OPTIMIZE

MERCURY BUSINESS AVAILABILITY CENTER™

Upgrading Mercury Business Availability Center 4.5 - 6.2

MERCURY™

BUSINESS TECHNOLOGY OPTIMIZATION

Mercury Business Availability Center

Upgrading Mercury Business Availability Center

Version 4.5 to Version 6.2

Document Release Date: June 20, 2006

MERCURY™

Mercury Business Availability Center, Version 6.2
Upgrading Mercury Business Availability Center 4.5-6.2

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_UPG4.5_6.2/01

Table of Contents

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

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

Chapter 2: Upgrade Checklist 3
Before You Begin 3
Upgrade Checklist 5

Chapter 3: Upgrading the Servers 11
Server Architecture for Mercury Business Availability Center 12
Upgrading Considerations 12
Installing Mercury Business Availability Center 6.1 and the 6.2 Add-on on a Windows Platform 13

Chapter 4: Verifying and Upgrading the Database Schema 19
Introducing Upgrade Methodology 20
Using the Verify and Upgrade Utility 20
Verifying the Database Schema.....23
Upgrading the Database Schema.....28
Creating Database Users for the Upgrade Procedure 31
Troubleshooting Database Schema Verify and Upgrade Errors 32

Chapter 5: Configuration Upgrade.....35
Upgrading Configuration Data 35

Chapter 6: Dashboard Views Upgrade 41
The Views Upgrade Page 42
Simulating a View Upgrade.....44
Upgrading a View 45
Displaying an Upgraded View.....46
Troubleshooting 46
Notes and Limitations.....47
Rollback 49

Chapter 7: Upgrading Service Level Management to Mercury Business Availability Center 6.2 51
Prerequisites....52
SLA Upgrade and the Business Process Monitor Adapter Source....53
SLA Upgrade and the SiteScope Adapter Source....55
Upgrading SLAs from 5.x to 6.2....56
Upgrading Custom Reports....59
Upgrading the Report Repository....60
Upgrading Rules Used For SLA Conversions....61
Upgrade Messages....69

Chapter 8: Switching Mercury Business Availability Center URL on the Data Collectors....75
Overview of Switching Data Collectors....75
Redirecting the Business Process Monitor URL....76
Redirecting the Client Monitor URL....77
Redirecting the SiteScope URL....78

Chapter 9: Upgrading Components to Work with Mercury Business Availability Center 6.2....81
Upgrading Business Process Monitor....82
Client Monitor....83
SiteScope....86
Real User Monitor....88
Mercury Virtual User Generator....89

Index....93

Welcome to Upgrading Mercury Business Availability Center

This guide provides detailed instructions on how to upgrade Topaz 4.5 FP2 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.

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 6.2.

Upgrade Checklist

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

Upgrading the Servers

Describes how to upgrade your servers 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.

Configuration Upgrade

Describes how to upgrade your data to Mercury Business Availability Center 6.2.

Dashboard Views Upgrade

Describes how to upgrade your Mercury Business Availability Center custom Dashboard views to Mercury Business Availability Center 6.2 views

Upgrading Service Level Management to Mercury Business Availability Center 6.2

Describes how to upgrade service level agreements (SLAs) to work with Mercury Business Availability Center 6.2

Switching Mercury Business Availability Center URL on the Data Collectors

Describes how to configure your data collectors to work with new Mercury Business Availability Center 6.2 servers.

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 Topaz 4.5 FP2.

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).

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.

Major Upgrade Steps

Upgrading your platform to Mercury Business Availability Center 6.2 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 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.

This chapter describes:	On page:
Before You Begin	3
Upgrade Checklist	5

Before You Begin

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

- Direct upgrade from Topaz 4.5 FP2 on Solaris to Mercury Business Availability Center 6.2 on Solaris is not supported. If you require this upgrade scenario, contact Mercury Customer Support.
- 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.
- In Mercury Business Availability Center 6.2, different server types are used than those in Topaz 4.5 FP2. For details, refer to "Server Architecture for Mercury Business Availability Center" on page 12.

- If you are upgrading from Topaz 4.5 FP2 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 6.2, 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 6.2.
- 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.
- During the upgrade process, SiteScope and Business Process Monitor downtime events are replicated. The scheduled downtime events will run as configured, and the replication of the downtime events has no impact on the system other than them being displayed in the Downtime/Event schedule in Mercury Business Availability Center. It is recommended that you do not remove the replicated entries unless necessary, and if so, you should contact your Mercury representative for assistance.

Upgrade Checklist

The following checklist should be used when upgrading from Topaz 4.5 FP2 to Mercury Business Availability Center 6.2:

Step	Description	Details
1 Backup files.	Backup various files and directories that are required during the upgrade process, or as a precautionary measure.	Backup the following files and directories: ➤ **MercuryAM\conf\ TopazInfra.ini** – file needed for upgrading the databases in step 6. For details on upgrading the databases, see "Verifying and Upgrading the Database Schema" on page 19. ➤ **For Topaz 4.5 FP2 systems incorporating Views** – contact Mercury Customer Support for details of backup requirements for upgrading Views in step 14. In addition, backup any other files or directories you want to keep for security or historical purposes.
2 Shut down existing Topaz 4.5 FP2 servers.	Stop the Topaz Supervisor service on each of the old Mercury Business Availability Center servers. Make sure there are no open connections to Mercury Business Availability Center databases.	➤ For Windows – Select **Start > Programs > Topaz > Administration > Stop Topaz**. ➤ For Solaris – Execute the command: **<Topaz_Home_Dir>/ scripts/run_topaz stop**.

Step	Description	Details
3 If upgrading to Mercury Business Availability Center 6.2 using the existing 4.5 FP2 server machines, uninstall Topaz 4.5 FP2.	Uninstall Mercury Business Availability Center 4.5 FP2 from all machines.	➤ For Windows – Select **Start > Programs > Topaz > Uninstall Topaz**. ➤ For Solaris – Execute the commands: **cd <installation directory> /_uninst** **./uninstall**
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 "Installing Mercury Business Availability Center 6.1 and the 6.2 Add-on on a Windows Platform" on page 13.
5 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 details on installing Mercury Business Availability Center 6.2, see *Upgrading Mercury Business Availability Center*.
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*.

Step	Description	Details
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 19.
8 Update the database port in the management database.	Before connecting to the management database, manually update the database port in the upgraded management database.	Run the following query on the upgraded management database: **UPDATE SESSIONS SET SESSION_DB_PORT = '1433' WHERE SESSION_DBTYPE IN (2,4) AND SESSION_DB_PORT IS NULL**
9 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*.	➤ For Windows – Select **Start Menu** > **Programs** > **Mercury Business Availability Center** > **Administration** > **Connect to Database**. ➤ For Solaris – Execute the command: **./setmngdbWizard.sh**

Step	Description	Details
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.	➤ For Windows – Select **Start > Programs > Mercury Business Availability Center > Administration > Enable Business Availability Center**. ➤ For Solaris – Execute the command: **<Mercury Business Availability Center server root dir>/scripts/ run_topaz start** ➤ 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 6.2 license key.	After starting Mercury Business Availability Center for the first time, and before proceeding with the steps for upgrading your data, reenter the Mercury Business Availability Center 6.2 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 configuration data.	Run all manual data upgrades.	See "Upgrading Configuration Data" on page 35.

Step	Description	Details
14 For Topaz 4.5 FP2 systems incorporating Views: Upgrade Views to Mercury Business Availability Center 5.x Dashboard.	Upgrade the views and repositories used with Topaz 4.5 FP2 to work with Mercury Business Availability Center 5.x Dashboard.	For additional instructions contact Mercury Customer Support.
15 For Topaz 4.5 FP2 systems incorporating Views: Backup the CMDB directory.	Backup the CMDB directory for use in the next step.	Backup the **MercuryAM\CMDB** directory needed for upgrading Dashboard views in step 13. For details on upgrading Dashboard views, see "Dashboard Views Upgrade" on page 41.
16 For Topaz 4.5 FP2 systems incorporating Views: Upgrade Dashboard Views.	Run the Dashboard upgrade process to upgrade Mercury Business Availability Center 5.x Dashboard to Mercury Business Availability Center 6.2.	See "Dashboard Views Upgrade" on page 41.
17 Upgrade SLAs.	Run the SLM upgrade process.	See "Upgrading Service Level Management to Mercury Business Availability Center 6.2" on page 51.
18 Switch URLs on data collectors (only if upgrading to Mercury Business Availability Center 6.2 on new servers).	If you installed the Mercury Business Availability Center 6.2 on new machines with different URLs, switch the URLs on your data collectors to report to Mercury Business Availability Center 6.2 servers.	See "Switching Mercury Business Availability Center URL on the Data Collectors" on page 75.
19 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 81.

3

Upgrading the Servers

This chapter describes how to upgrade your servers to Mercury Business Availability Center 6.2. 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	12
Upgrading Considerations	12
Installing Mercury Business Availability Center 6.1 and the 6.2 Add-on on a Windows Platform	13

Note:

- If running Topaz 4.5 FP2 in a Windows environment, you first upgrade your servers to Mercury Business Availability Center 6.1, and then install the 6.2 Add-on on top of the 6.1 servers.
- If running Topaz 4.5.2 in a Solaris environment, direct upgrade from Topaz 4.5 FP2 to Mercury Business Availability Center 6.2 on Solaris is not supported. If you require this upgrade scenario, contact Mercury Customer Support.

Server Architecture for Mercury Business Availability Center

In Mercury Business Availability Center 6.x, 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 on new machines or on the same machine(s) on which your current system is running.

If installing Mercury Business Availability Center 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 current system requirements.

If installing Mercury Business Availability Center 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 current system requirements.

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 and the 6.2 Add-on 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. After upgrading to Mercury Business Availability Center 6.1, upgrade to Mercury Business Availability Center 6.2 from the Add-on CD_ROM.

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 6.2 (Windows or Solaris) Setup CD-ROM root directory for the latest technical and troubleshooting information.

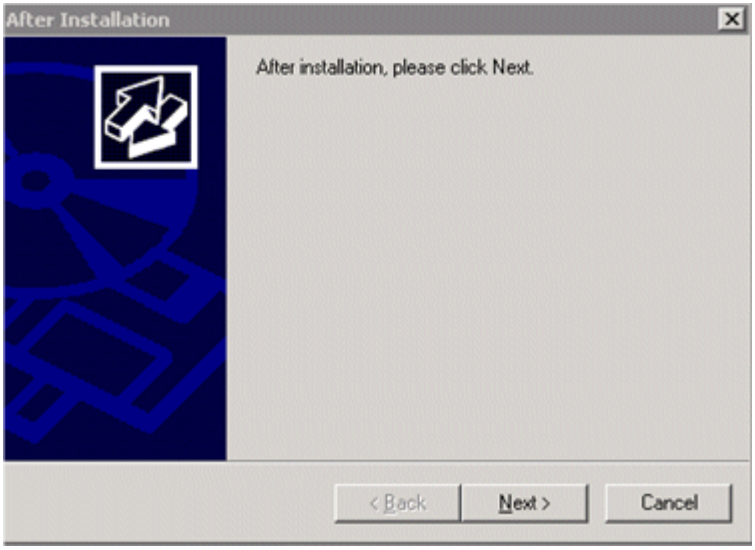
To install Mercury Business Availability Center servers on a Windows platform:

1. Insert the Mercury Business Availability Center 6.1 Windows 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 or restart servers at this stage. See "Upgrade Checklist" on page 3 for the correct sequence for connecting to the management database.

7 Install the Mercury Business Availability Center 6.2 Add-on from the Add-on CD-ROM.

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

Tip: When you are done, 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 6.2.

This chapter describes:	On page:
Introducing Upgrade Methodology	20
Using the Verify and Upgrade Utility	20
Verifying the Database Schema	23
Upgrading the Database Schema	28
Creating Database Users for the Upgrade Procedure	31
Troubleshooting Database Schema Verify and Upgrade Errors	32

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 21) and the upgrade stage (for details, see "Upgrade Stage" on page 22).

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 32.

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 31.

Note:

- During the verify stage, you must browse to the **TopazInfra.ini** file (**<Topaz root directory>\conf\TopazInfra.ini**) from the previous Topaz 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:

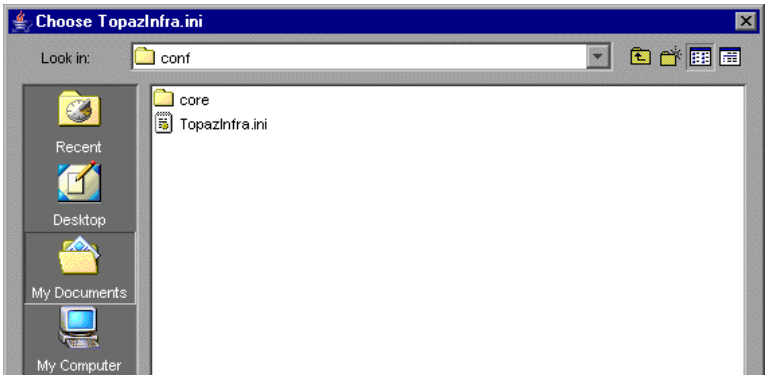
```
run_schema_upgrade.bat
```

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
```

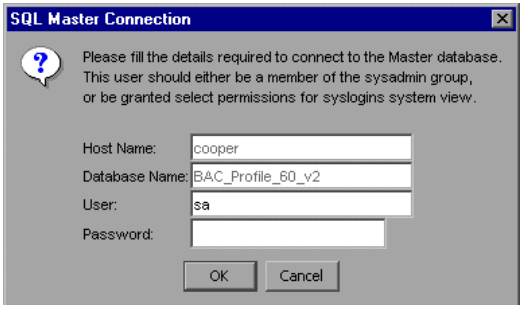
The database verify program starts.

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



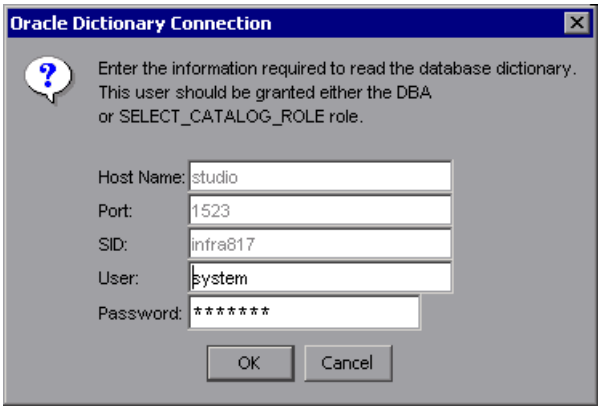
3 Specify the details required to connect to the appropriate database:

➤ 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**.

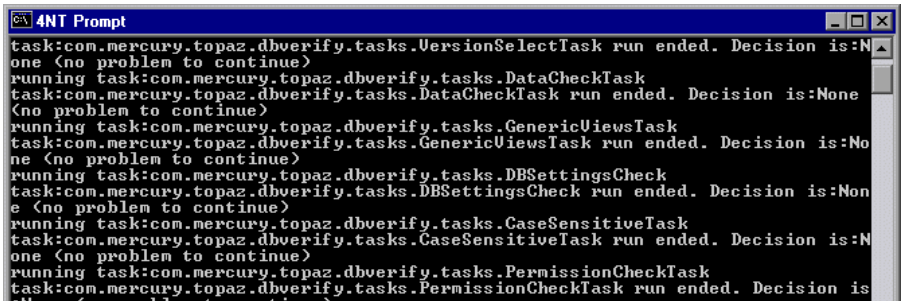
Note:

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

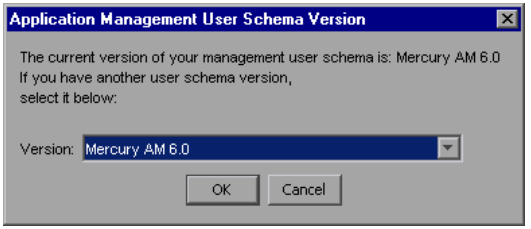
➤ If you do not want to supply your database administrator account user name and password, you can create a user name with the minimum privileges required for the verify program to operate. For details on how to create this user, see "Creating Database Users for the Upgrade Procedure" on page 31.

---

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

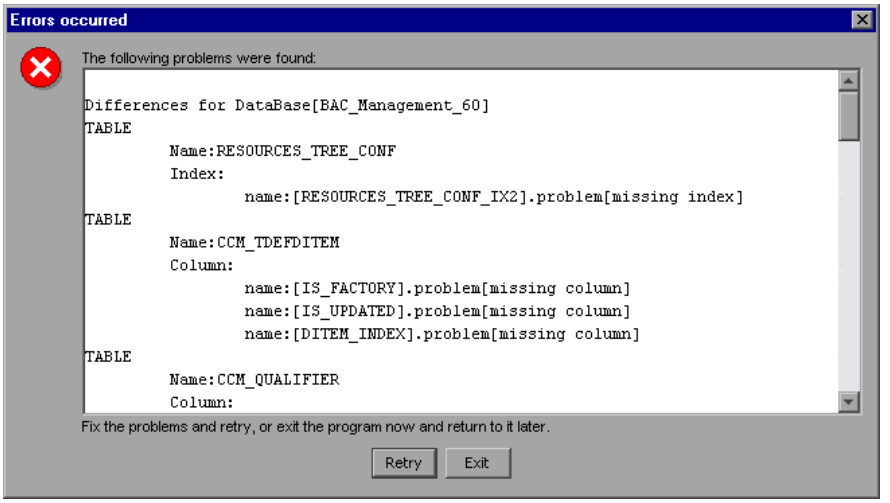


5 Check that your schema version is displayed in the Application Management User Schema Version dialog box.



Click **OK**.

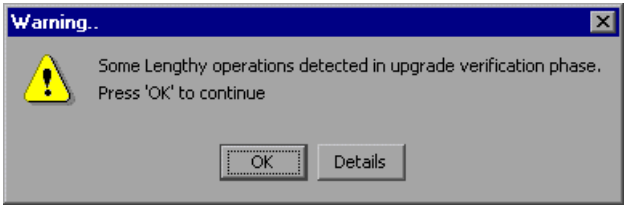
6 If problems occur during the database verification, a dialog box is displayed listing the errors.



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.

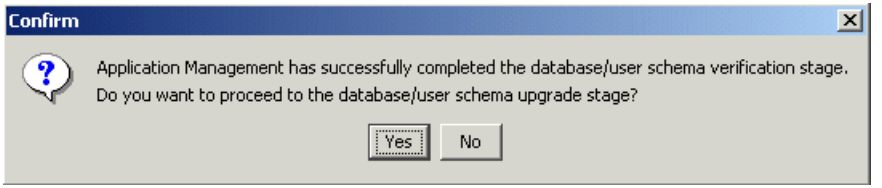
You can view a log file of the errors located in the **<Mercury Business Availability Center server root directory>\dbverify\log** directory.

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 28.

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 23), 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:

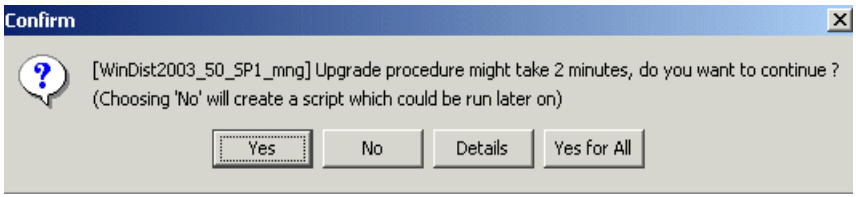
1. If you left the dbverify program open at the end of the database verification stage, click **Yes** to proceed with the database schema upgrade.

   If you closed dbverify, rerun it according to the instructions on page 23. 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 32.

---

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.

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 6.2 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 6.2.
Custom Reports Upgrade	Upgrades custom and trend reports to Mercury Business Availability Center 6.2. 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	Reconfigures the downtime/event schedules so that each schedule is event-based and can be assigned to multiple profiles. Downtime/events in Topaz 4.5 were defined per profile. If you were using the same downtime/event for different profiles you had to redefine it for each profile. When working in Mercury Business Availability Center 6.2, you can specify a specific downtime/event for a specific profile but you can also define a common downtime/event to which you can assign more than one profile. When you upgrade to Mercury Business Availability Center 6.2, you get a list of all downtime/events and their corresponding profiles. If a downtime/event appears in more than one profile, you can make it common by opening it and assigning to it all the profiles where it appears. For details, refer to the Downtime/Event Scheduling chapter in *Platform Administration*. Moves all downtime events for profiles to CMDB.
RUM MA Upgrade (5.1 to 6.2)	Removes Real User Monitor Monitor entries from the Mercury Business Availability Center 6.2 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 6.2.
Dashboard Filters Upgrade	Upgrades filter persistency to Mercury Business Availability Center 6.2. Also adds support for filter sharing between users and wildcards.

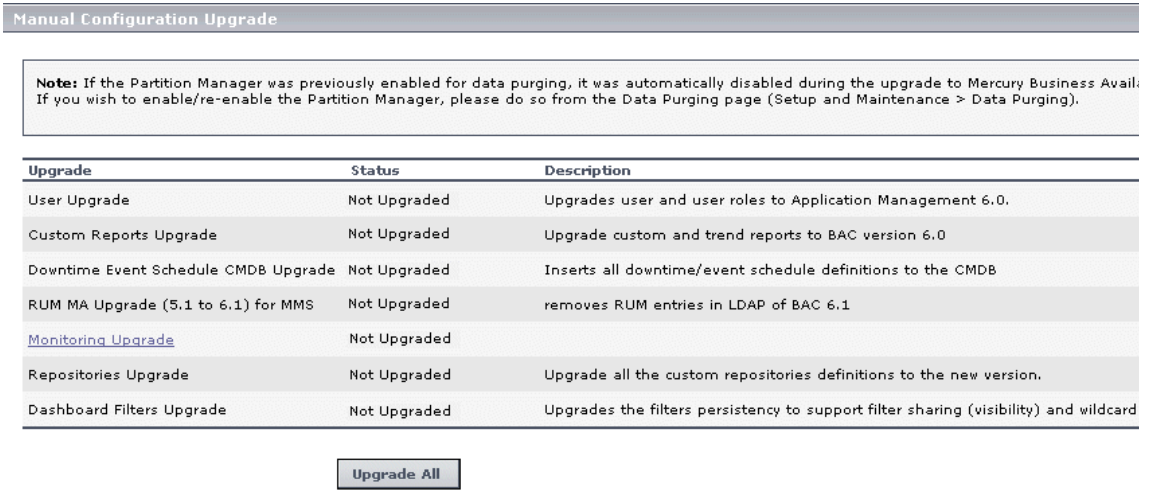
The system automatically upgrades global data and configures new data types for Mercury Business Availability Center 6.2 the first time that you access the Manual Configuration Upgrade page.

For a detailed explanation of the effects of data upgrade on certain components, see "Upgrading Components to Work with Mercury Business Availability Center 6.2" on page 81.

To run a configuration upgrade:

1. Wait until all source adapters have been inserted into the CMDB, otherwise the configuration upgrade will fail. From **CMDB Administration**, in the **Source Manager** tab, make sure that the **Last Update** column has a date for all the sources listed.
2. 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.
3. 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.

4 Select **Admin** > **Platform** > **Setup and Maintenance** > **Configuration Upgrade**. The Manual Configuration Upgrade page opens.

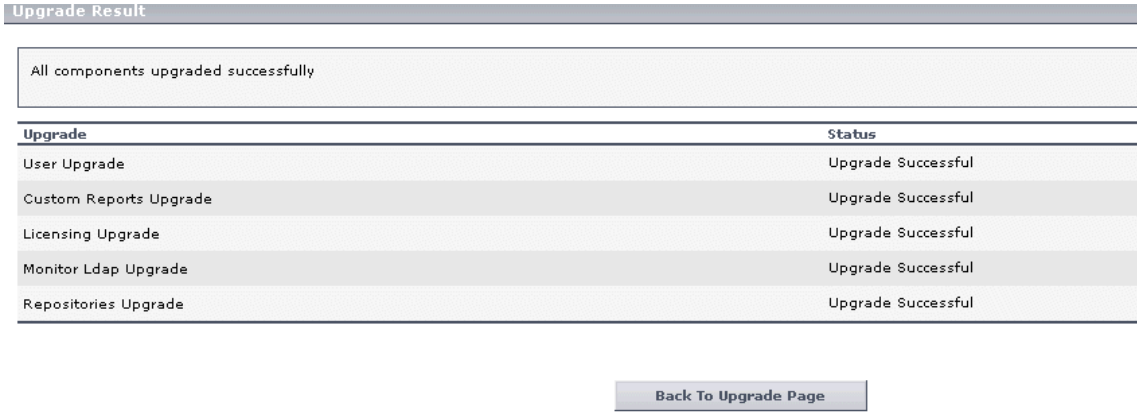


Note: Only administrators with superuser permissions can view and use the Manual Configuration Upgrade page.

---

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

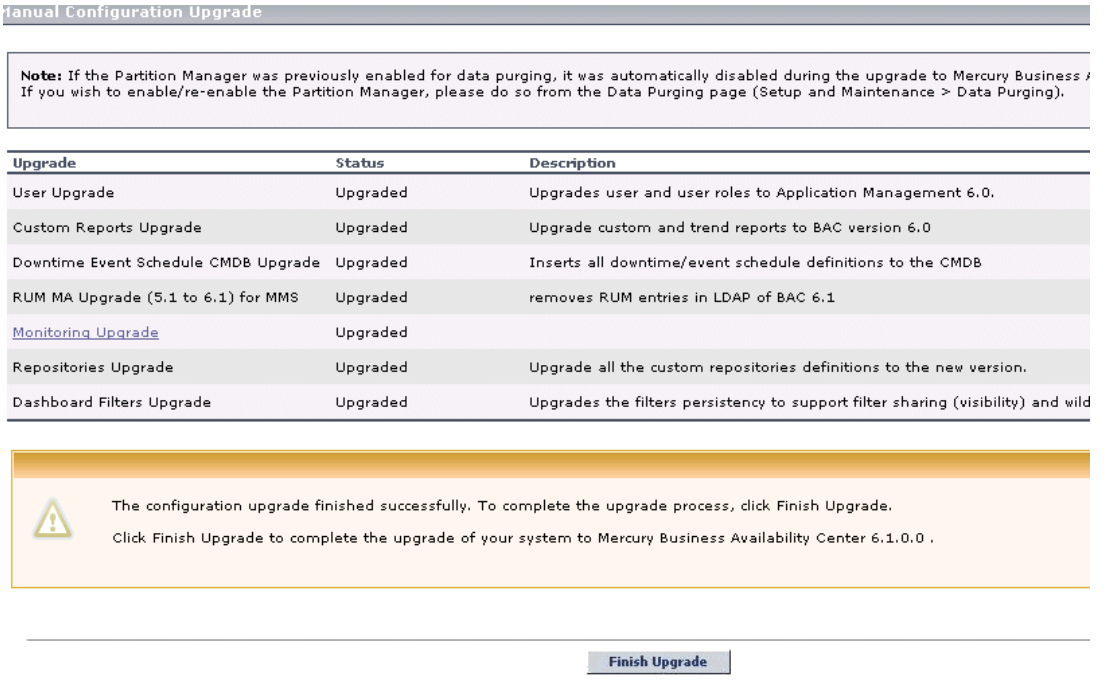
The following page opens and displays information about the data upgrade taking place.:



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**.

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



7 Click the **Finish Upgrade** button.

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

6

Dashboard Views Upgrade

This chapter describes how to upgrade your Mercury Business Availability Center 4.5 FP2 custom Dashboard views to Mercury Business Availability Center 6.2 views.

This chapter describes:	On page:
The Views Upgrade Page	42
Simulating a View Upgrade	44
Upgrading a View	45
Displaying an Upgraded View	46
Troubleshooting	46
Notes and Limitations	47
Rollback	49

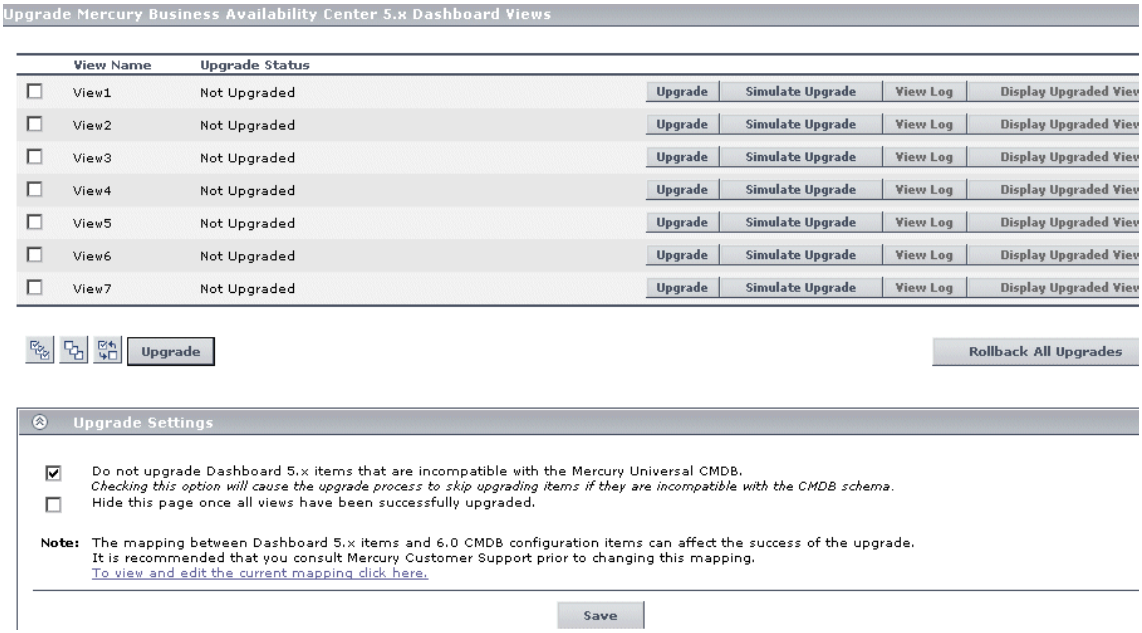
Important:

- Before starting the Dashboard views upgrade, you must first copy the **<Topaz root directory>\CMDB** directory from your old Topaz 4.2 FP2 system that you saved in step 15 of the checklist to **<Mercury Business Availability Center root directory>\CMDB\5.x** in the Mercury Business Availability Center 6.2 system.
- After upgrading all the views, refer to "Troubleshooting" on page 46 for additional steps.

The Views Upgrade Page

You upgrade your Mercury Business Availability Center 5.x custom Dashboard views to Mercury Business Availability Center 6.2 views from the Views Upgrade page in the Mercury Business Availability Center 6.2 site.

To access the Views Upgrade page, log in to Mercury Business Availability Center as an administrator with superuser permissions, and select **Admin** > **Platform** > **Setup and Maintenance** > **Views Upgrade**. The Views Upgrade page opens.



The top area of the page displays a list of all your Mercury Business Availability Center 5.1 custom Dashboard views, showing their upgrade status, and has the following action buttons for each view:

- **Upgrade.** To perform the upgrade for the view. This option is only enabled if the view has not already been upgraded.
- **Simulate Upgrade.** To perform a simulation of the upgrade before actually upgrading the view, to check for errors. This option is only enabled if the view has not already been upgraded.

- **View Log.** To display a log of the upgrade process carried out. This option is only enabled after an upgrade has been performed.
- **Display Upgraded View.** To display how the upgraded view will appear in Mercury Business Availability Center 6.2. This option is only enabled after a successful upgrade has been performed.

The middle area of the page contains selection buttons, as well as buttons for upgrading multiple views and for rolling back (undoing) already completed upgrades.

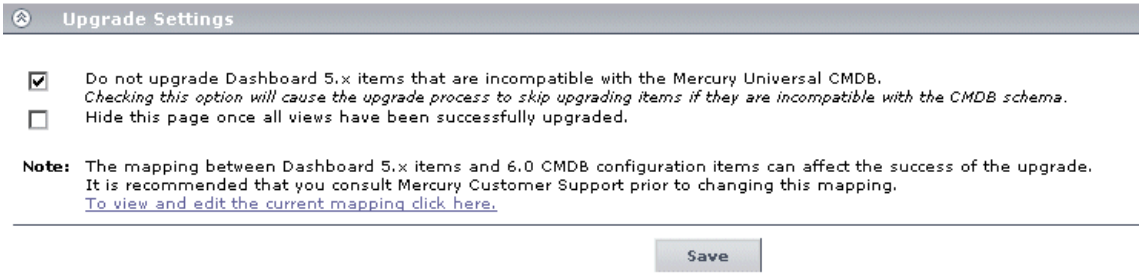


To select a view for upgrading, you can either select the check box to the left of the view, or you can use the selection buttons for **Select All**, **Clear All**, and **Invert Selection**.

The bottom area of the page contains upgrade settings.

Upgrade Settings

There are two settings you can configure in the Views Upgrade page. To activate a setting, select the check box to the left of it, and to deactivate a setting, clear the check box. Click the **Save** button at the bottom of the Upgrade Settings section to save your setting selections.



- The first setting determines how the upgrade relates to Mercury Business Availability Center 5.x Dashboard items that are incompatible with the Mercury Universal CMDB schema. Selecting this setting causes the upgrade process to ignore such incompatible items and to complete the upgrade for all the other items in the view. Not selecting this setting causes the upgrade process to fail if it encounters incompatible items.

- If you select the second setting, Mercury Business Availability Center hides the Views Upgrade page once you have upgraded all your Mercury Business Availability Center 5.1 Dashboard views to Mercury Business Availability Center 6.2.
- By clicking the link **To view and edit the current mapping click here**, you can view and edit the XML definition containing the mapping between Mercury Business Availability Center 5.x Dashboard items and Mercury Business Availability Center 6.2 CMDB configuration items.

Note: Changing any of the mappings can cause the views upgrade process to fail. It is recommended not to change any of these mappings.

Simulating a View Upgrade

To find out what errors the upgrade process will encounter during the upgrade of a specific view, you can run an upgrade simulation for the view.

To run an upgrade simulation for a view, click the **Simulate Upgrade** button for the appropriate view.

When the upgrade simulation process is complete, a log file is displayed showing details of items that can successfully be upgraded, as well as details of errors that will be encountered.

You can choose to ignore the errors during a real upgrade by activating the relevant upgrade setting (for details, see "Upgrade Settings" on page 43), or you can contact Mercury Customer Support for assistance in trying to correct the potential errors before upgrading the view.

Upgrading a View

You can choose to upgrade a single view, or multiple views.

To upgrade an individual view, click the **Upgrade** button for the appropriate view.

To upgrade multiple views, select the check boxes for the views and click the **Upgrade** button under the Views table.



When a view is successfully upgraded, its status will change from **Not Upgraded** to **Succeeded**, or **Succeeded with warnings**, and the check box for the view is disabled. The **Upgrade** and **Simulate Upgrade** buttons are disabled, and the **View Log** and **Display Upgraded View** buttons are enabled.

If a view upgrade fails, the view's status will change from **Not Upgraded** to **Failed (View Log)** and the **View Log** button is enabled.

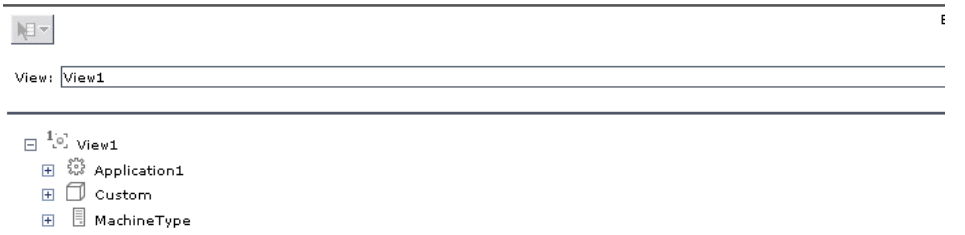
To display a log of the upgrade process showing details of items that were successfully upgraded, warnings, and any errors encountered, click the **View Log** button for the appropriate view. A new window opens displaying the upgrade log.

If errors were encountered and the upgrade was unsuccessful, you can try to correct the errors and rerun the upgrade process. For assistance in trying to correct the errors, contact Mercury Customer Support.

Displaying an Upgraded View

Once you have upgraded a view, you can display the upgraded view to see how it will look in Mercury Business Availability Center 6.2.

To display an upgraded view, click the **Display Upgraded View** button for the appropriate view. A new window opens displaying the upgraded view.



Expand the tree branches to see all configuration items.

Troubleshooting

After upgrading views, it is possible that a KPI may have two sets of Threshold objectives, which is invalid for Mercury Business Availability Center.

Once all the views have been upgraded, and you can see views and status colors in Dashboard, check to see if there are any duplicate objectives for KPIs.

To check for duplicate objectives:

On the Online Data Processing Server, open the **MercuryAM\log\ EJBContainer\bam.app.rules.log** file and search for the following text:

ERROR - Too many Objectives For KPI

If the text is not found, continue with the upgrade process according to the steps in the upgrade checklist.

If the text is located in the **bam.app.rules.log** file, correct the duplicate objectives.

To correct duplicate objectives:

1. Log in to the Mercury Business Availability Center 6.2 system with administrator privileges.
2. In **Admin** > **CMDB**, select the **Source Manager** tab.
3. Edit the **Business Process Monitor** adapter.
4. Click the **Edit Template** button to edit the Business Process Monitor adapter template.
5. In the template, locate the **customer** entity name:

   <entity id="customer"
6. In this entity, change the value of the **logic id** to a different number (in the example below, the logic id number has been changed from 1 to 17):

   <logic><id>17</id></logic>
7. Click **OK** to save the change and exit the Edit Source window.

Notes and Limitations

- The following Mercury Business Availability Center 5.x Dashboard sources are not upgraded to Mercury Business Availability Center 6.2 and will cause errors in the views upgrade process:
  - CA
  - Generic EMS
  - HP OpenView
  - HP OpenView Service Navigator (if additional levels have been generated using node factory)
  - Tivoli Tec
  - XML File

Note: Configure new source adapters for these types in Mercury Business Availability Center 6.2.

- The following Mercury Business Availability Center 5.x Dashboard sources are not supported in Mercury Business Availability Center 6.2 and will cause errors in the views upgrade process:
  - Application Mapping
  - Remedy HelpDesk
  - dbAdapter
  - Siebel
  - Service Level Management
- Mercury Business Availability Center 6.2 includes the following default source adapters:
  - Business Process Monitor
  - Real User Monitor
  - SiteScope

  The Mercury Business Availability Center 5.x source adapters of the same types are not upgraded. If you made any changes to the templates of these source adapters in Mercury Business Availability Center 5.x, and wish to have the same changes in Mercury Business Availability Center 6.2, manually change the Mercury Business Availability Center 6.2 default source adapter templates in **Admin** > **CMDB** > **Source Manager** prior to carrying out the views upgrade.
- Custom source adapters are not upgraded. If you made any changes to custom source adapter templates in Mercury Business Availability Center 5.x, and wish to have the same changes in Mercury Business Availability Center 6.2, configure a new source adapter in Mercury Business Availability Center 6.2 and manually change the source adapter template in **Admin** > **CMDB** > **Source Manager** prior to carrying out the views upgrade.

- Mercury Business Availability Center 6.2 uses default properties for CIs. If you made changes to Mercury Business Availability Center 5.x Dashboard item properties, and wish to have the same changes in Mercury Business Availability Center 6.2, manually make the changes in the **Admin** > **CMDB** > **IT Universe Manager** > **Properties** tab. To prevent your changes from being overridden in Mercury Business Availability Center 6.2, ensure that the **Allow CI Update** check box is not selected.
- In Mercury Business Availability Center 5.x, it is possible to have multiple Dashboard items with the same name, each appearing in a different view, and each with different properties.

  In Mercury Business Availability Center 6.2, each CI in the CMDB must have a unique name; this CI can appear in multiple views, but each instance of the CI will have the same properties. Each 5.x Dashboard item with the same name will collectively create one equivalent CI in Mercury Business Availability Center 6.2, and this CI will be assigned the properties from the last 5.x item with that name that is upgraded as part of a view upgrade.
- In Mercury Business Availability Center 5.x, regardless of the **Hierarchy structure** setting in the Business Process Monitor source adapter, transactions and locations at the bottom level of a Business Process Monitor tree are displayed using their configured name only. In Mercury Business Availability Center 6.2, setting the **Hierarchy structure** setting to **Transaction/Location** causes the transactions and locations at the bottom level of a Business Process Monitor tree to be displayed using an alternate format, which by default is set to **transaction name from location name**. You can change the format of the alternate display by editing the **BPM Transaction from Location** CIT from the **CI Type Manager** tab in CDMB Admin.

Rollback

You can rollback (undo) view upgrades and revert to the original Mercury Business Availability Center 5.x Dashboard views by clicking the **Rollback All Upgrades** button in the middle of the Views Upgrade page. However, Mercury Business Availability Center 5.x Dashboard views will not be visible in Mercury Business Availability Center 6.2 until they are upgraded.

Note: The rollback process will undo all completed view upgrades. You cannot roll back an individual upgraded view.

7

Upgrading Service Level Management to Mercury Business Availability Center 6.2

This chapter describes how to upgrade service level agreements (SLAs) to work with Mercury Business Availability Center 6.2. You can upgrade SLAs, Service Level Management custom reports, and reports saved to the report repository.

Mercury Business Availability Center displays the Service Level Management Upgrade page only after all other upgrade processes have concluded. That is, before you begin the Service Level Management upgrade process, Mercury Business Availability Center has upgraded all SLAs to version 5.x.

Because of differences in architecture between Mercury Business Availability Center versions 5.x and 6.x, Service Level Management calculations may not be identical in the two versions. An SLA will probably show the same result for monitor (leaf) data, but data attached to CIs nearer the root may not be the same in both versions.

This chapter describes:	On page:
Prerequisites	52
SLA Upgrade and the Business Process Monitor Adapter Source	53
SLA Upgrade and the SiteScope Adapter Source	55
Upgrading SLAs from 5.x to 6.2	56
Upgrading Custom Reports	59
Upgrading the Report Repository	60
Upgrading Rules Used For SLA Conversions	61
Upgrade Messages	69

Prerequisites

This section includes issues that should be considered before beginning the upgrade procedure:

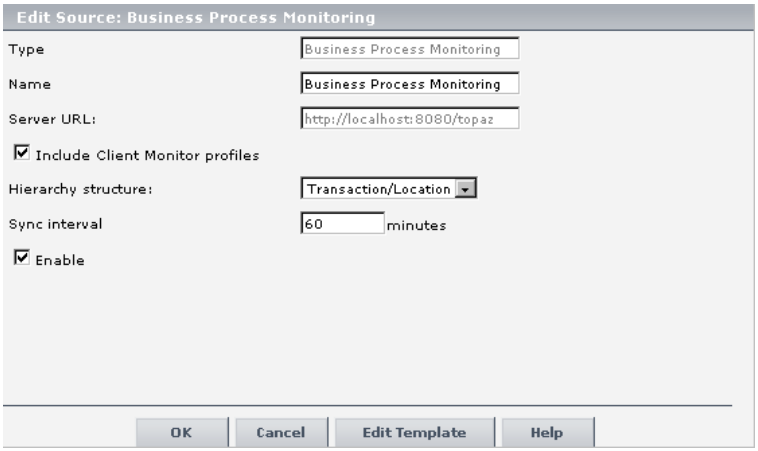
- Due to backward compatibility issues, an upgraded SLA configuration is different to the previous version. Before performing the upgrade procedure, therefore, you should save important reports to the report repository. For details, see "Saving a Report to the Report Repository" in *Application Administration*. This step is optional.
- To verify version 5.x SLA configuration data, you can display the Service Level Panorama report to view the SLA configuration in its entirety, in report format. To access the report: **Applications** > **Service Level Management** > **Offline Reports** > **Service Level Panorama**. This step is optional.
- The version 6.x default KPI definitions for the upgrade process are stored in an XML file in the Infrastructure Settings Manager (select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, click **Applications**, select **Service Level Management**, and locate the **Upgrade KPIs** entry in the Service Level Management – SLM Admin table). Prior to upgrade, it is recommended to view this file and make any necessary changes.
- The version 6.x default objectives are stored in an XML file in the Infrastructure Settings Manager (select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, click **Applications**, select **Service Level Management**, and locate the **Default KPIs** entry in the Service Level Management – SLM Admin table). Prior to upgrade, it is recommended to make yourself familiar with the objective values.
- Verify that the Monitor configuration item type (CIT) has been successfully upgraded. For details, refer to *Upgrading Mercury Business Availability Center*. Verify, too, that monitors, transactions, and measurements have been successfully upgraded by viewing them in IT Universe or Monitor Administration. For details, see *Working with Monitor Administration*.
- Because you cannot roll back the custom report upgrade, before upgrading custom reports, back up the custom reports table in the database. This step is optional.

SLA Upgrade and the Business Process Monitor Adapter Source

If a 5.x transaction is filtered by location, you can avoid losing data in version 6.x SLAs by configuring the Business Process Monitor adapter source (before performing the upgrade process) so that CIs include location information.

To configure the Business Process Monitor adapter source:

1. Display the Edit Source window: **Admin** > **CMDB** > **Source Manager**.
2. Click the **Edit** button for the Business Process Monitor source adapter.
3. Select **Transaction/Location** in the Hierarchy structure field:



For details on the hierarchy structure, see "Business Process Monitor Hierarchies" in *Source Manager Administration*.

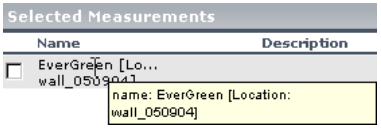
Tip: If most of the 5.x SLAs are filtered by location, set an adapter's hierarchy structure to **Transaction/Location**. If most SLAs are not filtered by location, set the hierarchy structure to **Regular**.

Example of 6.x SLA Dependent on Adapter Mode

In 5.x, an SLA may or may not include location information. The upgrade process upgrades the SLA according to:

- whether the SLA includes location information
- how the Business Process Monitor adapter source is configured

The following table shows how the upgrade process configures the 6.x SLA:

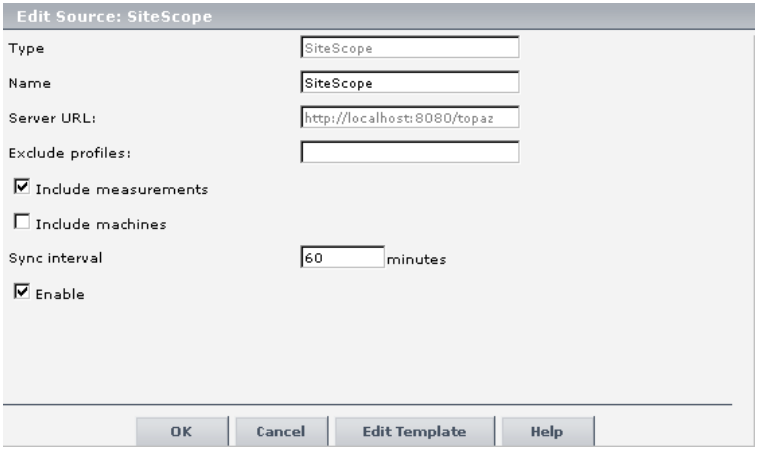
Version 5.x	**Version 6.x**	
	Business Process Monitor Adapter Source Set at Transaction/Location	**Business Process Monitor Adapter Source Set at** Regular
Transaction (EverGreen) filtered by location (wall_050904):  	EverGreen └ wall_050904 Upgrade process adds a CI of type BP Step and below it, a CI of type Transaction from Location, thereby replicating the 5.x SLA exactly.	EverGreen └ EverGreen Upgrade process does not recognize location, so adds transaction only to the SLA.
Transaction not filtered by location	EverGreen ├ wall ├ wall_05 └ wall_050904 Upgrade process adds a CI of type BP Step and below it, a CI of type Transaction from Location for all 6.2 locations.	EverGreen └ EverGreen Upgrade process replicates the 5.x SLA exactly.

SLA Upgrade and the SiteScope Adapter Source

If a 5.x monitor is filtered by monitor and measurement, you can avoid losing data in version 6.x by configuring the SiteScope source adapter (before performing the upgrade process) so that CIs include measurement performance objectives—and not only monitor objectives.

To configure the SiteScope adapter source:

1. Display the Edit Source window: **Admin** > **CMDB** > **Source Manager**.
2. Click the **Edit** button for the SiteScope source adapter.
3. Select the **Include measurements** check box in the Edit Source window:



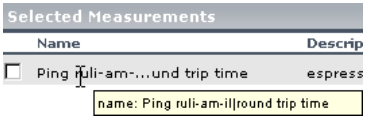
For details on editing the SiteScope source, see "SiteScope Hierarchies" in *Source Manager Administration*.

Example of 6.x SLA Dependent on Adapter Mode

In 5.x, an SLA may or may not include measurement information. The upgrade process upgrades the SLA according to:

- whether the SLA includes a SiteScope performance objective
- how the SiteScope adapter source is configured

The following table shows how the upgrade process configures the 6.x SLA:

Version 5.x	**Version 6.x**	
	SiteScope Adapter Source: Include Measurements **Check Box Selected**	**SiteScope Adapter Source:** Include Measurements **Check Box Not Selected**
Monitor (Ping ruli-am-il) filtered by measurement (round trip time):  	With measurements: Ping ruli-am-il └ round trip time Upgrade process replicates the 5.x SLA exactly.	Monitor only: Ping ruli-am-il Upgrade process adds monitor only to the SLA. **Note:** You will lose SiteScope performance objectives data for this customer.

Upgrading SLAs from 5.x to 6.2

This section explains how to upgrade service level agreements from version 5.x to 6.2 and how to delete 5.x SLAs.

The SLA table includes the following components:

- **Name.** The name of the SLA
- **Description.** The description of the SLA
- **Status**. Shows whether the upgrade process has run

You can sort the list by name, description, or status: An arrow next to a title shows by which column the SLAs are sorted, and also the direction in which the column has been sorted (that is, ascending or descending).

Actions – These buttons show the actions that you can perform on the SLA: **Simulate**, **Upgrade**, **Roll Back**, and **View Log**.

To upgrade version 5.x SLAs to version 6.2:

1. Select **Admin** > **Platform** > **Setup and Maintenance** and click the **Service Level Management Upgrade** link to open the upgrade page. The page shows a list of SLAs that are not compatible with version 6.2, organized alphabetically.
2. Locate the SLA you want to upgrade.

Note: If the SLA has the same name as a version 6.2 SLA, Service Level Management does not perform the upgrade process. You must change the name of either of the SLAs.

---

3. To view upgrade results and identify configuration changes, click **Simulate**. This step is optional but highly recommended.

   Service Level Management displays the Upgrade Warnings window. Read through the warnings. You can copy the information in this window to a text editor by copying and pasting.

   During simulation, Service Level Management updates all components of an SLA apart from its associations with KPIs and objectives.
4. If you are satisfied with the results, return to the upgrade page and click **Upgrade**. The SLA's status changes to **Upgraded** and the **Upgrade** button changes to **Roll Back**.

   At the end of the upgrade process, the Upgrade Warning window is displayed again. The first message informs you that the SLA has been upgraded successfully. The other messages are intended to help you decide whether you want to change the SLA in version 6.2 or to accept the upgraded version. Click **OK** to return to the Upgrade page.
5. To review the changes to the upgraded SLA in the Service Level Agreements page, click **Review 6.2 Configuration**. The SLA is now displayed in the list of SLAs that are compatible with version 6.2. For details on this page, see "The Service Level Agreements Page" in *Application Administration*.

Note:

- An upgraded 6.2 SLA is not identical with the original 5.x version.
- It is highly recommended to use the SLA Wizard to check the SLA, make changes to the SLA (if necessary), and save it. For details, see "SLA Definition Workflow" in *Application Administration*.

  When checking an SLA, pay special attention to the default objectives, especially if they are replacing 5.x services and groups (in the cases where the 5.x SLA does not include overall objectives).
- You must start the SLA (that is, click the **Start** button) for Service Level Management to calculate the SLA. Service Level Management calculates the SLA for the past three months only.

---

6 Click **View Log** to view a chronological account of the upgrade process and the warning messages.

Logs are saved to the Data Processing Server.

7 Continue to upgrade the SLAs. Repeat steps 2 to 5 for each SLA.

To upgrade or roll back several SLAs simultaneously:

Note: This procedure is not recommended as it slows down performance and creates many warning notifications.

---

1 Select the check boxes of the SLAs you want to upgrade or roll back.

2 Click the **Upgrade** or **Roll Back** button below the list of SLAs.

3 Continue with the upgrade process, as described in the previous section.

The next step is to upgrade the custom reports. For details, see "Upgrading Custom Reports" on page 59.

To delete version 5.x SLAs:

You can upgrade custom reports to version 6.2 only after you have upgraded all 5.x SLAs. If there are SLAs that you do not wish to upgrade (for example, because they are no longer relevant to your system), you must delete them.

1. Select the check boxes of the SLAs you want to delete.
2. Click the **Delete** button below the list of SLAs.

Upgrading Custom Reports

You can upgrade Service Level Management custom reports only when all SLAs have been upgraded.

Important: You cannot roll back custom reports. Before performing the upgrade, verify that you are satisfied with the upgraded SLAs. You can also back up the custom report tables before upgrading the SLAs.

To upgrade custom reports:

- Click **Upgrade** to update existing Service Level Management custom reports.
- Click **Review 6.2 Configuration** to access the list of custom reports.

Version 5.x Reports	Version 6.2 Report
Executive Scorecard	SLAs Summary
Availability Snapshot Performance Snapshot	SLAs Summary – only WeekToDate time range is saved, with a Day granularity
Service Status	CI Status – only the service is saved to this version
Availability Over Time vs. SLA	CIs Over Time vs. Target

Version 5.x Reports	Version 6.2 Report
Time Range Comparison	Time Range Comparison – only the service is saved to this version
Service Outages	Outages Summary – only the service is saved to this version. All outage categories are displayed.

➤ There is no Availability by Location/Group report. To produce a similar report, you must create an SLA to which you assign CIs for specific locations or groups.

Upgrading the Report Repository

Note: You can upgrade the Service Level Management report repository without upgrading the SLAs or custom reports.

➤ Click **Upgrade** to update the Service Level Management reports saved to the report repository.

➤ Click **Review 6.2 Configuration** to access the Report Repository page.

Upgrading Rules Used For SLA Conversions

Service Level Management uses a very complex algorithm to map SLAs from previous versions to version 6.2. However, due to backward compatibility issues (deriving from a difference in hierarchical structure), an upgraded 6.2 SLA is not identical with the 5.x SLA. The reasons for these differences are listed in this section.

Note: Transactions, measurements, and external data are collectively called data sources in this section.

For a note on the meaning of default objectives, see "Prerequisites" on page 52.

This section includes the following topics:

- "SLA Structure Issues" on page 61
- "Data Source and Objective Issues" on page 62
- "Downtime and Other Event Issues" on page 65
- "Service Level Management Report Issues" on page 66
- "Time Interval Issues" on page 67
- "Time Zone Issues" on page 68
- "Day of the Week Issues" on page 68
- "Notes" on page 68

SLA Structure Issues

- The upgraded SLA structure depends on the source adapter's hierarchy structure. For details, see "Business Process Source Parameters" in *Source Manager Administration*.
- The start date is set to three months prior to the date on which the SLA is upgraded. The end date is set at a year ahead of the upgrade date.

- For a previous version's SLA groups and services, the upgrade process creates a CI for each group and service (to preserve the SLA's structure).
- Any groups or services that do not have data sources are discarded.
- For a CI created from an SLA group, SLA, or service, the upgrade process gives default objectives to the CI. For SLA groups, however, if an overall objective was set in 5.x, the CI is given the 5.x overall objective and not the default objective.

Data Source and Objective Issues

- If a group includes data sources other than Business Process Monitor and SiteScope sources (that is, Real User Monitor data or external data), the data sources are discarded and are not included in the SLA.
- Previously, a data source was filtered by location. The upgrade process adds a CI of type BP Step to the SLA for each data source. Under this CI, the upgrade process adds a CI of type BP Transaction from Location for each previously-existing location.

  If a 5.x transaction was not filtered by location and, before running the upgrade process, you set the adapter to a Transaction/Location hierarchy structure (for details, see "Prerequisites" on page 52), the upgrade process assigns each existing location to a transaction (with a CI of type BP Transaction from Location). This means that each SLA includes more information.

  If the original SLA did not have a node equivalent to the CI of type BP Step and no objectives were defined for the SLA, the upgrade process assigns default objectives for the new CIs. For details on the default KPI definitions for the upgrade process, see "Prerequisites" on page 52.
- If a data source appears more than once in the original SLA, the upgrade process maps all instances of the data source to only one CI. The upgrade process selects the first occurrence of a KPI or objective. Furthermore, identical data sources running on the same location are also mapped to one CI and here, too, the first occurrence of a KPI or objective is selected.

To retain the original 5.x data, use one of the following options:

a Create an SLA (in version 6.2) for each service.

For example, a 5.x SLA includes one transaction and two services: Transaction A has an objective of 99% in Service 1, and 97% in Service 2. Create two SLAs, SLA 1 for Service 1 and SLA 2 for Service 2. Assign an objective of 99% to SLA 1 and an objective of 97% to SLA 2.

Tip: Clone the SLA, creating the same number of SLAs as there are services. Change each SLA according to one of the services. For details, see "Cloning an SLA" in *Application Administration*.

---

b Configure the upgraded SLA so that it includes more than the Exceeded and Failed targets (for details, see "Defining an SLA: Properties" in *Application Administration*). Define an objective and set its 5.x higher value to the higher target and the lower value to the lower target.

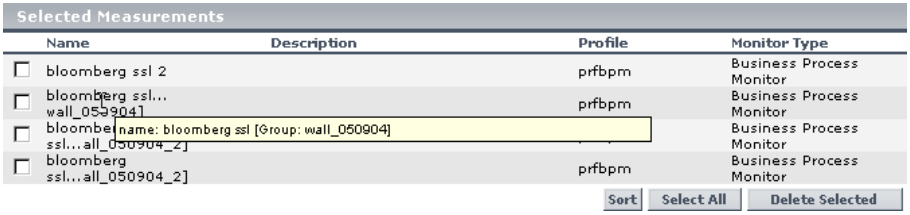
For example, a 5.x SLA includes one transaction and two services: Transaction A had an objective of 99% in Service 1, and 97% in Service 2. Set the objectives for the 6.2 SLA so that Exceeded has an objective of 99% and Met has an objective of 97%.

- If an SLA previously included a service without any data sources, the upgrade process removes the service from the SLA's hierarchy.
- If an SLA previously included a service with data sources filtered by one or more locations, the upgrade process adds a CI of type BP Step to the SLA for each location.
- If an SLA did not previously include a performance percentile objective, the upgrade process cannot add a Six Sigma performance objective to the SLA, and the objective is discarded.

  To support the Performance Six Sigma metric in version 6.2, the following objectives must have been defined for an SLA in version 5.x: percentile performance objectives and Six Sigma performance objectives.
- If the upgrade process cannot locate a Business Process Monitor or SiteScope monitor in version 6.2 that existed in version 5.x, the monitor is not added to the SLA.

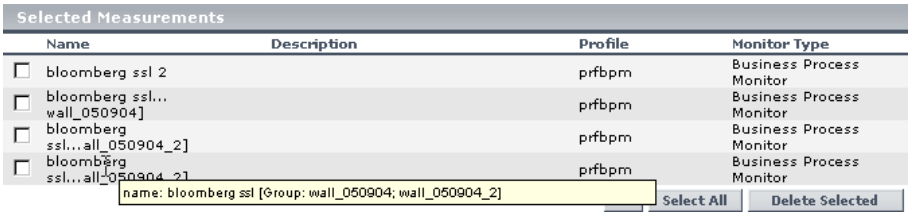
- If the upgrade process cannot locate a Business Process Monitor transaction or a SiteScope measurement in version 6.2 that existed in version 5.x, the measurement is not added to the SLA.
- Before the upgrade process, if an adapter was not configured to support CIs per measurement, the upgrade process cannot upgrade the overall performance objectives for the SLA's groups.
- The definition of a data source in version 5.x is not the same as in 6.2: a data source in version 5.x can receive data from any location, whereas a data source in version 6.2 can receive data only from locations already defined in version 6.2.
- You cannot automatically filter Business Process Monitor transactions by group. This is because groups are not included in the IT Universe. You can, however, manually define a new configuration item (CI) with dedicated selectors and associate it with the SLA.
- If a data source was previously filtered by BPM group (that do not exist in version 6.2), the upgrade process removes the group filter from the SLA for that data source. Following the upgrade, the SLA includes only one instance of the data source which does not include any group filter. Also, the SLA's objective is taken from the first occurrence found by the upgrade process.

  Example 1: a 5.x SLA contains two measurements, bloomberg ssl filtered on group wall_050409 and bloomberg ssl filtered on group wall_050409_2:



  The upgrade process creates an SLA with CI bloomberg ssl.

Example 2: a 5.x SLA contains a measurement, bloomberg ssl, filtered on two groups, wall_050904 and wall_050904_2:



The upgrade process creates an SLA with a CI named bloomberg ssl.

- Outlier trimming is not supported. Trimming is supported.

  Previously, in version 5.x, you could import outlier thresholds from the transaction threshold configuration in Monitor Administration. In version 6.2, the outlier trimming setting is no longer supported. Trimming is now calculated by the trimming condition rule parameter.

Downtime and Other Event Issues

- If an event's end date has expired (that is, the end date falls before the 6.2 SLA's start date), the upgrade process discards the event.
- Downtime granularity was changed to 5 minutes in version 6.0. Following upgrade, you should check downtime durations.

  During upgrade, event start times are rounded downwards and end times are rounded upwards. For example, the period 12:37 to 13:31 becomes 12:35 to 13:35.
- If an event is defined on a BPM group, the upgrade process discards the event (because BPM groups no longer exist in version 6.2).
- The **All SLAs** downtime value is replicated for each SLA during the upgrade process; the event receives the original name and the SLA name.
- For event CIs of type BP Group Location, the upgrade process discards the event, due to a backward compatibility issue.
- If an event's name already exists in version 6.2, the upgrade process changes the current event name by appending the SLA name in brackets to the event name.

- If an event's CI of type BP Step is not found, the upgrade process discards the event.
- If an event's CI of type BP Location is not found, the upgrade process discards the event.
- If an event's CI of type BP Transaction from Location is not found, the upgrade process discards the event.

Service Level Management Report Issues

- The following reports take a different format in version 6.2:

Version 5.x Reports	Version 6.2 Report
Executive Scorecard Availability Snapshot Performance Snapshot	SLAs Summary
Service Status	CI Status
Availability Over Time vs. SLA	CIs Over Time vs. Target
Time Range Comparison	Time Range Comparison
Service Outages	Outages Summary

- There is no Availability by Location/Group report. To produce a similar report, you must create an SLA to which you assign CIs for specific locations or groups.
- Report customizations are not upgraded.
- When upgrading custom reports, the upgrade process substitutes the SLA's creator name with the name of the user who upgraded the SLA.
- If the upgrade process does not succeed in upgrading one component of a custom report, you should use the Custom Report Manager to delete the component.
- The upgrade process calculates to-date reports till yesterday midnight.
- The upgrade process cannot upgrade reports that include active filters.

- The upgrade process can upgrade reports for predefined tracking periods only. For example, the process will not upgrade a report which includes a single value for the last three days.
- The upgrade process assigns calendar tracking periods only to reports. The minimum tracking period granularity is one hour.
- Version 6.2 does not support Service Level Management Scheduled reports produced in previous versions. That is, the reports are not upgraded.
- The upgrade process cannot assign headers or footers from version 5.x SLAs to version 6.2 SLAs Service Level Management reports. However, if the header and footer are part of a custom report, they are upgraded. You define headers and footers for reports in the Infrastructure Settings Manager. For details, see "Customizing Reports" in *Platform Administration*.
- The upgrade process stores reports in the report repository in .pdf format only.

Time Interval Issues

- Time intervals can no longer be associated with a specific SLA, but are now global functions.
- If no objectives were associated with a time interval in version 5.x, the time interval is not added to the version 6.2 SLA.
- Time intervals no longer include calculation metrics, which are now incorporated in a KPI's business rule. Therefore, you cannot now define different metrics for a CI's time intervals (for example, you cannot define an average performance metric for the 24x7 time interval, and a percentile performance metric for Business Hours).
- For version 6.2, each time interval is unique and includes a specific schedule. Previously, it was possible to define different schedules for a time interval, depending on the SLA with which the time interval was associated. During the upgrade process, only one time interval with one schedule is created, based on the time interval name. All SLAs that were associated with the previous time interval (no matter which schedule was chosen for each SLA) are now associated with the new time interval. Check each SLA; if the schedule is not suitable, create a time interval and associate it with the SLA.

Time Zone Issues

➤ If a version 5.x time zone is not supported in version 6.2, the upgrade process assigns to the SLA the first occurrence of a time zone with the same time difference as the 5.x time zone.

Day of the Week Issues

➤ During upgrade, if the first day of the week has not been defined for the same day in versions 5.x and 6.2, you are asked to choose which definition to use as a default.

Notes

➤ Any changes you make to running 6.2 SLAs (configuration changes, time interval changes, or downtime event changes) do not affect the SLA retroactively, unless the changes are made before you start the SLA. To update the SLA for previous tracking periods, you must recalculate the data. For details, see "Recalculation" in *Application Administration*.

➤ Service Level Management can recalculate SLAs for the past three months only. (This parameter is configurable in the Infrastructure Settings Manager. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**, click **Applications**, select **Service Level Management**, and locate the **Recalculation period limit** entry in the Service Level Management – SLM Admin table.)

➤ The upgrade process can fail if one of the following is exceeded: the CMDB object quota, the active TQL quota, the number of views.

Upgrade Messages

The following table includes the messages that Service Level Management displays following the successful upgrade of an SLA. The message order in this table is the same as in the Service Level Management application.

Message	Description
SLA end date is set to (<value>).	The start date is set to three months prior to the date on which the SLA is upgraded. The end date is set at a year ahead of the upgrade date. **Note:** The start date is configurable. For details, see the explanation in "Notes" on page 68.
Time zone <value> is not supported in 6.2. Assigning SLA to <value> time zone instead.	If a version 5.x time zone is not supported in version 6.2, the upgrade process assigns to the SLA the first occurrence of a time zone with the same time difference as the 5.x time zone.
SLA Owner name not found (User ID: <value>).	If a version 5.x does not include a user ID, the SLA owner name is ignored.
Time Interval (<value>) already exists. Associating it with the SLA. Verify that its scheduling matches.	For version 6.2, each time interval is unique and includes a specific schedule. Previously, it was possible to define different schedules for a time interval, depending on the SLA with which the time interval was associated. During the upgrade process, only one time interval with one schedule is created, based on the time interval name. All SLAs that were associated with the previous time interval (no matter which schedule was chosen for each SLA) are now associated with the new time interval. Check each SLA; if the schedule is not suitable, create a time interval and associate it with the SLA.
Time Interval (<value>) has no objectives in 5.x, and therefore is not added to the 6.2 SLA.	If no objectives were associated with a time interval in version 5.x, the time interval is not added to the version 6.2 SLA.
Service (<value>) had no data sources, removed from SLA's hierarchy.	If an SLA previously included a service without any data sources, the upgrade process removes the service from the SLA's hierarchy.

Message	Description
Group (<value>) contains Data Sources of type other than BPM and SiS. Those Data Sources are discarded.	The upgrade process upgrades Business Process Monitor and SiteScope data sources only. Other data sources, such as Real User Monitor and custom classes, are discarded.
Service Data Source (<value>) is filtered by several locations. Adding CI for each of the locations.	Previously, a data source was filtered by location. The upgrade process adds a CI of type BP Step to the SLA for each data source. Under this CI, the upgrade process adds a CI of type BP Transaction from Location for each previously-existing location. If the original SLA did not have a node equivalent to the CI of type BP Step and no objectives were defined for the SLA, the upgrade process assigns default objectives for the new CIs.
Service Data Source (<value>) is filtered by single location. Adding CI the location.	

Message	Description
Service Data Source (<value>) ingredients already appears in the SLA. Please note that the objectives were already upgraded.	If a data source appears more than once in the original SLA, the upgrade process maps all instances of the data source to only one CI. The upgrade process selects the first occurrence of a KPI or objective. Furthermore, identical data sources running on the same location are also mapped to one CI and here, too, the first occurrence of a KPI or objective is selected. **To retain the original 5.x data, use one of the following options:** ➤ Create an SLA (in version 6.2) for each service. For example, a 5.x SLA includes one transaction and two services: Transaction A has an objective of 99% in Service 1, and 97% in Service 2. Create two SLAs, SLA 1 for Service 1 and SLA 2 for Service 2. Assign an objective of 99% to SLA 1 and 97% to SLA 2. **Tip:** Clone the SLA, creating the same number of SLAs as there are services. Change each SLA according to one of the services. For details, see "Cloning an SLA" in *Application Administration*. ➤ Configure the upgraded SLA so that it includes more than the Exceeded and Failed targets (for details, see "Defining an SLA: Properties" in *Application Administration*). Define an objective and set its 5.x higher value to the higher target and the lower value to the lower target. For example, a 5.x SLA includes one transaction and two services: Transaction A has an objective of 99% in Service 1, and 97% in Service 2. Set the objectives for the 6.2 SLA so that Exceeded has an objective of 99% and Met has an objective of 97%.
Service Data Source (<value>) ingredients do not appear in 6.2, and therefore the data source is not added.	If the data source does not exist in the CMDB, the data source is not added to the 6.2 SLA.
Service Data Source (<value>) is filtered by Group(s). Adding CI for each of the locations.	If an SLA was previously filtered by BPM groups (that do not exist in version 6.2), the upgrade process adds a CI of type BP Step with a child for each location.

Message	Description
Service Data Source (<value>) is filtered by Location(s), but the model does not support by-location CIs.	If a 5.x SLA includes transactions filtered by one or more locations and the hierarchy structure is set to Regular, the upgrade process adds a CI of type BP Step to the SLA without any children. To include locations in the SLA, you must change the hierarchy structure. For details, see "SLA Upgrade and the Business Process Monitor Adapter Source" on page 53.
Service Data Source (<value>) is not filtered, but the model supports by-location CIs.	If a 5.x SLA includes transactions not filtered by location and the hierarchy structure is set to Transaction/Location, the upgrade process assigns all 6.2 locations to a transaction (with a CI of type BP Transaction from Location). Following the upgrade process, when you check the SLA, you can remove the unwanted locations. **Note:** Do not remove all locations from the transaction, otherwise the data is disabled. You must leave at least one location (as a data source) in the SLA.
Performance 6-Sigma Objective cannot be defined for group (<value>), because no performance objective defined.	If an SLA did not previously include an overall performance percentile objective, the upgrade process cannot add a Six Sigma performance objective to the SLA, and the objective is discarded. To support the Performance Six Sigma metric in version 6.2, the following objectives must have been defined for an SLA in version 5.x: percentile performance objectives and Six Sigma performance objectives.
The SiteScope monitor was not found in version 6.2 for the measurement (<value>).	If the upgrade process cannot locate a SiteScope monitor in version 6.2 that existed in version 5.x, the monitor is not added to the SLA. For a note on other reasons for a missing object, see "Prerequisites" on page 52.
The SiteScope measurement was not found in version 6.2 for the version 5.1 measurement (<value>).	If the upgrade process cannot locate a SiteScope measurement in version 6.2 that existed in version 5.x, the measurement is not added to the SLA.

Message	Description
SiteScope has not been configured to support by-measurement CIs, so performance objectives cannot be upgraded for measurement (<value>).	If performance objectives have been defined for a version 5.x SLA that includes a service with System class (SiteScope) measurements, you can avoid losing the measurement data in version 6.2. Configure the SiteScope source adapter so that the upgrade process upgrades measurement performance objectives—and not only monitor objectives. This must be done before performing the upgrade process. For details, see "SLA Upgrade and the SiteScope Adapter Source" on page 55.
SiteScope has not been configured to support by-measurement CIs, so the overall performance objective cannot be upgraded for group (<value>).	
Cannot upgrade event defined on BPM group. Event name: (<value>).	If an event is defined on a BPM group, the upgrade process discards the event (because BPM groups no longer exist in version 6.2).
Events on location from profile are not supported. Event: (<value>).	Due to backward compatibility issues, the upgrade process cannot upgrade events based on a specific profile's location.
Discarding event (<value>). Its end date has expired.	If an event's end date has expired (that is, the end date falls before the 6.2 SLA's start date), the upgrade process discards the event.
The event name (<value>) already exists. Changing name to (<value>).	If an event's name already exists in version 6.2, the upgrade process changes the current event name by appending the SLA name in brackets to the event name.
Location CI (<value>) was not found for event (<value>). Discarding this event.	If an event's location cannot be mapped to a 6.2 CI, the upgrade process discards the event. The reason that the event is not found in version 6.2 may be because the object on which the event is based no longer exists. For a note on other reasons for a missing object, see "Prerequisites" on page 52.
BP Group CI was not found for event (<value>). Discarding this event.	
BP Step CI was not found for event (<value>). Discarding this event.	
BP transaction from location CI was not found for event (<value>). Discarding this event.	

Message	Description
Changing event (<value>) scheduling. Previous scheduling: start limit date <value>, event range: <value> - <value>. Upgraded scheduling: start limit date <value>, event range: <value> - <value>.	➤ Due to backward compatibility issues, the upgrade process concatenates the start limit date and hour to one value. ➤ During upgrade, event start times are rounded downwards and end times are rounded upwards. For example, the period 12:37 – 13:31 becomes 12:35 – 13:35. ➤ Downtime granularity was changed to 5 minutes in version 6.0. Following upgrade, you should check downtime duration periods.
Changing event (<value>) start limit time from <value> to <value>.	
Changing event (<value>) scheduling from <value> - <value> to <value> - <value>.	

8

Switching Mercury Business Availability Center URL on the Data Collectors

This chapter describes how to configure your data collectors to work with new Mercury Business Availability Center 6.2 servers.

This chapter describes:	On page:
Overview of Switching Data Collectors	75
Redirecting the Business Process Monitor URL	76
Redirecting the Client Monitor URL	77
Redirecting the SiteScope URL	78

Overview of Switching Data Collectors

If you install Mercury Business Availability Center 6.2 on a new machine or machines, you must update all the data collectors (Real User Monitor, Business Process Monitor, Client Monitor, and SiteScope) to report to the new Mercury Business Availability Center 6.2 servers.

Note: If you installed Mercury Business Availability Center 6.2 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

Use the following procedure if you need to update the Business Process Monitor data collector to report to the new Mercury Business Availability Center 6.2 server.

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 6.2 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.
5. Add scripts used for Topaz 4.5 FP2 Business Process Transaction Monitors to the Mercury Business Availability Center 6.2 Script Repository. For details on adding scripts to the Script Repository from Monitor Administration, refer to *End User Management Data Collector Configuration*.

Redirecting the Client Monitor URL

Use the following procedure if you need to update the Client Monitor data collector to report to the new Mercury Business Availability Center 6.2 server.

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

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.

5 Add scripts used for Topaz 4.5 FP2 Client Monitor Transaction Monitors to the Mercury Business Availability Center 6.2 Script Repository. For details on adding scripts to the Script Repository from Monitor Administration, refer to *End User Management Data Collector Configuration*.

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.

5 Add scripts used for Topaz 4.5 FP2 Client Monitor Transaction Monitors to the Mercury Business Availability Center 6.2 Script Repository. For details on adding scripts to the Script Repository from Monitor Administration, refer to *End User Management Data Collector Configuration*.

Redirecting the SiteScope URL

If Mercury Business Availability Center 6.2 is installed using the same machines as the previous Topaz 4.5 FP2 system, it is not necessary to redirect the SiteScope URL for SiteScope 8.x, but you must update the port number.

To redirect the port number for version 8.x if Mercury Business Availability Center 6.2 is installed on existing Topaz 4.5 FP2 machines:

1. Before the upgrade, detach SiteScope from Mercury Business Availability Center.
2. After the upgrade, edit SiteScope in Monitor Administration and change the port to the port number of the new SiteScope interface. The default port number is 8080.
3. Attach SiteScope to Mercury Business Availability Center

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>

9

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.

This chapter describes:	On page:
Upgrading Business Process Monitor	82
Client Monitor	83
SiteScope	86
Real User Monitor	88
Mercury Virtual User Generator	89

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, 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 6.2 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 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.

There is no upgrade path from Real User Monitor version 5.x and earlier to version 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 in the same directory as the previous Real User Monitor. The Real User Monitor database must be installed on the same machine as the prior version.

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.

Index

A

architecture (server) 12

B

Business Process Monitor
    upgrading 82

C

checklist
    upgrade 5
Client Monitor, upgrading 83
components, upgrading 81
configuration, upgrading 35

D

dashboard views
    display upgraded view 46
    notes and limitations 47
    troubleshooting 46
    upgrade rollback 49
    upgrade settings 43
    upgrade simulation 44
    upgrading 41, 45
data collectors
    changing URL 75
    upgrading 81
database schema
    upgrading 19, 28
    verifying 19, 23
database users, creating for upgrade 31
dbverify 20
downtime events
    variations 65

I

Infrastructure Settings Manager
    upgrading SLAs 52, 67

J

Java run time, modifying mx parameter 32

R

Real User Monitor, upgrading 88
rollback, upgraded views 49

S

server architecture 12
server installation
    Windows platform 13
servers, upgrading 11
service level agreements
    differences between 5.x and 6.1 61
    upgrading from 5.x to 6.1 56
Service Level Management
    report variations 66
    upgrading custom reports 59
    upgrading report repository 60
    upgrading to work with Mercury
        Business Availability Center 6.1 51
SiteScope
    upgrading 86

T

time intervals
    variations 67
transactions
    differences with objectives 62

troubleshooting
    dashboard views 46
    dbverify errors 32
    views 46

U

upgrade
    checklist 5
    components 81
    configuration 35
    considerations 12
    dashboard views 41, 45
    database schema 19
    dbverify utility 20
    getting started 3
    introduction 1
    major steps 2
    methodology 20
    servers 11
    views 41, 45
upgrade settings, dashboard views 43
upgrade simulation
    dashboard views 44
    views 44
upgrade view, display 46
URL, changing on data collectors 75

V

verify utility 20
verifying database schema 19
views
    display upgraded view 46
    notes and limitations 47
    troubleshooting 46
    upgrade 45
    upgrade rollback 49
    upgrade settings 43
    upgrade simulation 44
    upgrading 41
Virtual User Generator, upgrading 89

W

Windows platform, upgrading servers 13