OPTIMIZE

MERCURY BUSINESS AVAILABILITY CENTER™

Upgrading Mercury Business Availability Center 6.1.x - 6.2

MERCURY™

BUSINESS TECHNOLOGY OPTIMIZATION

Mercury Business Availability Center

Upgrading Mercury Business Availability Center

Version 6.1.x to Version 6.2

Document Release Date: July 18, 2006

MERCURY™

Mercury Business Availability Center, Version 6.2
Upgrading Mercury Business Availability Center 6.1.x-6.2

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

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

AMLIB_UPG6.1.X_6.2/01

Table of Contents

Welcome to Upgrading Mercury Business Availability Center

This guide provides detailed instructions on how to upgrade Mercury Business Availability Center 6.1.x to Mercury Business Availability Center 6.2.

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

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 6.2.

Upgrade Checklist

Describes what actions to perform before and during the upgrade to Mercury Business Availability Center 6.2.

Verifying and Upgrading the Database Schema

Describes the methodology for upgrading your database schema to Mercury Business Availability Center 6.2.

Upgrading Repositories and Source Adapters from Version 6.1.x to Version 6.2

Describes the process to upgrade repositories and source adapters from Mercury Business Availability Center version 6.1.x to version 6.2.

Upgrading Components to Work with Mercury Business Availability Center 6.2

Describes how to upgrade your components for Mercury Business Availability Center 6.2.

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 6.2. Mercury Business Availability Center supports direct schema and data upgrade from Mercury Business Availability Center 6.1.x.

The aim of the procedures and recommendations provided in this guide is to enable you to upgrade your platform to Mercury Business Availability Center 6.2 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 6.2 (Windows or Solaris) Setup** CD-ROM.
- From the **Documentation\pdfs** directory on the **Mercury Business Availability Center 6.2 (Windows or Solaris) Documentation and Utilities** CD-ROM.
- From the Mercury Business Availability Center Documentation Portal area on the Mercury Customer Support Web site (support.mercury.com).

Major Upgrade Steps

Upgrading your platform to Mercury Business Availability Center 6.2 requires the following major activities:

- Installing the Mercury Business Availability Center 6.2 Add-on on top of existing 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 Checklist." 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 Checklist

This chapter describes what actions to perform before and during the upgrade to Mercury Business Availability Center 6.2 from Mercury Business Availability Center 6.1.x.

Before You Begin

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

- Uninstalling Mercury Business Availability Center 6.2 does not roll back to a previous version of Mercury Business Availability Center. It completely removes the software.
- 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 6.1.x to Mercury Business Availability Center 6.2:

Step	Description	Details
1 Back up files.	Back up various files and directories that are required during the upgrade process, or as a precautionary measure.	Back up the following files and directories: ➤ **MercuryAM\conf\ TopazInfra.ini** ➤ **MercuryAM\CMDB** ➤ **<Mercury Business Availability Center server root directory>\openldap \bdb** In addition, backup any other files or directories you want to keep for security or historical purposes.
2 Shut down existing Mercury Business Availability Center 6.1.x 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 Stop the Web server process on Mercury Business Availability Center servers.	Stop the IIS Admin Service for IIS, or Apache service for Apache Web Server, on all Mercury Business Availability Center servers.	For details, refer to your Web server documentation.
4 Install the Mercury Business Availability Center 6.2 Add-on on all machines.	Install the Mercury Business Availability Center 6.2 Add-on on all machines. After installation, do not start (enable) Mercury Business Availability Center 6.2.	For additional details on installing Mercury Business Availability Center 6.2, see *Deploying Servers*.

Step	Description	Details
5 Restart the Web server process on Mercury Business Availability Center servers.	Restart the IIS Admin Service for IIS, or Apache service for Apache Web Server, on all Mercury Business Availability Center servers.	For details, refer to your Web server documentation.
6 Back up the databases.	Back up the existing management and profile databases.	For information on backing up your databases, refer to the database server documentation or to the Mercury Business Availability Center database administration document *Preparing the Database Environment*.
7 Run the database schema upgrade.	Run **dbupgrade** from any one of the Mercury Business Availability Center 6.2 servers to verify and upgrade the management and profile databases to Mercury Business Availability Center 6.2 compatibility. Do not proceed to the next step until database upgrade has completed successfully.	See "Verifying and Upgrading the Database Schema" on page 9.
8 Connect each Mercury Business Availability Center 6.2 machine to the management database.	On each Mercury Business Availability Center 6.2 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 6.2 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**.

Step	Description	Details
9 Delete previously compiled .jsp files.	Delete the contents of the directory **<Mercury Business Availability Center root directory>\EJBContainer\server\mercury\work.**	This is required to ensure proper functionality of Mercury Business Availability Center once servers are started.
10Start Mercury Business Availability Center 6.2 on all machines.	Enable Mercury Business Availability Center 6.2 on all machines. It can take approximately 20-25 minutes for Mercury Business Availability Center to be available for login after starting all servers for the first time.	➤ 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**.
11 Reenter the Mercury Business Availability Center 6.1.x license key.	After starting Mercury Business Availability Center for the first time, reenter the Mercury Business Availability Center 6.1.x 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*.
12 Check that data has been inserted into CMDB.	A few minutes after Mercury Business Availability Center 6.2 has been restarted, check that Adapters have 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.
13 Upgrade repositories and source adapters.	Perform the manual procedure that upgrades 6.1.x repositories and source adapters to 6.2 compatibility.	See "Upgrading Repositories and Source Adapters from Version 6.1.x to Version 6.2" on page 25.

Step	Description	Details
14 Restart Mercury Business Availability Center on the Data Processing Server.	Restart Mercury Business Availability Center on the Data Processing Server machine. In a distributed architecture, restart Mercury Business Availability Center on the Modeling Data Processing Server machine.	➤ To stop Mercury Business Availability Center, select **Start** > **Programs** > **Mercury Business Availability Center** > **Administration** > **Disable Business Availability Center**. ➤ To restart Mercury Business Availability Center, select **Start** > **Programs** > **Mercury Business Availability Center** > **Administration** > **Enable Business Availability Center**.
15 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 6.2.	See "Upgrading Components to Work with Mercury Business Availability Center 6.2" on page 29

3

Verifying and Upgrading the Database Schema

This chapter describes the methodology for upgrading your database schema to Mercury Business Availability Center 6.2.

Introducing Upgrade Methodology

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

To access the database schema verify and upgrade utility in Mercury Business Availability Center 6.2, 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 6.2. 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 11) and the upgrade stage (for details, see "Upgrade Stage" on page 12).

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 22.

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 6.2 (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 also checks for possible lengthy operations that could slow down the upgrade process and notifies you of the estimated time they may take.

The verify program asks 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 21.

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 6.2 machine on which you will be running the database verify utility.
- 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 should have informed 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 6.2 server machine.

On a Solaris platform, you must run the database schema verify utility **dbverify** from a machine that supports UI mode, and make sure that the DISPLAY environment variable is properly configured on the machine. For example:

```
setenv DISPLAY <terminal host name>:0.0
```

To verify databases:

1 From any of the Mercury Business Availability Center 6.2 servers, select **Start** > **Programs** > **Mercury Business Availability Center** > **Administration** > **Upgrade Database Schema**.

The database verify program starts.

Run the verify program according to your operating platform:

Copy the **dbverify** directory from the Mercury Business Availability Center 6.2 Windows (or Solaris) Documentation & Utilities CD-ROM supplied with your package, (**<CD root directory>\tools_and_utilities**), to the local disk on your Mercury Business Availability Center server machine, or Core Server machine if you have a distributed deployment.

If you are running dbverify from a Windows platform, open a command prompt (**Start** > **Programs** > **Accessories** > **Command Prompt**) and enter the path to the local copy of the **dbverify\bin** folder.

Enter the command:

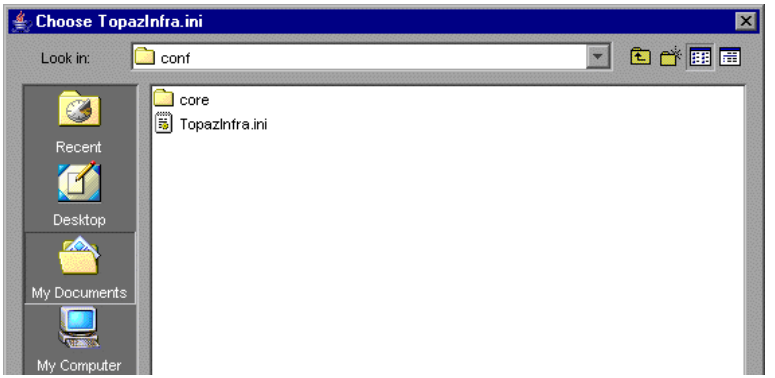
```
run_schema_upgrade.bat
```

If you are running dbverify from a Solaris platform, make sure that the DISPLAY environment variable is set. Open an X-terminal window and move to the location of the local copy of the dbverify directory, then type:

```
./run_schema_upgrade.sh
```

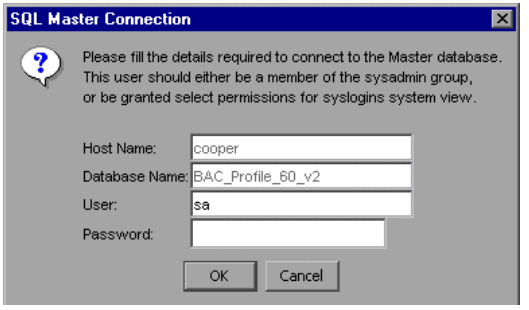
The database verify program starts.

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



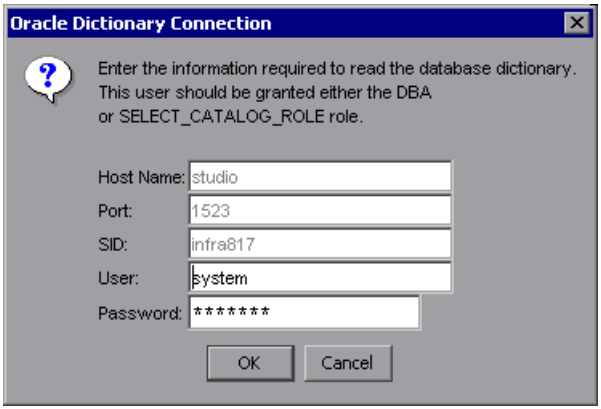
3 Specify the details required to connect to the appropriate database:

➤ 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**.

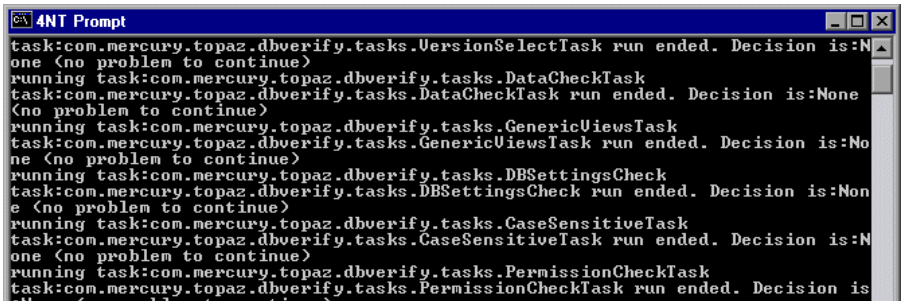
Note:

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

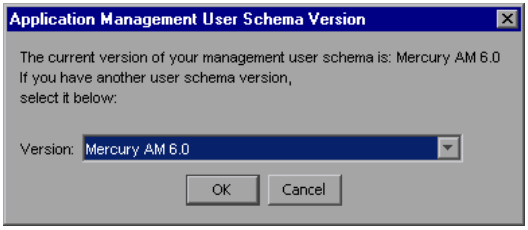
➤ If you do not want to supply your database administrator account user name and password, you can create a user name with the minimum privileges required for the verify program to operate. For details on how to create this user, see "Creating Database Users for the Upgrade Procedure" on page 21.

---

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

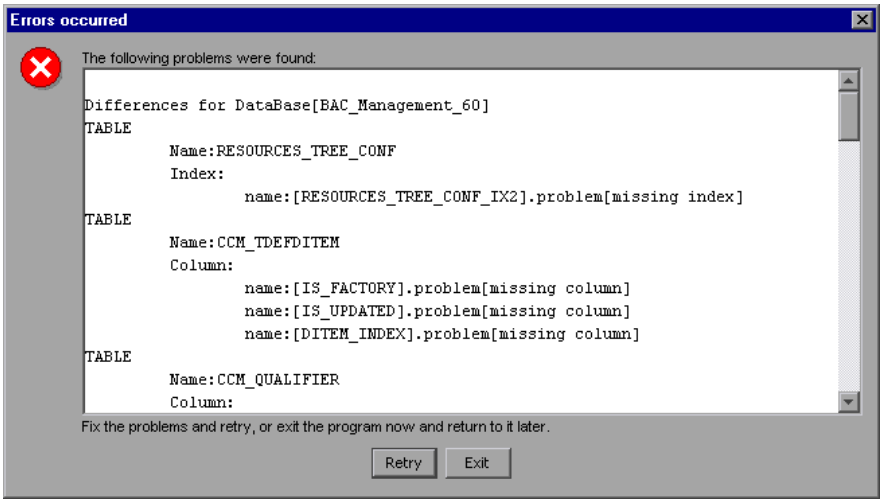


5 Check that your schema version is displayed in the Application Management User Schema Version dialog box.



Click **OK**.

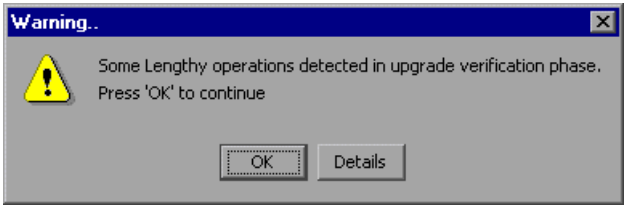
6 If problems occur during the database verification, a dialog box is displayed listing the errors.



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.

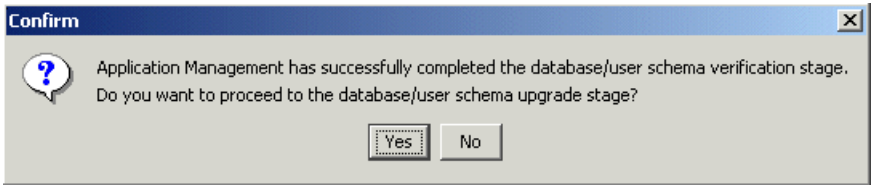
You can view a log file of the errors located in the **<Mercury Business Availability Center server root directory>\dbverify\log** directory.

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 18.

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 13), 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:

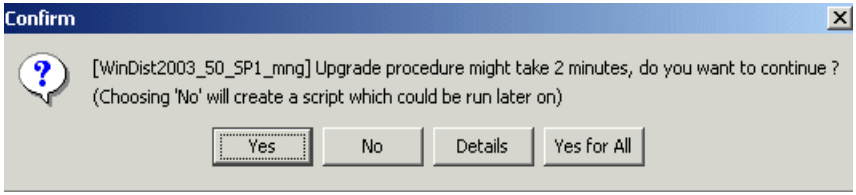
1. If you left the dbverify program open at the end of the database verification stage, click **Yes** to proceed with the database schema upgrade.

   If you closed dbverify, rerun it according to the instructions on page 13. 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 6.2 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 22.

---

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:

Open the appropriate file for your operating platform:

1. On a Windows platform 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.

   ➤ On a Solaris platform, locate the **run_schema_upgrade.sh** script under the dbverify directory that you copied to your local disk (**../DbVerify/bin/run_schema_upgrade.sh**) and open it 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.

4

Upgrading Repositories and Source Adapters from Version 6.1.x to Version 6.2

This chapter describes the process to upgrade repositories and source adapters from Mercury Business Availability Center version 6.1.x to version 6.2.

Note: You must upgrade the repositories before upgrading the source adapters, otherwise the source adapters will not be correctly upgraded.

Upgrading Repositories

Mercury Business Availability Center version 6.1.x repositories are upgraded through the JMX console. Customer objects that you have created in the repositories, such as custom KPIs, business rules, and so forth, are not included in the upgrade.

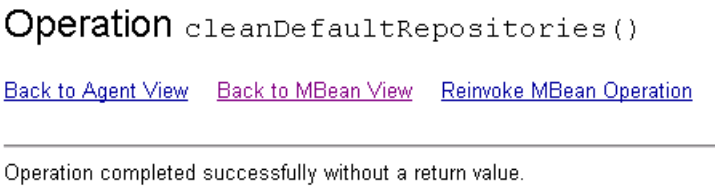
To upgrade repositories:

1. In a Web browser, open:
http://<Data Processing Server machine name>:8080/jmx-console.

   The JMX MBean View window opens.

2. In the **Topaz** section, click **service=repositories_manager.**

3. In **cleanDefaultRepositories**, click **Invoke**. An informational message is displayed when the upgrade has completed.



Upgrading Source Adapters

Mercury Business Availability Center version 6.1.x source adapters are upgraded through an adapter upgrade utility.

Note: Do not upgrade source adapters until you have upgraded repositories. For details, see "Upgrading Repositories" on page 26.

To upgrade source adapters:

1. In a Web browser, open:
http://<Centers Server machine name>/topaz/adaptersUpgrade.jsp.

   The Adapter Upgrade Page dialog box opens.

2. Click **Upgrade**.

3. An informational message is displayed when the upgrade has completed.

Note: After upgrading source adapters, you must restart Mercury Business Availability Center on the Data Processing Server machine. In a distributed architecture, restart Mercury Business Availability Center on the Modeling Data Processing Server machine.

5

Upgrading Components to Work with Mercury Business Availability Center 6.2

This chapter describes how to upgrade Mercury Business Availability Center components to work with Mercury Business Availability Center 6.2.

Upgrading Business Process Monitor

Mercury Business Availability Center 6.2 includes Business Process Monitor 6.2, but works with Business Process Monitor 4.5 FP2 and later. You do not need to upgrade Business Process Monitor unless you want to benefit from the enhanced functionality of later versions.

Note:

- Business Process Monitor 6.2 does not support versions of QuickTest Professional earlier than version 9.0.
- 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 6.2.

Business Process Monitor 6.2

Business Process Monitor 6.2 includes the following enhanced functionality:

- Business Process Monitor can now color transactions for Diagnostics for any HTTP based protocol.
- Business Process Monitor reports to Mercury Business Availability Center failed transactions in scripts that did not end properly.

To upgrade Business Process Monitor to 6.2:

1 If you are using a version of Business Process Monitor prior to 5.0, the upgrade involves uninstalling the current version with the option to save the current configuration.

2 Access the Business Process Monitor 6.2 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 6.2 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 6.2. For details, refer to *Platform Administration*.

Client Monitor

Mercury Business Availability Center 6.2 includes Client Monitor 6.2, 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.

Note: You can continue to work with Client Monitors already installed on end-user machines. Client Monitor scripts recorded in Client Monitor versions 4.5 FP2/5.x must be converted, using a converter tool, to be compatible with Client Monitor 6.2. For details, contact Mercury Customer Support.

Client Monitor 6.2 includes the following enhanced functionality:

- keyword support for host filtering in Mercury Business Availability Center
- Windows 2003 support for Client Monitor

- enhanced configuration for connecting to Mercury Business Availability Center
- improved persistency
- network optimization
- compatibility with the new Mercury Business Availability Center Client Monitor large deployment

Client Monitor Upgrade Notes

Note the following information regarding upgrading to Client Monitor 6.2:

Database Schema Upgrade

Database schema upgrade from Mercury Business Availability Center 6.1.x to 6.2 includes creating six new tables for Client Monitor large deployment:

- CM_GROUPS
- CM_GROUP_FILTERS
- CM_HOST_PROPERTIES
- CM_GROUP_HOSTS
- CM_GROUP_SCRIPTS
- CM_GROUP_TRACEROUTES

Database Data Upgrade

There is no support of data upgrade for version 6.2 in Client Monitor large deployment. This means that if you upgrade to Mercury Business Availability Center 6.2 from an existing Mercury Business Availability Center with data, version 6.2 starts with the following initial configuration:

- **Platform/Data Collector Maintenance.**

  You begin with no declared groups or containers, and with no Client Monitor host properties for a group's filters. In other words, the hosts that were registered before the upgrade are not included in the filters after the upgrade until you register them again in Mercury Business Availability Center 6.2.

➤ **Client Monitor hosts.**

Job assignments for the Client Monitor hosts that were set before the upgrade are not kept. Note the following:

- In Monitor Administration, the old profiles and monitors do not have any assignment to the groups. Note that if you refresh the LDAP, you may loose the traceroutes monitors and will have to declare them again.
- In Dashboard, Client Monitor profiles appear empty.
- All CIs which appeared in Client Monitor 6.1 (for example, **Business Process Step**, **Business Process Monitor Transaction From Location**, **Location**, **Business Process Group Location**), are removed from CMDB in Mercury Business Availability Center 6.2. This means that all Service Level Agreements and thresholds that were defined using these CIs are also removed and must be redefined again.
- The Client Monitor hosts that had jobs (transactions and traceroutes in profiles that are assigned to the Client Monitor) assigned to them before the upgrade and are now registered to Mercury Business Availability Center 6.2, do not have those jobs after the upgrade. This means that immediately after the upgrade, there are no registered jobs. You must assign the hosts to groups and then assign jobs to those groups.

  Note: Job assignments made before the upgrade can be extracted from the database. They are not removed from the old tables until you delete the profile. You can extract the following tables: ACTIONS, GROUPS, EXT_GROUP_SCHEDULES, and TRACE_ROUTE_DEFINITION.

➤ **End User Management.**

All End User Management reports, both scripts and traceroutes, continue to work after the upgrade with historic data.

To upgrade Client Monitor 4.5/5.x to 6.2:

1. Uninstall the old Client Monitor.
2. Access the Client Monitor 6.2 setup file in Mercury Business Availability Center from **Admin** > **Platform** > **Setup and Maintenance** > **Downloads** > **Mercury Client Monitor**, and install Client Monitor 6.2 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.

SiteScope

For a compete list of enhanced functionality provided by SiteScope 8.2, refer to the SiteScope release notes.

Note the following about SiteScope support in Mercury Business Availability Center 6.2:

- Mercury Business Availability Center 6.2 includes SiteScope 8.2, but supports SiteScope 7.9.0.0 and later. You must upgrade to SiteScope 8.2 to benefit from enhanced functionality and to be able to administer SiteScope from Monitor Administration.

  For details of SiteScope versions and their compatibility with Mercury Business Availability Center 6.2, refer to the compatibility matrix in the readme file, available in:

  - From the **Deployment_Documentation** directory on the **Mercury Business Availability Center 6.2 (Windows or Solaris) Setup** CD-ROM.
  - From the **Documentation\readme** directory on the **Mercury Business Availability Center 6.2 (Windows or Solaris) Documentation and Utilities** CD-ROM.
  - From the Mercury Business Availability Center Documentation Portal area on the Mercury Customer Support Web site (support.mercury.com).
- 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 currently have SiteScopes attached to Topaz Monitor Configuration in Topaz 4.5 FP2 or Monitor Administration in Mercury Business Availability Center 5.x (also known as Application Management 5.x), 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 version 8.2.
  - Previous SiteScope profiles created in Topaz are automatically upgraded when upgrading to Mercury Business Availability Center 6.2. 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 6.2, contact Mercury Customer Support.

To upgrade SiteScope to 8.2:

1. Backup the <**SiteScope_home**>**cache** directory
2. Backup the <**SiteScope_home**>**groups** directory.

3 Access the SiteScope 8.2 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 6.2 includes Real User Monitor 6.2.

Note: Real User Monitor Engine 6.2 is only supported in a Windows environment.

Real User Monitor 6.2 includes the following enhanced functionality:

- Meaningful names can be created for pages that are not configured. Siebel and PeopleSoft applications have predefined templates for meaningful names.
- Global Statistics report now includes pages with errors.
- Snapshot on error (SSOE) can be configured per application.
- Real User Monitor is included in the Mercury Self-Alert Monitor.
- The system health reporting is improved in the Real User Monitor Web console.
- There is an open API for user name resolution.
- There are general performance improvements.

Contact Mercury Customer Support for assistance in performing an upgrade from pre-6.1 versions of Real User Monitor to Real User Monitor 6.2.

To upgrade Real User Monitor from 6.1.x to 6.2:

1. Uninstall the Real User Monitor engine. For details, refer to *Real User Monitor Administration*. When prompted during the uninstall procedure, do not delete the files in the Real User Monitor directory.
2. Install Real User Monitor 6.2 engine in the same directory as the previous Real User Monitor engine. The Real User Monitor database must be installed on the same machine as the prior version.
3. Install the Real User Monitor 6.2 probe.

Note:

- The Real User Monitor 6.2 probe supports only Red Hat Enterprise Linux 4 (RHEL 4). Red Hat 9 is not supported.
- If you install Real User Monitor 6.2 probe on a different machine, you must configure it in Mercury Business Availability Center Monitor Administration just like a new probe. For details, refer to *Real User Monitor Administration*.
- Real User Monitor 6.2 engine does not support earlier versions of Real User Monitor probe.

Limitation

A user custom report with an event summary component of Real User Monitor is not displayed after the upgrade. Delete the event summary component, create a new one, and set the desired filter.

Mercury Virtual User Generator

Mercury Business Availability Center 6.2 includes Mercury Virtual User Generator (VuGen) version 8.1. Upgrade VuGen to be compatible with the Business Process Monitor for Mercury Business Availability Center 6.2, and to benefit from the following improved functionality:

Note: The version of VuGen included with Mercury Business Availability Center 6.2 is the same as that included with Mercury Business Availability Center 6.1. Therefore, if you are upgrading from Mercury Business Availability Center 6.1 and installed the version of VuGen included with 6.1, you do not need to upgrade VuGen.

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: 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 6.2.

Discovery Probe

If you are upgrading to Mercury Business Availability Center 6.2 from Mercury Business Availability Center 6.1, you must uninstall the 6.1 Discovery Probe and install Discovery Probe 6.2 before running the discovery process. To install the Discovery Probe, select **Admin** > **Platform** > **Downloads** and then click the **Auto Discovery Probe** link.

Index