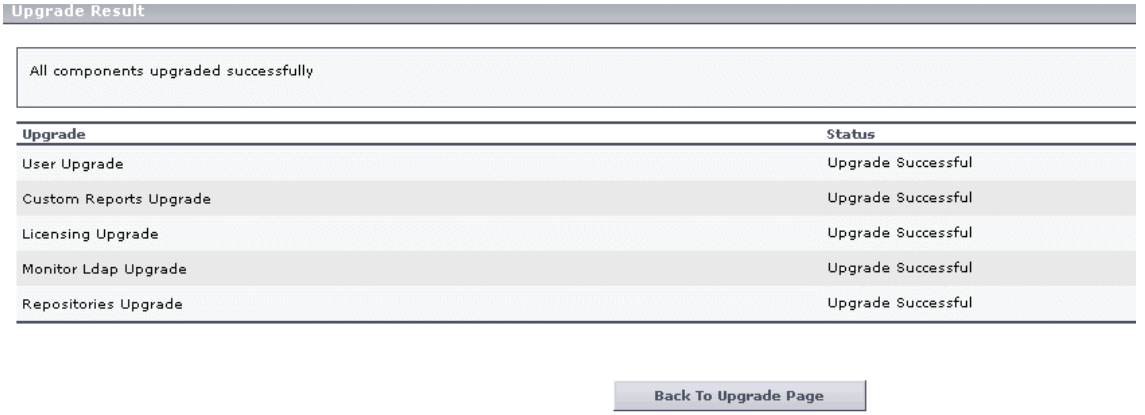


Note: Only administrators with superuser permissions can view and use the Manual Configuration Upgrade page.

---

4 Click the **Upgrade All** button to perform an upgrade of the elements requiring upgrade (as indicated in the Status column).

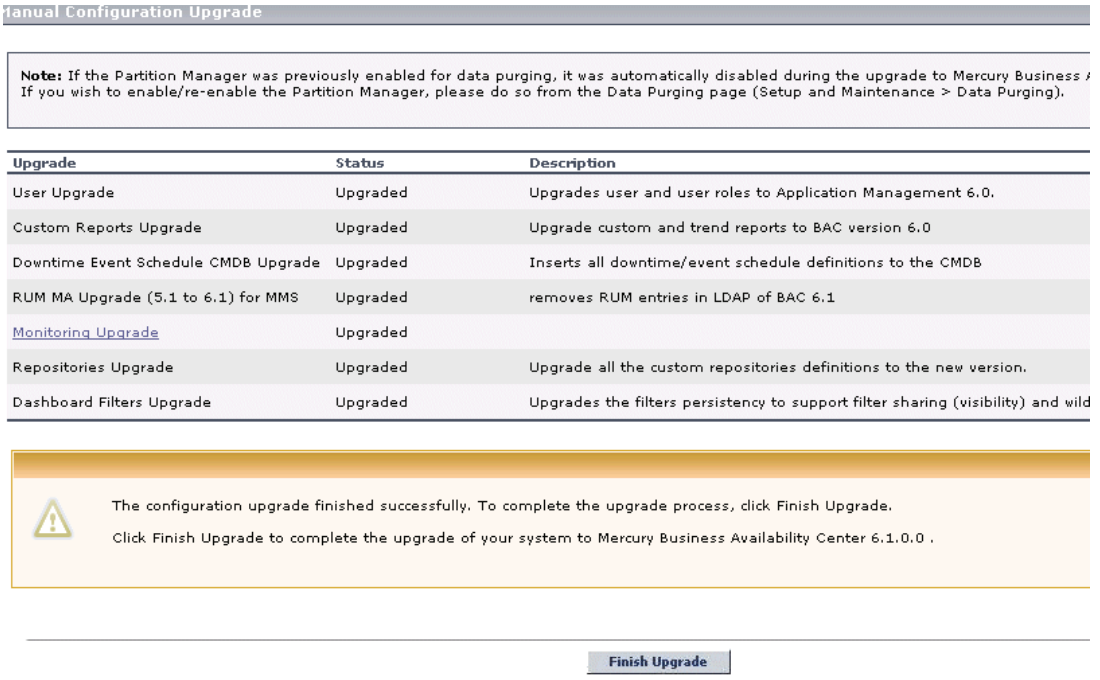
The following page opens and displays information about the data upgrade taking place.:



When the data upgrade finishes, the table should show Upgrade Successful for the whole list of elements.

If some elements are marked as Upgrade Failed click the **Back to Upgrade Page** button and consult Mercury Customer Support, or try troubleshooting using the upgrade log in **<Mercury Business Availability Center root directory>\log\topaz_all.ejb.log**.

5 Click the **Back to Upgrade Page** button to confirm that all entities are upgraded.



6 Click the **Finish Upgrade** button.

Tip: When you are done, proceed with the next step in the checklist.

6

Upgrading the Components to Work with Mercury Business Availability Center 6.1

This chapter describes how to upgrade your components to work with Mercury Business Availability Center 6.1.

This chapter describes:	On page:
Switching Mercury Business Availability Center URL on the Data Collectors	33
Upgrading the Components to Mercury Business Availability Center 6.1	37

Switching Mercury Business Availability Center URL on the Data Collectors

If you installed Mercury Business Availability Center 6.1 on a new machine or machines, you must update all the data collectors (Business Process Monitors, Client Monitors, and SiteScopes) to report to the new Mercury Business Availability Center 6.1 servers.

Note: If you installed Mercury Business Availability Center 6.1 on new servers, but those servers are behind load balancers whose URL did not change, you do not need to update the data collectors that are using the load balancer's URL. You may, however, need to update the load balancer with the IPs of the new Mercury Business Availability Center server machines. For details on implementing a distributed deployment of Mercury Business Availability Center servers, refer to *Deploying Servers*.

Redirecting the Business Process Monitor URL

To redirect the Business Process Monitor URL:

1. On each Business Process Monitor host machine, open Business Process Monitor Admin.
2. For each Business Process Monitor instance, edit the URL for the Core Server to point to the new Mercury Business Availability Center 6.1 Core Server machine. For more details, refer to *Business Process Monitor Administration*.
3. Click **Save Changes and Restart Instance**. The Business Process Monitor restarts the instance.
4. Repeat for each Business Process Monitor instance.

Redirecting the Client Monitor URL

To redirect the Client Monitor URL for pre-version 5.0 FP1 Client Monitor Agents:

1. On the end-user machine, run the file \<**MercuryClient Monitor root directory**>**bin****OLConfig.exe**.
   The Client Monitor Agent Settings dialog box opens.
2. Enter the new URL in the **AM Core URL** box.
3. Click **Save & Exit**.
4. Restart Client Monitor.

To redirect the Client Monitor URL for version 5.0 FP1 Client Monitor Agents and above:

1. From the Start menu of a Client Monitor Agent machine, click **Programs** > **Mercury Client Monitor** > **Client Monitor Agent Settings**. Client Monitor opens the Client Monitor Agent Settings dialog box.

   Note that if the Client Monitor Agent has not been configured to appear in the Start menu, you can open the Settings utility by running the following executable: \<**MercuryClient Monitor root directory**>**bin****OLConfig.exe**.

2. Enter the new URL in the **AM Core URL** box.
3. Save the changes.
4. Restart Client Monitor.

Redirecting the SiteScope URL

To redirect the SiteScope 8.0 SP1 and later URL:

1. Before the upgrade, detach SiteScope from Mercury Business Availability Center.
2. Using the old SiteScope interface, change the Mercury Business Availability Center Core Server name, user name, and user password.
3. Restart SiteScope.
4. In Monitor Administration, change the Mercury Business Availability Center Core Server, user name, and user password. Also, change the port number to the port number of the new SiteScope interface. The default port number is 8080.
5. Attach SiteScope

   For details, see *SiteScope Administration*.

To redirect the SiteScope 8.0 URL:

1. Before the upgrade, detach SiteScope from Mercury Business Availability Center.
2. Stop SiteScope.
3. Export the SiteScope configuration.

4. Change all occurrences of the Mercury Business Availability Center Core Server name, user name, and user password.
5. Import the configuration.
6. Start SiteScope.
7. In Monitor Administration, change the Mercury Business Availability Center Core Server, user name, and user password. Also, change the port number to the port number of the new SiteScope interface. The default port number is 8080.
8. Attach SiteScope

   For details, see *SiteScope Administration*.

To redirect the SiteScope 7.9.1.0/7.9.5 URL:

1. Before the upgrade, detach SiteScope from Mercury Business Availability Center.
2. Stop SiteScope.
3. Export the SiteScope configuration.
4. Change all occurrences of the Mercury Business Availability Center Core Server name, user name, and user password.
5. Import the configuration.
6. Start SiteScope.
7. In Monitor Administration, change the Mercury Business Availability Center Core Server, user name, and user password.
8. Attach SiteScope

   For details, see *SiteScope Administration*.

Note:

To import or export SiteScope 7.9.1.0/7.9.5 configurations, run the following command from the **classes** directory:

\java\bin\java COM.freshtech.TopazIntegration.AMServerSettings import/export <filename>

Upgrading the Components to Mercury Business Availability Center 6.1

Business Process Monitor

Mercury Business Availability Center 6.1 includes Business Process Monitor 6.1, but works with Business Process Monitor 4.5.2 and later. You do not need to upgrade Business Process Monitor unless you want to benefit from the enhanced functionality of later versions.

Business Process Monitor 6.1

Business Process Monitor 6.1 includes the following enhanced functionality:

- Compatibility with QuickTest Professional 9.0, providing the following enhancements when using QuickTest Professional 9.0 with Mercury Business Availability Center:
  - Full support for action iterations
  - Full support for test and action parameters
  - Full support for Data Table usage and Data Table formulas
  - New test run cleanup solution
  - More accurate transaction times
  - Support for exit functions (ExitAction, ExitActionIteration, ExitIteration)
  - Support for distributed transactions and manually entered transaction data

  - ➤ New Silent Test Runner utility in QuickTest Professional enables you to simulate test runs from Business Process Monitor, so that you can check for problems in advance

- ➤ Runs on the Red Hat Enterprise Linux 3 operating system.
- ➤ Ability to add or overwrite headers to the HTTP request sent by Business Process Monitor to Mercury Business Availability Center.
- ➤ WS_SOAP VuGen scripts run by Business Process Monitor support reporting breakdown data without the need of special configurations of Business Process Monitor. WebJS (Web GUI) VuGen scripts support reporting breakdown, as well as SOE.

Note:

Business Process Monitor 6.1 does not support versions of QuickTest Professional earlier than version 9.0

Business Process Monitor 6.1 provides backward compatibility, but not forward compatibility for scripts recorded with VuGen 8.1. This means that scripts recorded with VuGen 8.1 can only run on Business Process Monitor 6.1 and later. Scripts recorded with older versions of VuGen, however, can run on Business Process Monitor 6.1.

To upgrade Business Process Monitor to 6.1:

1 If you are using a version of Business Process Monitor prior to 5.0, uninstall Business Process Monitor. It is not necessary to uninstall Business Process Monitor version 5.0 and later.

If you uninstall Business Process Monitor, the configuration settings are saved on the machine for the next installation.

2 Access the Business Process Monitor 6.1 setup file for your operating system in Mercury Business Availability Center from **Admin** > **Platform** > **Setup and Maintenance** > **Downloads** > **Mercury Business Process Monitor**, and install Business Process Monitor 6.1 according to the instructions in *Business Process Monitor Administration*.

If the Business Process Monitor setup file does not appear on the Downloads page, refer to *Deploying Servers* for details on installing components setup files on the Downloads page.

Note: You can remotely upgrade Business Process Monitor from within Mercury Business Availability Center 6.1. For details, refer to *Platform Administration*.

Client Monitor

Mercury Business Availability Center 6.1 includes Client Monitor 6.1, but works with Client Monitor 5.0 and later. You do not need to upgrade Client Monitor unless you want to benefit from the enhanced functionality of later versions.

Client Monitor scripts recorded in Client Monitor version 5.0 or less must be converted to be compatible with Client Monitor 6.1. For details, contact Mercury Customer Support.

Client Monitor 6.1

Client Monitor 6.1 includes the following enhanced functionality:

- Ability for selected Web transactions to continue even when the user has browsed to another link before the current download is finished.
- Improved logging mechanism.
- Possibility of specifying the installation directory.

To upgrade Client Monitor to 6.1:

1. Uninstall the old Client Monitor.
2. Access the Client Monitor 6.1 setup file in Mercury Business Availability Center from **Admin** > **Platform** > **Setup and Maintenance** > **Downloads** > **Mercury Client Monitor**, and install Client Monitor 6.1 according to the instructions in *Client Monitor Administration*.

   If the Client Monitor setup file does not appear on the Downloads page, refer to *Deploying Servers* for details on installing components setup files on the Downloads page.

Note: You can remotely upgrade Client Monitor from within Mercury Business Availability Center 6.1. For details, refer to *Platform Administration*.

SiteScope

Mercury Business Availability Center 6.1 includes SiteScope 8.1.2, but supports SiteScope 7.9.0.0 and later. You do not need to upgrade SiteScope, but it is recommended that you do upgrade SiteScope to benefit from enhanced functionality. For a complete list of new features, refer to the What's New document, available from the Mercury Business Availability Center 6.1 Help menu.

Note the following about SiteScope support in Mercury Business Availability Center 6.1:

- Mercury Business Availability Center 6.1 supports SiteScope 7.9.0.0 and later. For details of SiteScope versions and their compatibility with Mercury Business Availability Center 6.1, refer to the compatibility matrix in the readme file, available in:
  - the **Documentation\readme** directory on the Mercury Business Availability Center Documentation and Utilities CD-ROM.
  - the root directory on the Mercury Business Availability Center Setup CD-ROM.

- the Mercury Documentation Portal in the Mercury Customer Support Web site (http://support.mercury.com/cgi-bin/portal/CSO /docViewAndSearch.jsp).

- If you are using 7.9.0 and need to change the URL because Mercury Business Availability Center is installed on a new server machine, you must upgrade to SiteScope 7.9.5.0 (SiteScope 7.9.0 does not support changing the URL).
- If you want monitors to report custom data to Mercury Business Availability Center you must upgrade to SiteScope 7.9.5.0 or higher.
- If you want to administer SiteScope from Monitor Administration in Mercury Business Availability Center 6.1, you must upgrade to SiteScope 7.9.5.0 or higher.
- If you currently have SiteScopes attached to Topaz Monitor Configuration in Topaz 4.5 FP2 or Monitor Administration in Mercury Business Availability Center 5.0 (also known as Application Management 5.0), you must detach and upgrade them before upgrading servers.
- If you want to administer SiteScope from the SiteScope machine and not from Mercury Business Availability Center, you do not need to upgrade to 7.9.5.0.
  - Previous SiteScope profiles created in Topaz are automatically upgraded when upgrading to Mercury Business Availability Center 6.1. You will be able to view SiteScope data in Mercury Business Availability Center. Additionally, all the features of those profiles will be displayed but you will not be able to change them using Monitor Administration (only by using SiteScope administration).
  - You can create a new empty profile in Monitor Administration by entering the name of the profile in the **SiteScope Display Name** box and the name of the machine on which Mercury Business Availability Center is running in the **Host Name** box and by clearing **Import SiteScope Configuration**. Then you go to SiteScope administration and connect to the profile you created. This new profile allows you to view SiteScope data in Mercury Business Availability Center but you cannot add features such as **Preferences**, **Health**, and so forth.

Note: If you are not sure how to proceed with your SiteScope under Mercury Business Availability Center 6.1, contact Mercury Customer Support.

To upgrade SiteScope to 8.1.2:

1. Backup the **<SiteScope_home>\cache** directory
2. Backup the **<SiteScope_home>\groups** directory.
3. Access the SiteScope 8.1.2 setup file in Mercury Business Availability Center from **Admin** > **Platform** > **Setup and Maintenance** > **Downloads** > **SiteScope**, and install SiteScope according to the instructions in *SiteScope Administration*.
4. Check that SiteScope is running with the correct configuration (the original groups).
5. In Mercury Business Availability Center, go to **Admin** > **Monitors** and attach each SiteScope. For details, refer to *Managing SiteScope*.

   If the SiteScope setup file does not appear on the Downloads page, refer to *Deploying Servers* for details on installing components setup files on the Downloads page.

Real User Monitor

Mercury Business Availability Center 6.1 includes Real User Monitor 6.1. Real User Monitor 6.1 is a significantly revised version of Real User Monitor, and includes a new Engine, database, new reports, and improved configuration features.

There is no upgrade path to Real User Monitor 6.1 from previous versions. For installation instructions, refer to *Real User Monitor Administration*.

For a complete list of new and improved Real User Monitor features, refer to the What's New document, available from the Mercury Business Availability Center 6.1 Help menu.

J2EE

Mercury Business Availability Center is fully integrated with Mercury Diagnostics, enabling you to monitor the performance of your enterprise applications on J2EE, .NET, and SAP platforms throughout the application lifecycle. For more information contact Mercury Customer Support.

Mercury Virtual User Generator

Mercury Business Availability Center 6.1 includes Mercury Virtual User Generator (VuGen) version 8.1. Upgrade VuGen to be compatible with the Business Process Monitor for Mercury Business Availability Center 6.1, and to benefit from the following improved functionality:

Workflow Wizard

The new Workflow Wizard guides you through the steps of creating a Vuser script. Each wizard screen presents an overview of the step with links to additional information or dialog boxes.

The wizard also provides summary reports for record and replay, along with links to the troubleshooting guide in the event of an error.

In conjunction with the wizard, VuGen features a new Task Pane with a list of all the tasks required for creating a script. An arrow in the task list, indicates the current task. You can move from one task to another by clicking on the desired task.

Thumbnails and Transaction Editor

VuGen now supports a thumbnail view of scripts for Web, SAPGUI, and Citrix-ICA Vusers. You can rename and annotate the thumbnails, and filter them to show only the primary thumbnails.

The Transaction editor gives you an visual overview of the script's transactions using thumbnails. You drag transaction brackets to mark the beginning and end of a transaction.

The Transaction editor also provides a filterable list of transactions, and allows you to rename and remove existing transactions.

Debugging Capabilities

VuGen features a new Run Time Data tab that lets you view run-time information during the script run. It shows the iteration number, the action name, the line number, and parameter values.

VuGen's Breakpoint Manager provides a single interface for managing breakpoints. Using the Breakpoint Manager, you can add, remove, enable, and disable breakpoints within you script.

VuGen lets you set bookmarks within your script. You can navigate between the bookmarks in each section of the script with a single key stroke.

Enhanced NTLM Authentication

VuGen has enhanced support for NTLM authentication. VuGen provides a user interface for entering NTLM login information, while automatically capturing the domain and user names. This eliminates the need to modify the script manually with the user name and password.

To upgrade VuGen to version 8.1:

1. If you are installing to the same machine running your existing Virtual User Generator, uninstall the existing version.
2. Access the Virtual User Generator setup file in Mercury Business Availability Center from **Admin** > **Platform** > **Setup and Maintenance** > **Downloads** > **Mercury Virtual User Generator**, and install the Mercury Virtual User Generator 8.1 according to the on-screen instructions

   If the Virtual User Generator setup file does not appear on the Downloads page, refer to *Deploying Servers* for details on installing components setup files on the Downloads page.

Note: Business Process Monitor 6.1 provides backward compatibility, but not forward compatibility for scripts recorded with VuGen 8.1. This means that scripts recorded with VuGen 8.1 can only run on Business Process Monitor 6.1 and later. Scripts recorded with older versions of VuGen, however, can run on Business Process Monitor 6.1.

Index

A

architecture 7

B

Business Process Monitor, upgrading 37

C

checklist
    upgrade 4
    upgrading from Topaz 4.5.x 4
Client Monitor, upgrading 39
components, upgrading 37
configuration, upgrading 27

D

data collectors, changing URL 33
database schema
    upgrading 13, 21
    verifying 13, 17
database users, creating for upgrade 24
dbverify 14

J

J2EE 43
Java run time, modifying mx parameter 25

M

Mercury Diagnostics 43

R

Real User Monitor, upgrading 42

S

server architecture 7
server installation
    Windows platform 9
servers, upgrading 7
SiteScope
    upgrading 40

T

troubleshooting dbverify errors 25

U

upgrade
    checklist 4
    components 37
    configuration 27
    considerations 8
    database schema 13
    dbverify utility 14
    getting started 3
    introduction 1
    major steps 2
    methodology 14
    servers 7
URL, changing on data collectors 33

V

verify utility 14
verifying database schema 13
Virtual User Generator, upgrading 43

W

Windows platform
    upgrading servers 9