HP Business Availability Center

for the Windows and Solaris operating systems

Software Version: 7.0

Platform Administration

Document Number: BACPLAT7.0/01
Document Release Date: February 2008
Software Release Date: August 2007

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Third-Party Web Sites

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

Copyright Notices

Trademark Notices

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Intel®, Pentium®, and Intel® Xeon™ are trademarks of Intel Corporation in the U.S. and other countries.

Java™ is a US trademark of Sun Microsystems, Inc.

Microsoft®, Windows®, Windows NT®, and Windows® XP are U.S registered trademarks of Microsoft Corporation.

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California.

Unix® is a registered trademark of The Open Group.

Documentation Updates

This manual's title page contains the following identifying information:

- Software version number, which indicates the software version
- Document release date, which changes each time the document is updated
- Software release date, which indicates the release date of this version of the software

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

http://ovweb.external.hp.com/lpe/doc_serv/

Support

Mercury Product Support

You can obtain support information for products formerly produced by Mercury as follows:

- If you work with an HP Software Services Integrator (SVI) partner (**http://h20230.www2.hp.com/svi_partner_list.jsp**), contact your SVI agent.
- If you have an active HP Software support contract, visit the HP Software Support Web site and use the Self-Solve Knowledge Search to find answers to technical questions.
- For the latest information about support processes and tools available for products formerly produced by Mercury, we encourage you to visit the Mercury Customer Support Web site at: **http://support.mercury.com**.
- If you have additional questions, contact your HP Sales Representative.

HP Software Support

You can visit the HP Software Support Web site at: **www.hp.com/go/hpsoftwaresupport**

HP Software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To find more information about access levels, go to:
http://h20230.www2.hp.com/new_access_levels.jsp

To register for an HP Passport ID, go to:
http://h20229.www2.hp.com/passport-registration.html

Table of Contents

PART VIII: AUTHENTICATION

Welcome to This Guide

This guide provides detailed instructions on how to configure and administer the HP Business Availability Center platform.

How This Guide Is Organized

The guide contains the following parts:

Part I Accessing and Navigating HP Business Availability Center

Describes the various options for logging into and accessing HP Business Availability Center and how to navigate among its applications and administration options.

Part II Setup and Maintenance

Describes how to download components, manage licenses, administrate the profile and management databases, enable data purging, configure the infrastructure settings, view the audit log, and configure MMS Import.

Part III Data Collection

Describes how to configure the settings and resources related to data collection, including upgrading and removing data collectors; scheduling downtime and events; filtering and removing transactions, locations, and groups; setting the order for transactions to run; adding and updating definitions of user-defined samples; and setting filters for report data.

Part IV Scheduled Reports

Describes how to define and schedule user-defined reports.

Part V User Management

Describes how to create and manage users and user groups, as well as the permissions that apply to them across the platform's resources.

Part VI Personal Settings

Describes the customizations to set per user, including refresh interval, time zone, menus, and default pages.

Part VII Report Administration

Describes how to generate a report automatically and how to view, in a reports log, the errors that occurred when generating a report and all activities carried out on a report: creating a new report, generating a report, modifying the report filter(s), drilling down in reports, and so forth.

Part VIII Authentication

Describes how to configure HP Business Availability Center to work with authentication strategies.

Who Should Read This Guide

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

- HP Business Availability Center administrators
- HP Business Availability Center platform administrators

Readers of this guide should be knowledgeable about enterprise system administration and highly knowledgeable about HP Business Availability Center.

Getting More Information

For a complete list of all online documentation included with HP Business Availability Center, additional online resources, information on acquiring documentation updates, and typographical conventions used in this guide, see the the *HP Business Availability Center Deployment Guide* PDF.

Part I

Accessing and Navigating HP Business Availability Center

1

Logging into HP Business Availability Center

This chapter provides details on how to log into HP Business Availability Center.

Logging In and Out

You access HP Business Availability Center using a supported Web browser, from any computer with a network connection (intranet or Internet) to the HP Business Availability Center servers. The level of access granted a user depends on the user's permissions. For details on granting user permissions, see "Permissions Management" on page 311.

For details on Web browser requirements, as well as minimum requirements to successfully view HP Business Availability Center, see the "Reviewing System Requirements" chapter in the *HP Business Availability Center Deployment Guide* PDF.

Note to HP Managed Software Solutions customers: You access HP Business Availability Center via the Managed Software Solutions customer support Web site (mms.mercury.com).

Logging In

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

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

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

Customers running previous versions of HP Business Availability Center can still use bookmarks set to access the URL **http://<server_name>/mercuryam**.

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

Initial access can be gained using the default superuser login parameters: Login Name=**admin**, Password=**admin**. It is recommended that the system superuser change this password immediately to prevent unauthorized entry. For details on changing the password, see "Managing Users" on page 368.

For details on creating users in the HP Business Availability Center system, see "Creating Users" on page 365.

For details on login authentication strategies that can be used in HP Business Availability Center, see "Authentication Strategies" on page 411.

For login troubleshooting information, see "Troubleshooting HP Business Availability Center Login" on page 25.

Note: For details on accessing HP Business Availability Center securely, see the *HP Business Availability Center Hardening Guide* PDF.

Logging Out

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

To log out:

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

Advanced Login Options

Advanced login options enable you to automate login, limit login access, and provide direct login capabilities to specific pages in HP Business Availability Center.

This section includes the following topics:

Enabling Automatic Login in the Login Page

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

To enable automatic login:

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

Guidelines for Using Automatic Login

Keep the following in mind when using this option:

- Using the **Logout** option at the top of the HP Business Availability Center page cancels the option. If a user has logged out, the next time the user logs in, the Login page opens and the user must enter a login name and password. This can be useful if another user must log in on the same machine using a different user name and password.

- Automatic login can be enabled for a specific period of time (the default is 14 days). After that period of time has elapsed, the option must be selected again to enable it.
- This option could be considered a security risk and should be used with caution.
- You can configure this option and modify the default values in Infrastructure Settings. To access the relevant settings in Infrastructure Settings, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** > **Foundations** > **Security**. In this context, you can:
  - Completely remove this option from appearing in the login page by setting the **Enable automatic login** value to **false** (**true** is the default value).
  - Customize the number of days to enable the option by editing the **Days to remember login** value to the desired number of days (14 is the default value).

    For details on using the Infrastructure Settings page, see "Infrastructure Settings" on page 79.

Using the Automatic Login URL Mechanism

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

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

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

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

Limiting Access by Different Machines Using the Same Login Name

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

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

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

Feature Limitation

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

Using the Link to This Page Option (Direct Login) to Open a Specific Page

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

Depending on how you configure Direct Login, the receiver accesses the page using his own user name and password, or through a URL encrypted with either your user name and password or another user's user name and password. If accessing the page through an encrypted URL, the receiver bypasses the HP Business Availability Center login page because the URL supplies the user name and password information.

To configure direct login to a specific page:

1. Go to the page in HP Business Availability Center that you want to send to the receiver.
2. Select **Admin** > **Link to this page**. The Link to this page dialog box opens.
3. Select the method that the receiver uses to access the target page:
   - Choose **No credentials** if the receiver uses his own user name and password to access the page.
   - Choose **My credentials** if the page is accessed through your user name and password.
   - Choose **Use credentials** and fill in **Login name** and **Password** if the page is accessed through the login name and password you supply here. There is no default user account, so you must fill in both fields.
4. Select a method to generate the login resource:
   - Click **Create link** to generate a URL that, when loaded into the browser, opens the defined page. The URL is displayed in the Link box. Use the **Copy to clipboard** button to copy the URL to the clipboard for pasting elsewhere. If login credentials are specified, the user name and password are encrypted in the query string so that no login information is revealed.

➤ Click **Generate HTML** to generate an HTML page called **directLogin.html** that, when loaded into the browser, opens the defined page. Save the file to an appropriate location. If login credentials are specified, the user name and password are encrypted in the HTML source so that no login information is revealed.

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

6 Send the URL or HTML page to the receiver (for example, via e-mail or SMS) with appropriate usage instructions.

Limitations

➤ The user name sent in the URL must be an account with sufficient privileges to access the target page. If the account does not have sufficient privileges, the receiver is sent to the page above the target page.

For example, you want to direct the receiver to the Infrastructure Settings page. You configure Direct Login, however, with **Use Credentials** of a regular user. When the receiver uses this URL, he is sent to the Setup and Maintenance page and he cannot access Infrastructure Settings.

➤ Direct Login does not verify the user name and password sent in the URL. Verification is done only when the receiver tries to access the target page. If the user name and password are not correct, or the user account has been deleted, the receiver is sent to the HP Business Availability Center login page to log in normally. Once he is logged in, he does not proceed to the target page. There is no informational message about the reason for the Direct Login failure.

Security Notes and Precautions

➤ The user name and password in the URL are encrypted so that no login information is ever revealed.

➤ Sending encrypted information by e-mail still entails a security risk since the mail system can be breached. If the e-mail is intercepted, access to HP Business Availability Center is given to an unknown party.

➤ Do not use the URL from Direct Login as a link in any Web page.

➤ The receiver has all privileges of the user name he was given in the URL. Once the receiver accesses the target page, he can perform all actions permitted to that user name anywhere in HP Business Availability Center.

Troubleshooting HP Business Availability Center Login

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

Error No.	Problem/Possible Cause(s)	Solution(s)
LI001	HP Business Availability Center failed to connect to the JBoss application server running on the Gateway Server. This may be due to: ➤ JBoss server being down ➤ problems with the HP Business Availability Center service ➤ the port required by the application server being used by another application	**Solution 1:** Close all applications on the Gateway Server machine and restart the machine. **Solution 2:** Ensure that there are no other running applications on the Gateway Server machine that use this port (for example, applications that run from the Startup directory, another instance of JBoss, an MSDE or MS SQL Server, or any other process).

Error No.	Problem/Possible Cause(s)	Solution(s)
LI002	The JBoss application server running on the Gateway Server is not responding or is not installed correctly.	Restart the HP Business Availability Center application.
LI003	The management database might be corrupted (for example, if a user record was accidentally deleted from the database).	Try logging in as a different user, or ask the HP Business Availability Center administrator to create a new user for you.
LI004	The connection between the Tomcat servlet engine and the JBoss application server failed due to an RMI exception. This may be due to problems in RMI calls to JBoss.	Ensure that none of the JBoss ports are in use by another process. Also, ensure that the RMI ports are bound. For details on ports, see "Bus Communication and Port Usage" in the *HP Business Availability Center Deployment Guide* PDF.

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

Error No.	Problem/Possible Cause(s)	Solution(s)
LI005 (*cont'd)*	The HP Business Availability Center login fails or hangs.	**Solution 3:** Verify that the user has appropriate access permissions. For details, see "Permissions Management" on page 311. **Solution 4:** Verify that an authentication strategy has been configured correctly. For details, see "Authentication Strategies" on page 411.
LI006	The HP Business Availability Center login fails. This may be due to: ➤ incorrect cookie settings in the Web browser ➤ an unsupported character in the names of the machines running the HP Business Availability Center servers	**Solution 1:** Ensure that the client Web browser is set to accept cookies from HP Business Availability Center servers. **Solution 2:** Ensure that there are no underscore characters (_) in the names of the machines running the HP Business Availability Center servers. If this is the case, either rename the server or use the server's IP address when accessing the machine. For example, to access HP Business Availability Center, use http://111.222.33.44/HPBAC instead of http://my_server/HPBAC

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

2

Navigating HP Business Availability Center

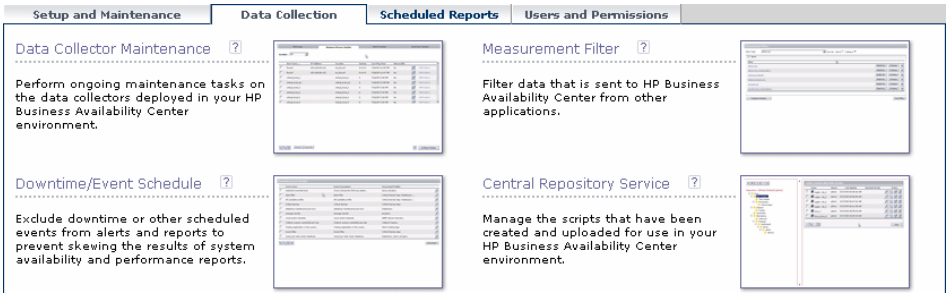
This chapter provides details on how to navigate HP Business Availability Center.

Navigating the HP Business Availability Center User Interface

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

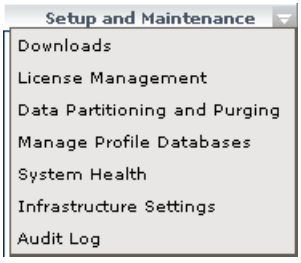
- **Site Map.** Enables quick access to all top-level contexts in the Applications menu or the Administration Console. The site map is the first page that opens, by default, after logging into HP Business Availability Center. If the default page is changed after login, you can access the site map by clicking the Site Map link, either in the top menu or from the Help menu.
- **Top menu bar.** Enables navigation to the applications, Administration Console pages, and help resources. The top menu bar also includes a link to the site map and the **Logout** button.

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



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

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



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

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

Menus and Options

The top menu bar enables navigation to the following applications and resources:

Business User Applications

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

Menu Option	Description
My BAC	Select to open the My BAC application, a portal that individual users can customize to display key content relevant to them. For details, see *Using My BAC*.
Dashboard	Select to open the Dashboard application, a real-time dashboard for viewing performance and availability metrics from a business perspective. For details, see *Using Dashboard*.

Menu Option	Description
Service Level Management	Select to open the Service Level Management application to proactively manage service levels from a business perspective. Service Level Management provides IT Operations teams and service providers with a tool to manage service levels and provide service level agreement (SLA) compliance reporting for complex business applications in distributed environments. For details, see *Using Service Level Management*.
End User Management	Select to open the End User Management application, used to monitor applications from the end user perspective and analyze the most probable cause of performance issues. For details, see *Using End User Management*.
Diagnostics	Select to open the HP Diagnostics application (if a licensed version of HP Diagnostics is installed), to gain end-to-end visibility and comprehensive diagnostics for Java 2 Enterprise Edition (J2EE), .NET-connected, Siebel, SAP, Oracle, and other complex environments. For details, see the HP Diagnostics documentation accessed from the Help menu in HP Business Availability Center.
Problem Isolation	Select to open the Problem Isolation application, used for triaging and isolating problems identified by HP Business Availability Center. For details, see *Using Problem Isolation*.
System Availability Management	Select to open the System Availability Management application, used for complete system and infrastructure monitoring as well as event management. For details, see *Using System Availability Management*.
Alerts	Select to open the Alerts application to view CI Status Alert, SLA Alert, and Event-Based Alert reports. For details, see *Custom Reporting and Alerting*.

Menu Option	Description
Universal CMDB	Select to open the Universal CMDB application, used to view the CIs of the currently selected view in graphical format, to compare CIs and views, to view reports about changes that are occurring in the CMDB, and to view breakdown reports. For details, see *IT World Model Management*.
HP Business Availability Center for Siebel Applications	Select to open HP Business Availability Center for Siebel Applications diagnostics tools. For details, see *Solutions and Integrations*.
HP Business Availability Center for SOA	Select to open HP Business Availability Center for SOA reports. For details, see *Solutions and Integrations*.
Application Performance Lifecycle	Select to open the Application Performance Lifecycle application, used to assist in constructing load tests based on real-user transaction data collected by the Real User Monitor. For details, see *Solutions and Integrations*

Administration Console

Administrators use the Administration Console to administer the HP Business Availability Center platform and applications. The Administration Console consists of several sections, organized by function. You access each functional area from the Admin menu. You select from the following menu options:

Menu Option	Description
My BAC	Select to open the My BAC Administration pages, where you manage portal modules (including portlets), and set viewing permissions. For details, see *Using My BAC*.

Menu Option	Description
Dashboard	Select to open the Dashboard Administration pages, where you attach Key Performance Indicators (KPIs) to CIs, define the custom and geographical maps, and customize the repositories. For details, see *Using Dashboard*.
Service Level Management	Select to open the Service Level Management Administration pages, where you create service level agreements (SLAs) and build services that link to the data that Service Level Management collects. For details, see *Using Service Level Management*.
End User Management	Select to open the End User Management Administration pages, where you configure and administer Business Process Monitor and Real User Monitor data collectors, as well as configure transaction order, color settings, and report filters. For details, see *Using End User Management*.
Diagnostics	Select to open the HP Diagnostics configuration page, where licensed HP Diagnostics users connect to an installed Diagnostics server and configure HP Diagnostics. For details, refer to the HP Diagnostics documentation installed with the product.
Problem Isolation	Select to open the Problem Isolation Administration pages, where you configure on-demand monitors and problem suspects. For details, see *Using Problem Isolation*.
System Availability Management	Select to open the System Availability Management Administration pages, where you configure and administer the SiteScope data collector. For details, see *Using System Availability Management*.
Alerts	Select to open the Alerts Administration pages, where you configure alerts and system recipients. For details, see *Custom Reporting and Alerting*.

Menu Option	Description
Universal CMDB	Select to open the Universal CMDB Administration pages, where you build and manage a model of your IT universe in the CMDB. From Universal CMDB Administration, you manage the Discovery process and the adapter sources that are used to populate the IT Universe model with configuration items (CIs), the templates for creating CIs, and the viewing system for viewing the CIs in HP Business Availability Center applications. You can also manually create CIs to add to the model. For details, see *IT World Model Management*.
Platform	Select to open the Platform Administration pages, which provide complete platform administration and configuration functionality.
EMS Integrations	Select to open the EMS Integrations application, where you access out-of-the-box integrations and customize the Integration Monitor configuration files to correctly map the data Integration Monitors collect to a format recognizable by HP Business Availability Center.
Link to this page	Select to access the **Link to this page** feature, where you can create a URL that enables direct access to a specific page in HP Business Availability Center. For details, see "Using the Link to This Page Option (Direct Login) to Open a Specific Page".
Personal Settings	Select to access the Personal Settings tab, which enables personalization of various aspects of HP Business Availability Center, including menus and passwords. Note that Personal Settings are available to all users.

Help Menu

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

- **Help on this page.** Opens the Documentation Library to the topic that describes the current page or context.
- **Documentation Library.** Opens the Documentation Library home page. The home page provides quick links to the main help topics.
- **Diagnostics Help.** Opens the HP Diagnostics Help, if an HP Diagnostics server is connected to HP Business Availability Center.
- **Troubleshooting & Knowledge Base.** Opens the Customer Support Web Site directly to the Knowledge Base landing page. The URL for this Web site is http://support.mercury.com/cgi-bin/portal/CSO/kbBrowse.jsp.
- **Customer Support Web Site.** opens the Customer Support Web Site. This site enables you to browse the knowledge base and add your own articles, post to and search user discussion forums, submit support requests, download patches and updated documentation, and more. The URL for this Web site is http://support.mercury.com.
- **HP Software Web Site.** Opens the HP Software Web site, which contains information and resources about HP Software products and services. The URL for this Web site is http://www.hp.com/managementsoftware.
- **Site Map.** Opens the site map, which enables quick access to all top-level contexts in the Applications menu or the Administration Console.
- **What's New?** Opens the What's New document, which describes the new features and enhancements of the version.
- **About HP Business Availability Center.** Opens the About HP Business Availability Center dialog box, which provides version, license, patch, and third-party notice information.

Working with the HP Business Availability Center Documentation Library

The sections below describe how to navigate and use the HP Business Availability Center Documentation Library.

Navigating the Documentation Library

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

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

  The home page is divided into the following tabs:

  - **Main Topics tab.** Organizes the various guides contained in the Documentation Library into logical sections.
  - **Get Started tab.** Provides a checklist of major steps required to get up and running with HP Business Availability Center, and links to details for each step.
  - **PDFs tab**. Organized similar to the Main Topics tab, but provides links to the guides in PDF format.

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

  The navigation pane is divided into the following tabs:

  - **Contents tab.** The Contents tab organizes the various guides in a hierarchical tree, enabling direct navigation to a specific guide or topic.
  - **Index tab.** The Index tab enables you to select a specific topic to display. Double-click the index entry to display the corresponding page. If your selection occurs in multiple documents, a dialog box is displayed enabling you to select a context.

- **Search tab.** The Search tab enables you to search for specific topics or keywords. Results are returned in ranked order.
- **Favorites tab.** The Favorites tab enables bookmarking specific pages for quick reference. Note that the Favorites tab is only available when using the Java implementation of the Documentation Library. If your browser does not support Java, the JavaScript implementation is automatically used and the Favorites tab is not displayed.

Documentation Library Functionality

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

- **Show Navigation button.** Click to display the navigation pane, which includes the Contents, Index, Search, and Favorites tabs. For details on the Navigation pane, see "Working with the HP Business Availability Center Documentation Library" on page 39. Note that this button is only displayed when the navigation pane is closed.

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

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

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

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

Part II

Setup and Maintenance

3

Downloads and Licenses

Once the servers for HP Business Availability Center are installed, there are several components that must be downloaded. These components include tools for monitoring your enterprise and recording business processes. HP Business Availability Center also includes a flexible licensing feature enabling you to update your own license information.

Downloads

You download components from the Downloads page, accessed from the Setup and Maintenance tab in Platform Administration. To view and download components from the Downloads page, after installing HP Business Availability Center, you must install the data collector setup file. For details, see "Installing Component Setup Files" in *the HP Business Availability Center Deployment Guide* PDF.

Note: If there is a component you want to download that does not appear on the Downloads page because it was not selected during data collector setup file installation, you can add it to the Downloads page at any time using the procedures described in "Installing Component Setup Files" in the *HP Business Availability Center Deployment Guide* PDF.

Depending on your operating system and on the options selected during data collector setup file installation, any of the following components may be available for download:

- HP Business Process Monitor for Windows 2000/2003/XP
- HP Business Process Monitor for Solaris
- Discovery Probe for Windows 2000/2003/XP
- SiteScope for Windows 2000/2003
- SiteScope for Linux
- SiteScope for Solaris
- HP Virtual User Generator
- Microsoft .NET framework 2.0
- Web Services Enhancements (WSE) 3.0 for Microsoft .NET
- Microsoft Visual C++ 2005
- Microsoft XML core services (MSXML) 6
- HP Real User Monitor Engine for Windows
- HP Real User Monitor Probe
- HP Dashboard Ticker

To download and install a component:

1. Select **Setup and Maintenance** > **Downloads** from the Platform Administration page in the Administration Console. The Downloads page opens.
2. Click the component you want to download.
3. Save the component's setup file to your computer.
4. To install the component, double-click its setup file.
   - For details on installing HP Business Process Monitor for Windows 2000/2003/XP, or Solaris, see "About Business Process Monitor Deployment" in the *Business Process Monitor Administration* PDF.
   - For details on installing the Discovery probe, see "Installing the Discovery Probe" in *Discovery*.

- For details on installing HP SiteScope for Windows 2000/2003, Linux, or Solaris, see "Introduction to SiteScope" in the *HP SiteScope Deployment Guide* PDF.
- For details on installing HP Virtual User Generator, start the installation process and follow the on-screen instructions.
- For details on installing HP Real User Monitor Engine, see "Installing the HP Real User Monitor Engine" in the *Real User Monitor Administration* PDF.
- For details on installing HP Real User Monitor Probes, see "Installing the HP Real User Monitor Probe" in the *Real User Monitor Administration* PDF.
- For details on installing HP Dashboard Ticker start the installation process and follow the on-screen instructions (for details, see "Dashboard Ticker" in *Using Dashboard*).

License Management

Note to HP Managed Software Solutions customers: HP Operations administers these pages and the interface is hidden from your view.

To run monitors and transactions, as well as use various integral applications in HP Business Availability Center, you must have a valid license key.

The HP Business Availability Center license enables you to simultaneously run a predetermined number of monitors and transactions for a specified period of time. The number of monitors and transactions that you can run simultaneously, the specific applications that you can run, and the license key expiration date, all depend on the license your organization has purchased from HP. You enter the license key during the installation process.

You can review the status of your maintenance number and license key by selecting **Help** > **About HP Business Availability Center**. The About HP Business Availability Center dialog box opens and displays your current license information.

A number of HP Business Availability Center applications require additional licensing. In order to use these applications, you must obtain an updated license key from HP and then update the license key in HP Business Availability Center. For more information on updating your license key and maintenance number, see "Updating License Key and Maintenance Number" on page 48.

Note: HP Business Availability Center posts a license expiration reminder on the login page of the Web site seven days before license expiration.

Viewing Current License Information

In Platform Administration, select **Setup and Maintenance** > **License Management** to open the License Management page.

The following information is displayed:

- General License Properties area including:
  - current license key
  - license host ID
  - current maintenance number
  - license type
  - license expiration date
- Business Process Monitor area including:
  - maximum number of transactions allowed to run simultaneously under the current license key
  - number of transactions currently running in all profiles
  - total number of transactions currently in the database

- Scripts Assignments area including:
  - maximum number of scripts allowed to run simultaneously under the current license key
  - number of scripts assignments currently running in all profiles
  - total number of scripts assignments currently in the database
- Applications area including:
  - validity of Dashboard license
  - validity of Service Level Management license
  - validity of End User Management license
  - validity of Real User Monitor license
  - validity of System Availability Management license
  - validity of Business Availability Center for Siebel Applications Applications license
  - validity of Diagnostics license
  - validity of Business Availability Center for Citrix license
  - validity of Business Availability Center for SAP Applications license
  - validity of Automatic Discovery license
  - validity of Business Availability Center for SOA license
  - validity of Problem Isolation license
  - validity of Application Performance Lifecycle license

Updating License Key and Maintenance Number

When installing or upgrading HP Business Availability Center, you may need to enter your license key or maintenance number.

To update your license key or maintenance number in Windows:

1 In Platform Administration, select **Setup and Maintenance** > **License Management** to open the License Management page.

2 Click **New Maintenance Number** or **New License Key**. The relevant dialog box opens.

3 Type the new or updated number for the license key or the maintenance number in the appropriate box.

4 Click **OK**.

To update your license key or maintenance number in Solaris:

Note: Do not use Platform Administration to install the initial license key and maintenance number. They are installed during the installation process.

---

1. Log in to Solaris as user **root**.
2. Go to directory <**HP Business Availability Center root directory**>/**scripts**.
3. Run the script **create_license.sh** with the parameters <**Management database user name**> <**Management database password**> <**database tns name**>. For example:

```
./create_license.sh TopazMng11 topaz spenser
```

4

Database Administration

You can maintain and administer the databases HP Business Availability Center uses to store profile and monitoring data.You can create and manage profile databases directly from the Platform Administration. You can also enable the Partition and Purging Manager to purge the data in the database periodically according to your organization's needs.

Database Management

Note to HP Managed Software Solutions customers: HP Operations administers these pages and the interface is hidden from your view.

Before you create profiles, you must configure the database into which you want profile data saved. A profile database can store data for multiple profiles, as well as from any type of profile (Business Process Monitor, SiteScope). You can either create one database for all profile data or create dedicated databases (for example, for each profile type).

Note: The term **database** is used to refer to a database in MS SQL Server. The term **user schema** refers to a database in Oracle Server.

HP Business Availability Center supports two database types:

- **Microsoft SQL Server.** This database runs on Windows operating systems only – for details, see page 54.
- **Oracle Server.** This database runs on Windows or Solaris operating systems – for details, see page 58.

The Profile Database Management page, accessed from **Admin** > **Platform** > **Setup and Maintenance**, enables you to perform the following database management tasks:

- **Create a new database.** HP Business Availability Center automatically creates a new database and populates it with profile tables.
- **Assign a default profile database**. You must assign a default profile database, to enable HP Business Availability Center to collect the following types of data:
  - Service Level Management data
  - SOA data
  - data from Real User Monitor
  - data used in Dashboard
  - HP Diagnostics data
  - persistent custom data
- **Add profile tables to an existing, empty database.** HP Business Availability Center connects to an empty database that was manually created on your database server, and populates it with profile tables.
- **Connect to an existing database populated with profile tables.** HP Business Availability Center connects to a profile database that was either manually created and populated with profile tables, or previously defined in Platform Administration.

  To deploy profile databases on MS SQL Server or Oracle Server for your organization's particular environment, follow the instructions in "Databases Used in HP Business Availability Center" in *the HP Business Availability Center Database Guide* PDF. It is recommended that you review the relevant portions of *the HP Business Availability Center Database Guide* PDF before performing profile database management tasks.

Configuring a Profile Database on MS SQL Server

You configure one or more profile databases on your MS SQL Server. Before you begin, make sure that you have the following connection parameters to the database server:

- **Server name.** The name of the machine on which MS SQL Server is installed.
- **Database user name and password.** The user name and password of a user with administrative rights on MS SQL Server (if using SQL server authentication).
- **Server port.** The MS SQL Server's TCP/IP port. The default port, 1433, is automatically displayed.

  If required, consult with your organization's DBA to obtain this information.

Note: It is recommended that you configure MS SQL Server databases manually, and then connect to them in the Database Management page. For details on manually configuring MS SQL Server databases, see "Overview of Microsoft SQL Server Deployment" in *the HP Business Availability Center Database Guide* PDF.

To configure a new or existing profile database on MS SQL Server:

1. In Platform Administration, select **Setup and Maintenance** > **Manage Profile Databases**. The Database Management page opens.
2. In the dropdown database list on the right side of the screen, select **MS SQL**, and click **Add**.

   The Profile Database Properties - MS SQL Server page opens.
3. Select or clear the **Create database and/or tables** check box as required:
   - To create a new database, or connect to an existing, empty database and populate it with profile tables, select the check box.
   - To connect to an existing database already populated with profile tables, clear the check box.

4 Select or clear the **Make this my default profile database (required for custom data types)** check box as required.

This setting is required if you are collecting Dashboard, Real User Monitor, HP Diagnostics (if installed), Service Level Management, SOA, or persistent custom data. For details about custom data, see "Working with Measurement Filters" on page 233.

Important: There can be only one default profile database. Selecting this check box overwrites the existing default profile database (if there is one) and makes it a regular profile database.

---

5 In the **Server name** box, type the name of the machine on which the MS SQL Server is installed.

6 In the **Database name** box, type:

- a descriptive name for the database, if you are configuring a new database
- the name of the existing database, if you are connecting to a database that was previously created

7 If the MS SQL Server's TCP/IP port is configured to work on a different port from the default port (1433), enter it in the **Port** box.

8 In the **Connect Using** section, select the type of authentication the MS SQL server is using:

- **Windows authentication.** The user name and password that runs the HP Business Availability Center service on the current machine is used.
- **SQL server authentication.** In the **User name** and **User password** boxes, type the user name and password of a user with administrative rights on MS SQL Server.

9 Click **Apply**. HP Business Availability Center configures or connects to the database, as instructed, adds it to the database table on the Database Management page, and displays the message: Operation Successful.

Important: Database creation can take several minutes.

---

10 To configure additional profile databases on the MS SQL Server, repeat steps 2 on page 54 through 9 on page 56.

Managing Profile Databases on MS SQL Server

You perform the following tasks, as required, to manage the profile databases configured on your MS SQL Server:

- **Edit database connection parameters.** You can change the type of authentication used, modify the user name and password that is used to connect to profile database on MS SQL Server (for SQL server authentication), if those parameters are changed on the database server, and change the port number used for connecting to the MS SQL Server machine.For details, see below.
- **Remove database connection.** You can disconnect a profile database from the HP Business Availability Center system. For details, see page 58.

Note: Disconnecting a database removes its reference from the Management database, but does not physically remove the database from the MS SQL Server machine. To delete a database from your MS SQL Server machine, follow the instructions provided in your MS SQL Server documentation.

To edit database properties:

1 On the Database Management page, click the **Edit Database Properties** button beside the MS SQL Server database whose properties you want to edit. The Profile Database Properties - MS SQL Server page opens.

2 Select or clear the **Make this my default profile database (required for custom data types)** check box as required.

This setting is required if you are collecting Dashboard data, Real User Monitor, HP Diagnostics (if installed), Service Level Management data, SOA data, or persistent custom data. For details about custom data, see "Working with Measurement Filters" on page 233.

Important: There can be only one default profile database. If a default profile database already exists, selecting this check box overwrites the existing database.

---

3 Change the type of authentication as required.

4 Modify the user name and password as required.

The existing password appears as a series of asterisks. To edit this field, highlight the current password value and enter the new value.

5 Change the port number as required.

6 Click **Apply** to save the settings and return to the Database Management page.

Click **Cancel** to return to the Database Management page without saving any changes.

To disconnect a database from the HP Business Availability Center system:

1 On the Database Management page, click the **Disconnect Database** button beside the MS SQL Server database that you want to disconnect. The Profile Database Properties - MS SQL Server page opens.

2 Click **Disconnect**. The database is disconnected and removed from the table on the Database Management page.

Click **Cancel** to return to the Database Management page without disconnecting the database.

Creating a User Schema on Oracle Server

You configure one or more profile user schemas on your Oracle Server. Before you begin, ensure that:

- You have created a dedicated default tablespace for profile user schemas (and a dedicated temporary tablespace, if required).
- You are using a secure network connection if you do not want to submit database administrator connection parameters over a non-secure connection. If you do not want to submit database administrator connection parameters via your Web browser at all, you can manually create profile user schemas and then connect to them from the Database Management page.

In addition, before you begin, make sure that you have the following connection parameters to the database server:

- **Host name.** The name of the machine on which the Oracle Server is installed.
- **SID.** The Oracle instance name that uniquely identifies the instance of the Oracle database being used, if different from the default value, **orcl**.
- **Port.** The Oracle listener port, if different from the default value, **1521**.
- **Database administrator user name and password.** The name and password of a user with administrative permissions on the Oracle Server. These parameters are used to create the HP Business Availability Center user, and are not stored in the system.

- **Default tablespace.** The name of the dedicated default tablespace you created for profile user schemas (for details on creating a dedicated tablespace, see "Overview of Oracle Server Deployment" in *the HP Business Availability Center Database Guide* PDF). If you did not create, and do not require, a dedicated default tablespace, specify an alternate tablespace. The default Oracle tablespace is called **users**.
- **Temporary tablespace.** The name of the dedicated temporary tablespace you created for profile user schemas. If you did not create, and do not require, a dedicated temporary tablespace, specify an alternate tablespace. The default Oracle temporary tablespace is called **temp**.
- **TNS name.** The TNS name of the Oracle Client, as specified in the **tnsnames.ora** file on the Gateway Server machine, located in the **<ORACLE_HOME>\network\admin** directory.

  If required, consult with your organization's database administrator to obtain this information.

Note: It is recommended that you configure Oracle Server user schemas manually, and then connect to them in the Database Management page. For details on manually configuring Oracle Server user schemas, see "Overview of Oracle Server Deployment" in *the HP Business Availability Center Database Guide* PDF.

To configure a profile user schema on Oracle Server:

1. In Platform Administration, select **Setup and Maintenance** > **Database Management**. The Database Management page opens.
2. In the database type list, select **Oracle**, and click **Add**.

   The Profile User Schema Properties - Oracle Server page opens.

3 Select or clear the **Create database and/or tables** check box as required:

- To create a new user schema, or connect to an existing, empty user schema, and populate it with profile tables, select the check box.
- To connect to an existing user schema already populated with profile tables, clear the check box.

Note: Clearing the **Create database and/or tables** check box disables the database administrator connection parameter, tablespace, and TNS name fields on the page, and instructs the platform to ignore the information in these fields when connecting to the Oracle Server machine.

---

4 Select or clear the **Make this my default profile database (required for custom data types)** check box as required.

This setting is required if you are collecting Dashboard data, Real User Monitor, HP Diagnostics (if installed), Service Level Management data, SOA data, or persistent custom data. For details about custom data, see "Working with Measurement Filters" on page 233.

Important: There can be only one default profile database. If a default profile database already exists, selecting this check box overwrites the existing database.

---

5 In the **Host name** box, enter the name of the machine on which Oracle Server is installed.

6 In the **SID** box, enter the required Oracle instance name, or accept the default value.

7 In the **Port** box, enter the required Oracle listener port, or accept the default value.

8 In the **New user schema name** box, enter:

- a descriptive name for the user schema, if you are configuring a new user schema
- the name of the existing user schema, if you are connecting to a user schema that was previously created

---

Note: You must specify a unique user schema name for each user schema you create for HP Business Availability Center on Oracle Server.

---

9 In the **TNS name** box, type the TNS name of the Oracle Client, as specified in the tnsnames.ora file on the Gateway Server machine, located in the **<ORACLE_HOME>\network\admin** directory.

10 In the **New user schema password** box, enter:

- a password that enables access to the user schema, if you are configuring a new user schema
- the password of the existing user schema, if you are connecting to a user schema that was previously created

11 In the **Retype password** box, retype the user schema password that you just entered in the previous step.

12 If you cleared the **Create database and/or tables** check box in step 3 on page 60, skip to step 16 on page 62.

If you selected the **Create database and/or tables** check box in step 3 on page 60, continue with step 13 on page 61.

13 In the **Database administrator username** and **Database administrator password** boxes, enter the name and password of a user with administrative permissions on Oracle Server.

14 In the **Default tablespace** box, type the name of the default tablespace designated for use with profile user schemas, if different from the default value, **users**.

15 In the **Temporary tablespace** box, type the name of the temporary tablespace designated for use with profile user schemas, if different from the default value, **temp**.

16 Click **Apply**. HP Business Availability Center configures or connects to the user schema, as instructed, adds it to the database table on the Database Management page, and displays the message: Operation Succeeded.

Note: User schema creation can take several minutes. The browser might time out before the creation process is completed. However, the creation process continues on the server side.

If a timeout occurs before you get a confirmation message, you can verify that the user schema was successfully created by checking that the user schema name appears in the database list on the Database Management page.

---

17 To configure additional profile user schemas on Oracle Server, repeat steps 2 on page 59 through 16 on page 62.

Managing Profile User Schemas on Oracle Server

You perform the following tasks, as required, to manage the profile user schemas configured on your Oracle Server:

- **Edit database connection parameters.** You can modify the password that HP Business Availability Center uses to connect to the profile user schema on Oracle Server, and change the port number used to connect to the Oracle Server machine. For details, see page 63.
- **Remove database connections.** You can disconnect a profile user schema from the system. For details, see page 63.

Note: Disconnecting a user schema removes its reference from the management database, but does not physically remove the user schema from the Oracle Server machine. To delete a user schema from your Oracle Server machine, follow the instructions provided in your Oracle Server documentation.

To edit user schema properties:

1 On the Database Management page, click the **Edit Database Properties** button beside the Oracle Server user schema whose properties you want to edit. The Profile User Schema Properties - Oracle Server page opens.

2 Select or clear the **Make this my default profile database (required for custom data types)** check box as required:

This setting is required if you are collecting Dashboard data, Real User Monitor, HP Diagnostics (if installed), Service Level Management data, SOA data, or persistent custom data. For details about custom data, see "Working with Measurement Filters" on page 233. There can be only one default profile database. If a default profile database already exists, selecting this check box overwrites the existing database.

3 Modify the user schema password as required.

The existing password appears as a series of asterisks. To edit this field, highlight the current password value and enter the new value.

4 Change the port number as required.

5 Click **Apply** to save the settings and return to the Database Management page.

Click **Cancel** to return to the Database Management page without saving any changes.

To disconnect a user schema from HP Business Availability Center:

1 On the Database Management page, click the **Disconnect Database** button beside the Oracle Server user schema that you want to disconnect. The Profile User Schema Properties - Oracle Server page opens.

2 Click **Disconnect**. HP Business Availability Center disconnects the user schema and removes it from the table on the Database Management page.

Click **Cancel** to return to the Database Management page without disconnecting the database.

Partitioning and Purging Historical Data from Profile Databases

---

Note to HP Managed Software Solutions customers: HP Operations administers these pages and the interface is hidden from your view.

The data collection tables in the profile databases can grow to a very large size. Over time, this can severely degrade system performance.

HP Business Availability Center's Partition and Purging Manager splits fast-growing tables into partitions at defined time intervals. After a defined amount of time has elapsed, data in a partition is made inaccessible for use in HP Business Availability Center reports. After an additional defined amount of time, a partition is purged from the profile database.

You use the Partition and Purging Manager to instruct the platform to automatically partition historical data for later removal from profile databases.

Important: HP strongly recommends that you enable the Partition and Purging Manager.

The Partition and Purging Manager can be used with profile databases located on the following database servers:

- **Oracle.** Any Oracle Server version supported by HP Business Availability Center
- **MS SQL.**
  - MS SQL Server 2000 Standard edition
  - MS SQL Server 2000 Enterprise editions (MS SQL Server 7.0 and MSDE are not supported)
  - MS SQL Server 2005 Enterprise edition

For details on advanced partitioning and purging capabilities, see "Data Partitioning and Purging" in the *HP Business Availability Center Database Guide* PDF.

Once enabled, the Partition and Purging Manager partitions and later removes data according to the time period listed for the database table. The size of each partition is determined by the EPM (events per minute) that you configured. These time periods specify how long the data is saved in the profile database table. After the time period set for each table, the Partition and Purging Manager removes data that has been aggregated.

HP Business Availability Center includes default time periods for keeping the data in each database table. You can also use the Partition and Purging Manager to set a specific time period—per table—for removing data.

If you do not modify the default time period and the Partition and Purging Manager is enabled, data is removed according to the default range listed for each table.

This section covers the following topics:

Enabling and Disabling the Partition and Purging Manager

By default, the Partition and Purging Manager is disabled. You can enable the Partition and Purging Manager to instruct HP Business Availability Center to begin the process of partitioning the data. Once enabled, the Partition and Purging Manager runs every hour to check if a new data partition needs to be created. The Partition and Purging Manager removes data only after the data has been aggregated.

Note: When working with an Oracle database, it is strongly recommended that you set **PARTITION_VIEW_ENABLED** parameter in the **init.ora** file to **true**. For details on purging data from an Oracle database, see "About Data Partitioning and Purging" in the *HP Business Availability Center Database Guide* PDF.

To enable the Partition and Purging Manager:

1. Select **Admin** > **Platform** > **Setup and Maintenance** > **Data Partitioning and Purging**. The Partition and Purging Manager page opens.
2. Click **Enable** to enable the Partition and Purging Manager.

To disable the Partition and Purging Manager:

1. Select **Admin** > **Platform** > **Setup and Maintenance** > **Data Partitioning and Purging**. The Partition and Purging Manager page opens.
2. Click **Disable** to disable the Partition and Purging Manager.

Modifying the Default Time Range Configurations

If required, you can modify the default time range configurations per table. You can make those modifications to the database tables globally, for all profile databases, or per profile database.

To modify the Partition and Purging Manager settings:

1. In Platform Administration, select **Setup and Maintenance** > **Data Partitioning and Purging**. The Enable/Disable Purging Manager page opens.
2. Select whether you want your changes to affect the selected table in all the profile databases in your platform (globally), or per individual profile database.
   - ➤ To change the time range for purging data in a table for all profile databases, select the **Global Settings** tab.
   - ➤ To change the time range for purging data in a table per profile database, select the **Database-Specific Settings** tab and select the profile database from the drop-down list at the top of the section.

Note: Once you modify tables for a specific profile (under the Database-Specific Settings tab), any changes made globally (under the Global Settings tab) do not affect the tables for that profile. Any additional changes to purging settings for that database must be made from the Database-Specific Settings tab.

It is recommended that you select the Global Settings tab unless there is a table in a specific profile database for which you must configure a different purging time period.

---

3 Select the check box next to all the database tables for which you want to change the purging time range to the same time period.

All database tables are listed by the data collector from which the data was gathered. There is also a table for Service Level Management data that is not considered raw data.

Choose from the following data types:

- Business Logic Engine
- Business Process Monitor
- Diagnostics
- Real User Monitor
- SOA (Service Oriented Architecture)
- Service Level Management
- SiteScope
- UDX (custom data)
- WebTrace

4 Set the new time range for keeping data in the selected database tables by selecting the number and the time unit in the appropriate **Keep Data for** boxes.

Note: The time range configured in the **Keep Data for** boxes indicates that the data is stored for **at least** the specified amount of time - it does not indicate when the data is purged.

---

5 Enter the Events per minute for the selected data type in the **EPM** box. The EPM number represents the amount of data per minute that is arriving in HP Business Availability Center. This number is determined via the following procedure:

➤ Open the file located at:

<Gateway Server root directory>\log\mercury_db_loader\LoaderStatistics.log

➤ Locate the line in the select data sample that reads:

Statistics for: DB Summary:<database name>Sample:<sample name> - (collected over <time period>):

➤ Locate the line in the statistics section of the data sample that reads:

Insert to DB EPS (MainFlow)

The selected number represents the events per second. Multiply this number by 60 to retrieve the events per minute.

6 Click **Apply**.

7 Repeat steps 3 on page 68 through 6 on page 69 for additional time periods you want to set, selecting the database tables that are purged for that time period.

Configuration changes automatically take effect at the beginning of the next Partition and Purging Manager cycle.

Guidelines and Tips for Using the Partition and Purging Manager

➤ Prior to purging, the Partition and Purging Manager performs an additional check to ensure that raw data is not purged before it has been aggregated and reported to HP Business Availability Center.

If a particular profile database's data is scheduled for purging but its raw data has not yet been aggregated, the Partition and Purging Manager does not purge the data according to its schedule. The Partition and Purging Manager automatically purges the data on its next hourly run only after the data has been aggregated.

For example, if data was scheduled to be purged on Sunday at 8:00 but its data is only aggregated on Sunday at 10:00, the Partition and Purging Manager checks the data at 8:00, does not purge the data, and automatically purges the data on its next hourly run only after Sunday at 10:00 once the data has been aggregated.

- If you find that data is not being purged according to the schedules set in the Partition and Purging Manager and your profile databases are growing too large, check that the aggregator is running properly and view the Partition and Purging Manager logs located in **<HP Business Availability Center server root directory>/log/pmanager.log**.

  HP Business Availability Center displays raw data only in the following contexts: SiteScope Warning Summary and SiteScope Error Summary reports, transaction breakdown data used in trend reports, Service Level Management reports, Real User Monitor Reports, and Excel Reports that use raw data.

  Because aggregated data is not used in these reports, if the raw data for a specific time period has been removed from the profile database using the Partition and Purging Manager, those reports do not contain any data when generated for that time period.

- The default configuration uses the following principle: the length of time that raw data is kept is shorter than the length of time that one-hour chunks of aggregated data are kept, which is shorter than the length of time that one-day chunks of aggregated data are kept.

- Any changes made under the Global Setting tab affect the default time periods for new profile databases created in the system. If a new profile database is created after you have made modifications to the time periods under the Global Settings tab, data is kept in the tables of that new profile database for the time periods now listed under Global Settings for all tables.

Removing Unwanted Data from the Profile Database

Note to HP Managed Software Solutions customers: This section is not relevant to HP Managed Software Solutions customers.

The Data Marking utility enables HP Business Availability Center users with superuser security privileges to mark specific sets of data in profile databases as unwanted. While the utility does not physically remove marked data from the database, it renders it unusable in reports and applications by assigning the marked data a status of **unavailable** in the database. During installation, HP Business Availability Center installs the Data Marking utility on the Gateway Server.

After you mark a specific set of data from a given time period as unwanted, HP Business Availability Center reruns the aggregation process on remaining raw data for the relevant time period so that reports using aggregated data display only the relevant data. The Data Marking utility also enables you to re-aggregate a defined set of data without marking it as unavailable. For details, see "Enabling the Re-aggregation-Only Option" on page 75.

Currently, the Data Marking utility enables removal of unwanted Business Process Monitor and SiteScope data.

The Data Marking utility supports partitions. Thus, users running the Partition and Purging Manager can also use the Data Marking utility.

This section covers the following topics:

Working with the Data Marking Utility

The Data Marking utility enables you to select sets of data for removal by profile or by location for Business Process Monitor data, and by SiteScope target machine for SiteScope data.

- Business Process Monitor data:
  - **Profile view.** In the Profile view, you select a Business Process Monitor profile and then one or more transactions or locations for which you want to mark data for removal.

    This view is helpful if you want to remove data collected for specific transactions, such as transactions that ran during unexpected system downtime.
  - **Location view.** In the Location view, you select a location and then one or more Business Process Monitor profiles for which you want to mark data for removal.

    This view is helpful if you want to remove data collected from a specific location, such as a location at which the installed Business Process Monitor machine was experiencing technical problems for a period of time.
- SiteScope data:
  - **SiteScope view.** In SiteScope view, you select a SiteScope target machine for which you want to mark data for removal. The SiteScope target is the machine which the SiteScope is monitoring. The SiteScope target list includes all machines being monitored by all the SiteScopes for which profiles are running within your HP Business Availability Center platform. The target machine is listed with the name of the profile running the SiteScope in parentheses. If a target machine is monitored by more than one SiteScope, then the target machine is listed more than once with the different profile names in parentheses.

After selecting the above criteria, you specify a time range over which to mark data as unwanted.

Before executing the data marking run, you can review the number of data rows that will be affected using the **Get Info** button. After a data marking run is completed, use the **Get Info** button after a run to view the number of data rows still unmarked within the selected time period and filter criteria.

After the utility marks the specified data as unavailable, HP Business Availability Center automatically re-aggregates the remaining raw data for the selected time period.

To mark data as unwanted:

1. On the Gateway Server, double-click the **<HP Business Availability Center Gateway Server root directory>\tools\dataMarking\dataMarking.bat** file. A Command Prompt window opens, followed by the Data Marking utility login dialog box.
2. Enter the user name and password of an HP Business Availability Center user with superuser privileges.
3. Click **OK** to open the main Data Marking utility screen.
4. Select either **Profiles** or **Locations** in the **View by** box.
5. Choose the required filter criteria:
   - In the **Profile View**, select a profile as well as one or more transactions and one or more locations.
   - In the **Location View**, select a location as well as one or more profiles.
   - In the **SiteScope View**, select a target machine.
6. Choose the **Mark data as obsolete** check box.
7. In the **Start Time** section, select a starting date and time.
8. In the **Duration** section, select the period of time, starting from the specified start time, for which the utility will mark data as unavailable. You can set a maximum duration of up to 6 hours and 59 minutes for each data marking run. This value can be customized; for details, see "Customizing Data Marking Utility Configurations" on page 74.
9. Click the **Get Info** button before a run to view the number of data rows to be marked.

   The lower window of the Data Marking Information Window dialog box displays the SLAs affected by the marked data. You can recalculate the affected SLAs on the Agreements Manager tab under **Admin** > **Service Level Management**. For details, see "Working with the Service Level Management Application" on page 125 in Service Level Management.

10 Click **Start**, and confirm that you want to begin. The Data Marking utility starts its run. The utility displays the progress of the data marking and the reaggregation of remaining raw data for the specified time period.

11 When the run is completed, a status message is displayed.

In certain cases, not all data rows defined by the filter criteria may have been marked (for examples of such cases, see "Data Marking Utility Limitations" on page 77). Click the **Get Info** button to view the number of data rows still unmarked within the selected time period and filter criteria. If necessary, rerun the Data Marking utility with the same set of filters to mark the missed rows.

Customizing Data Marking Utility Configurations

You can configure the maximum duration for each data marking run. The current default is 6 hours and 59 minutes.

To configure the maximum duration:

1 Open the <**HP Business Availability Center Gateway Server root directory**>**\tools\dataMarking\dataMarking.bat** file in a text editor.

2 Add the **-DmaximumDuration=xx** property to the command line, where **<xx>** represents the maximum duration in hours.

For example, to change the maximum duration to 23 hours and 59 minutes, replace:

```
% _HOME%\JRE\bin\java -Dtopaz.home=%TOPAZ_HOME% -jar
datamarking.jar
```

with:

```
%TOPAZ_HOME%\JRE\bin\java -Dtopaz.home=%TOPAZ_HOME% -
DmaximumDuration=24 -jar datamarking.jar
```

3 Save and close the file.

Restoring Marked Data

The Data Marking utility also includes an un-mark feature that enables you to reverse the data marking action and clear data that has been marked as unavailable so that the data is made available again. Re-aggregation is automatically initiated once data has been un-marked.

To un-mark data that has been marked as unavailable:

1. Define the set of data you want to make available again, as described in "Working with the Data Marking Utility" on page 72.
2. In step 6 on page 73, choose the **Mark data as valid** check box.
3. Follow the rest of the data marking procedure from step 7 on page 73 through step 11 on page 74.

Enabling the Re-aggregation-Only Option

By default, the Data Marking utility always runs the data marking process, followed by the re-aggregation process. If required, you can enable a feature that allows you to instruct HP Business Availability Center to run only re-aggregation. This might be required if data marking passed successfully but re-aggregation failed. Alternatively, you can use this feature to reaggregate a defined set of data without marking it as unavailable (for example, if data was aggregated and then late-arriving data was inserted into the raw data tables in the database).

To enable the re-aggregation-only option:

1. Open the file **dataMarking.bat** in a text editor.
2. Change the line:

   %TOPAZ_HOME%\JRE\bin\java -Dtopaz.home=%TOPAZ_HOME% -jar datamarking.jar to

   %TOPAZ_HOME%\JRE\bin\java -Dtopaz.home=%TOPAZ_HOME% -DadvancedMode=true -jar datamarking.jar
3. Save the file. The next time you open the Data Marking utility, the **Advanced** button appears.

   After you enable this feature, you can instruct the Data Marking utility to only run the data reaggregation process when clicking the **Start** button.

To run data reaggregation only:

1. Define the set of data you want to reaggregate, as described in "Working with the Data Marking Utility" on page 72.
2. Click the **Advanced** button. The Advanced window opens.
3. Select the **Run reaggregation only** check box.
4. Select the categories of data for the reaggregation and click **OK** to confirm selection.
5. Click **Start**.

Troubleshooting Data Marking Utility Errors

Various types of errors might occur while using the Data Marking utility. Generally, when an error occurs, the utility displays the following error message:

The Data Marking utility must shut down due to an internal error. For details see: <HP Business Availability Center Gateway Server root directory> \log\datamarking.log

Reasons for which the utility might display this error include:

- failure to connect to the database server or profile database
- failure to complete the data marking process, for example, due to communication error between the Aggregation Server and database
- failure of HP Business Availability Center to successfully reaggregate raw data for the defined data set

In case of error, check the **<HP Business Availability Center Gateway Server root directory>\log\datamarking.log** file for error information.

Data Marking Utility Limitations

- The utility does not support the removal of late arriving data.

  For example, if a set of data for a specific time period is marked for removal and HP Business Availability Center later receives data from that time period (which arrived late due to a Business Process Monitor temporarily being unable to connect to the Gateway Server), the late arriving data is not available for use in reports. Use the **Get Info** button to check for late arriving data. If zero rows are not displayed, run the utility again, if required, to remove the data that arrived late.

- The utility does not support removal of data arriving during the data marking process.

  For example, if a set of data for a specific time period is marked for removal, and during that same time period (while the utility is running), data arrives and enters the profile database, the rows of newly arrived data are not marked for removal, and are therefore not removed. In this case, after the utility finishes running, use the **Get Info** button to determine whether all rows of data were removed for the selected time period. If rows are displayed, run the utility again, if required, to remove the data that arrived during the run. This is a rare scenario, as you typically mark data for a previous time period and not for a time period that ends in the future.

- While the utility is running and removing data, reports that are generated for that time period may not show accurate results. As such, it is recommended to run the utility during off-peak hours of HP Business Availability Center usage.

- Do not run more than one instance of the Data Marking utility at one time as this can affect the reaggregation process.

- Do not mark data sets for time periods that include purged data (data that has been removed using the Partition and Purging Manager) as this can affect the reaggregation process.

5

Infrastructure Settings

Note to HP Managed Software Solutions customers: HP Operations administers these pages and the interface is hidden from view, except for the user accessing with superuser permissions.

You can configure HP Business Availability Center settings to meet your organization's specifications for the platform and its applications. You configure most Infrastructure Settings directly within the Administration Console.

Understanding the Infrastructure Settings Manager

HP Business Availability Center enables you to define the value of many settings that determine how HP Business Availability Center and its applications run. For details on settings that are configured directly in files, see "Infrastructure Configurations Not Performed in the Infrastructure Settings Manager" on page 82.

Important: Modifying certain settings can adversely affect the performance of HP Business Availability Center. It is highly recommended not to modify any settings without first consulting Customer Support or your HP Services representative.

In the Infrastructure Settings Manager, you can select different contexts from which to view settings. These contexts are split into two groups:

➤ **Applications**

This list includes those contexts that determine how the various applications running within HP Business Availability Center behave. Contexts such as Dashboard Application, My BAC Application, and Service Level Management are listed.

➤ **Foundations**

This list includes those contexts that determine how the different areas of the HP Business Availability Center foundation run. Contexts such as UCMDB GUI, Connection Pool, and LDAP Authentication, are listed.

Editing Infrastructure Settings

You edit infrastructure settings within the Setup and Maintenance tab of Platform Administration.

To edit an infrastructure setting's value:

1 In Platform Administration, select **Setup and Maintenance** > **Infrastructure Settings.** The Infrastructure Settings Manager page opens.

2 Select the context for viewing the settings or XML format files you want to edit:

- **Applications.** Select if you are editing settings for one of the HP Business Availability Center applications.
- **Foundations.** Select if you are editing settings for one of the HP Business Availability Center foundations.
- **All.** Select to view all the settings for both Applications and Foundations.

3 Locate the setting you want to edit within the relevant context table and click **Edit** next to the current value.

An Edit dialog box opens displaying the setting name, a brief description of the setting, the current value, a range of acceptable values (if there is a range), and any relevant notes (for example, the change takes effect only after restarting HP Business Availability Center).

If the value is **<XML>**, the XML content is seen in its entirety in the Edit dialog box and can be edited there.

4 Edit and save the new value using one of the following options:

- To change the value, edit the value in the value field and click **Save**.

  If there is an acceptable range for the value, the value is checked when you click **Save**. If the entered value is out of range or illegal, you are given an error message and are returned to the dialog box.

- To return the setting's value to the default, click **Restore Default** and then **Save**.
- To return to the dialog box without changing any setting, click **Cancel**.

If the setting's value differs from the default, it is displayed in bold text.

Infrastructure Configurations Not Performed in the Infrastructure Settings Manager

The following infrastructure configuration procedures are not performed in the Infrastructure Settings Manager:

- Disabling Automatic Adjustment of Daylight Savings Time in HP Business Availability Center – for details, see below
- Modifying the Ping Time Interval – for details, see page 84
- Modifying the Location and Expiration of Temporary Image Files – for details, see page 84

Disabling Automatic Adjustment of Daylight Savings Time in HP Business Availability Center

When running HP Business Availability Center servers on Windows NT or Windows 2000 machines, it might be necessary to modify the way the machines and HP Business Availability Center handle the changeover to Daylight Saving Time (DST). It might also be necessary to modify the way DST is handled on the database server machine(s) on which HP Business Availability Center databases are located.

Note: If you are running HP Business Availability Center servers or databases on a Solaris platform, it is not necessary to modify settings.

DST Handling on Server Machines

It might be necessary to disable—on the machines running HP Business Availability Center servers—the operating system setting that automatically adjusts the machine clock for Daylight Saving Time (DST), and instead to manually adjust the machine clock when DST begins. This might be required when HP Business Availability Center servers are located in a geographic region where the exact date that DST begins differs from season to season, in multiple geographic regions whose dates of changeover to DST differ, or in multiple geographic regions of which some do not use DST.

DST Handling on Database Server Machines

It might be necessary to always leave the machine clock on the database server machine(s) on which the databases are located in Standard time (by disabling the operating system setting that automatically adjusts the machine clock for DST, and not adjusting the time manually for DST). This might be required when users are located in multiple geographic regions whose dates of changeover to DST differ from each other and/or that of the region where the database server is located.

If you choose to always leave the machine clock on the database server in Standard time, you must modify a setting in HP Business Availability Center so that HP Business Availability Center and the database server remain synchronized during DST.

To modify DST handling for HP Business Availability Center databases:

1. On the Gateway Server machine, open the file **<Gateway Server root directory>\conf\topaz.config** in a text editor.
2. Search for the line:

   ```
   ## Daylight saving time fix
   ```

3. Delete the comment marker (#) from the line:

   ```
   daylightsaving.database.adapts=true
   ```

4 Save the **topaz.config** file, and restart HP Business Availability Center on the Gateway Server machine.

If, in the future, you re-enable the operating system setting that automatically adjusts the machine clock's time zone for DST, return the comment marker to the above line.

Modifying the Ping Time Interval

You can modify the time interval after which the HP Business Availability Center Web site pings the server to refresh a session.

To modify the ping time interval:

1 Open the file **<Gateway Server root directory>\conf\settings\website.xml** in a text editor.

2 Search for the parameter: **user.session.ping.timeinterval**.

3 Change the value (120, by default) for the ping time interval. Note that this value must be less than half of the value specified for the session timeout period (the previous value defined in the file).

4 Restart HP Business Availability Center on the Gateway Server machine.

If you have multiple Gateway Server machines, repeat this procedure on all the machines.

Modifying the Location and Expiration of Temporary Image Files

When you generate a report in HP Business Availability Center applications, or when HP Business Availability Center automatically generates a report to send via the scheduled report mechanism, images (e.g. - graphs) are created. HP Business Availability Center saves these images, for a limited period of time, in temporary directories on the Gateway Server machine(s) on which the images are generated.

You can modify the following settings related to these images:

- **the path to the directory in which the temporary image files are stored.**

  For details, see "Modifying the Directory in Which Temporary Image Files Are Stored" on page 85.

- **the length of time that HP Business Availability Center keeps temporary image files before removing them.**

  For details, see "Modifying the Length of Time that HP Business Availability Center Keeps Temporary Image Files" on page 91.

- **the directories from which temporary images are removed.**

  You modify temporary image file settings in the **<Gateway Server root directory>\conf\topaz.config** file. For details, see "Specifying the Directories from Which Temporary Image Files Are Removed" on page 95.

Modifying the Directory in Which Temporary Image Files Are Stored

You can modify the path to the directory where HP Business Availability Center stores generated images used in scheduled reports and Analytics. For example, you might want to save generated images to a different disk partition, hard drive, or machine that has a greater storage capacity than the partition/drive/machine on which the Gateway Server machine is installed.

In certain cases, you might be required to modify the path to the directory in which images are stored. For example, if HP Business Availability Center reports are accessing the Gateway Server machine via a virtual IP—typical when there are multiple Gateway Server machines running behind a load balancer in the HP Business Availability Center architecture—since the load balancer could send requests to any of the Gateway Server machines, the image files need to be in a common location that is configured on all the Gateway Server machines and shared among them. For more details, see "Accessing Temp Directory with Multiple Gateway Server Machines" on page 87.

To support a shared location for temporary images in a Windows environment, the following configuration is recommended:

- All Gateway Servers—and the machine on which the shared image directory is defined, if different from the Gateway Servers—should be on the same Windows domain.
- The IIS virtual directory should be configured to use the credentials of an account that is a member of the domain users group.
- The account for the virtual directory should be given read/write permissions on the shared image directory.

Note: If your server configuration requires placing servers on different Windows domain configurations, contact Customer Support.

To support a shared location for temporary images in a Solaris environment, the following configuration is recommended:

- The shared directory must be mounted with read/write access from other machines.
- The HP Business Availability Center user account must have read/write access on the shared directory.

To modify the path to the directory holding temporary image files:

1. Open the file <**Gateway Server root directory**>**conf****topaz.config** in a text editor.
2. Search for the parameter **images.save.directory.offline**.
3. Remove the comment marker (#) from the line that begins **#images.save.directory.offline=** and modify the value to specify the required path.

Note: In Windows environments, use UNC path syntax (**server****path**) when defining the path. In a Solaris environment, use forward slashes (/) and not backslashes (\) when defining the path.

---

4. Save the **topaz.config** file.
5. Restart HP Business Availability Center on the Gateway Server machine.
6. Repeat the above procedure on all Gateway Server machines.
7. Map the newly defined physical directory containing the images to a virtual directory in the Web server on all Gateway Server machines. For details, see the next section.

Accessing Temp Directory with Multiple Gateway Server Machines

If you define a custom path to temporary images (as defined in the **images.save.directory.offline** parameter), you must map the physical directory containing the images to a virtual directory in the Web server on all Gateway Server machines.

To configure the virtual directory in IIS:

1. Rename the default physical directory containing the temporary scheduled report images on the Gateway Server machine.

   For example, rename:

   <Gateway Server root directory>\AppServer\webapps\site.war\Imgs\chartTemp\offline

   to

   <Gateway Server root directory>\AppServer\webapps\site.war\Imgs\chartTemp\old_offline

2. In the IIS Internet Services Manager on the Gateway Server machine, navigate to **Default Web site** > **Topaz** > **Imgs** > **ChartTemp**.

   The renamed offline directory appears in the right frame.

3. In the right frame, right-click and select **New** > **Virtual Directory**. The Virtual Directory Creation Wizard opens. Click **Next**.

4. In the Virtual Directory Alias dialog box, type offline in the Alias box to create the new virtual directory. Click **Next**.

5. In the Web Site Content Directory dialog box, type or browse to the path of the physical directory containing the temporary images (the path defined in the **images.save.directory.offline** parameter). Click **Next**.

6. If the physical directory containing the temporary images resides on the local machine, in the Access Permissions dialog box, specify **Read and Write** permissions.

   If the physical directory containing the temporary images resides on a machine on the network, in the User Name and Password dialog box, enter a user name and password of a user with permissions to access that machine.

7. Click **Next** and **Finish** to complete Virtual Directory creation.

8. Restart HP Business Availability Center on the Gateway Server machine.

9. Repeat the above procedure on all Gateway Server machines.

To configure the virtual directory on Apache HTTP Web Server:

1. Rename the default physical directory containing the temporary scheduled report images on the Gateway Server machine.

   For example, rename:

   <Gateway Server root directory>\AppServer\webapps\site.war\Imgs\chartTemp\offline

   to

   <Gateway Server root directory>\AppServer\webapps\site.war\Imgs\chartTemp\old_offline

2. Open the Apache configuration file **<Gateway Server root directory>\WebServer\conf\httpd.conf** with a text editor.

3. Map a virtual directory named **offline** to the physical location of the common directory by adding the following line to the file:

   Alias /Imgs/chartTemp/offline <shared_temp_image_directory>

   where <shared_temp_image_directory> represents the path to the physical directory containing the temporary scheduled report images (the path defined in the **images.save.directory.offline** parameter).

4. Save the file.

5. Restart HP Business Availability Center on the Gateway Server machine.

6. Repeat the above procedure on all Gateway Server machines.

To configure the virtual directory on Sun Java System Web Server:

1. Rename the default physical directory containing the temporary scheduled report images on the Gateway Server machine.

   For example, rename:

   <Gateway Server root directory>\AppServer\webapps\site.war\Imgs\chartTemp\offline

   to

   <Gateway Server root directory>\AppServer\webapps\site.war\Imgs\chartTemp\old_offline

2. Open the Sun Java System Web Server configuration file **<Sun Java System Web Server installation directory>\server\<server_nam>\config\obj.conf** with a text editor.

3. Add the following line inside the <Object name=default> directive (but before the line **NameTrans fn="pfx2dir" from="/Imgs" dir="ProductDir/Site Imgs/"**, if it exists, and before the line **NameTrans fn=document-root root="$docroot"**):

   NameTrans fn="pfx2dir" from=”/topaz/Imgs/chartTemp/offline" dir="<shared_temp_image_directory>"

   where <shared_temp_image_directory> represents the path to the physical directory containing the temporary scheduled report images (the path defined in the **images.save.directory.offline** parameter).

4. Save the file.

5. Restart the Sun Java System Web Server on the Gateway Server machine.

6. Repeat the above procedure on all Gateway Server machines.

Modifying the Length of Time that HP Business Availability Center Keeps Temporary Image Files

You can modify settings that control how long HP Business Availability Center keeps temporary image files generated by the Gateway Server machine, before removing them from the defined temporary directories. You can modify settings for the following directories in the **<HP Business Availability Center Gateway Server root directory>\conf\topaz.config** file:

Directory Setting	Description
remove.files.0.path=../../AppServer/webapps/site.war/Imgs/chartTemp/offline	Path to images created when generating scheduled reports and Analytics reports
remove.files.1.path=../../AppServer/webapps/site.war/Imgs/chartTemp/online	Path to images created when generating reports in HP Business Availability Center applications
remove.files.3.path=../../AppServer/webapps/site.war/snapshots	Path to images created by the Snapshot on Error mechanism and viewed in Error Summary reports

For the above temporary image directories, you can modify the following settings:

- **remove.files.directory.number=<number of directories>**

  Specifies the total number of directories for which you are defining settings.

- **remove.files.<num_of_path>.path=<path to directory>**

  Specifies the path to the directory that contains the files you want to remove. For the default directories that remove temporary image files, these values must match the **images.save.directory.online** and **images.save.directory.offline** parameters, also defined in the topaz.config file.

Note: In Windows environments, use UNC path syntax (**server****path**) when defining the path. In Solaris environments, use forward slashes (/) only when defining the path.

➤ **remove.files.<num_of_path>.expirationTime=<file expiration time in sec>**

Specifies the time, in seconds, that HP Business Availability Center leaves a file in the specified directory. For example, if you specify "3600" (the number of seconds in 1 hour), files older than one hour are removed.

Leave this setting empty if you want HP Business Availability Center to only use maximum size criteria (see below).

➤ **remove.files.<num_of_path>.maxSize=<maximum size of directory in KB>**

Specifies the total size to which the defined directory can grow before HP Business Availability Center removes files. For example, if you specify "100000" (100 MB), when the directory exceeds 100 MB, the oldest files are removed in order to reduce the directory size to 100 MB.

If you also define a value in the **remove.files.<num_of_path>.expirationTime** parameter, HP Business Availability Center first removes expired files. HP Business Availability Center then removes additional files if the maximum directory size limit is still exceeded, deleting the oldest files first. If no files have passed their expiration time, HP Business Availability Center only removes files based on the maximum directory size criteria.

This parameter is used in conjunction with the **remove.files.<num_of_defined_path>.deletePercents** parameter (see below), which instructs HP Business Availability Center to remove the specified percentage of files, in addition to the files removed using the **remove.files.<num_of_path>.maxSize** parameter.

Leave this and the **remove.files.<num_of_defined_path>.deletePercents** settings empty if you want HP Business Availability Center to only use the expiration time criterion.

➤ **remove.files.<num_of_path>.deletePercents=<percent to remove>**

Specifies the additional amount by which HP Business Availability Center reduces directory size—expressed as a percentage of the maximum allowed directory size—after directory size has been initially reduced according to the **remove.files.<num_of_path>.maxSize** parameter. HP Business Availability Center deletes the oldest files first.

Leave this and the **remove.files.<num_of_path>.maxSize** settings empty if you want HP Business Availability Center to only use the expiration time criterion.

➤ **remove.files.<num_of_path>.sleepTime=<thread sleep time in sec>**

Specifies how often HP Business Availability Center runs the mechanism that performs the defined work.

Example

HP Business Availability Center is instructed to perform the following work once every 30 minutes: HP Business Availability Center first checks whether there are files older than 1 hour and, if so, deletes them. Then HP Business Availability Center checks whether the total directory size is greater than 250 MB, and if so, it reduces directory size to 250 MB by removing the oldest files. Finally, HP Business Availability Center reduces the total directory size by 50% by removing the oldest files. As a result, HP Business Availability Center leaves files totaling 125 MB in the directory.

```
# remove files older than 1 hour (3600 sec.)
remove.files.0.expirationTime=3600
# reduce folder size to 250 MB
remove.files.0.maxSize=250000
# remove an additional 50% of max. folder size (125 MB)
remove.files.0.deletePercents=50
# perform work once every 30 min. (1800 sec)
remove.files.0.sleepTime=1800
```

Note: You can configure the file removal mechanism to remove files from any defined directory. You define the parameters and increment the index. For example, to clean out a temp directory, you would specify **6** instead of **5** for the number of directories in the **remove.files.directory.number** parameter; then you would define the directory's path and settings using the index value **4** (since 0-4 are already being used by the default settings) in the **num_of_path** section of the parameter. Do not use this mechanism to remove files without first consulting with your Customer Support representative.

To modify the default settings:

1 Open the file **<HP Business Availability Center Gateway Server root directory>\conf\topaz.config** in a text editor.

Tip: Before modifying the values, back up the file or comment out (using #) the default lines so that the default values are available as a reference.

---

2 Modify the settings as required.

3 Save the **topaz.config** file.

4 Restart HP Business Availability Center on the Gateway Server machine.

Repeat the above procedure on all Gateway Server machines.

Specifying the Directories from Which Temporary Image Files Are Removed

By default, temporary image files are removed from the root path of the specified directory. However, you can also configure HP Business Availability Center to remove temporary image files from the subdirectories of the specified path.

To configure HP Business Availability Center to remove temporary images files from subdirectories:

1. Open the file <**Gateway Server root directory**>**conf****topaz.config** in a text editor.
2. Insert the following line after the specified path's other settings (described in the previous section):

   remove.files.<num_of_path>.removeRecursively=yes

3. Save the **topaz.config** file.
4. Restart HP Business Availability Center on the Gateway Server machine.
5. Repeat the above procedure on all Gateway Server machines.

6

System Health

This chapter includes the main concepts of System Health.

Important: If you do not deploy the new System Health interface, your system will default to the Legacy System Health application. For details on Legacy System Health, see "Legacy System Health" on page 187.

Introduction to System Health

System Health uses the SiteScope monitoring system to monitor the servers, databases, and data collectors running on your HP Business Availability Center system.

You use System Health to:

- Measure HP Business Availability Center performance by viewing the output from monitors running on the various HP Business Availability Center components.
- Measure areas of the databases that influence HP Business Availability Center performance.
- Display problematic areas of the HP Business Availability Center servers, databases, and data collectors.
- Perform operations on your HP Business Availability Center environment, such as:
  - Move Backend Services
  - Configure Backup Servers
  - Manage BAC Processes
- View log files on specific components in a variety of formats.
- View information on HP Business Availability Center components and monitors in .csv (displaying current status), and Quick Report (displaying status of past 24 hours) format.

System Health Setup Wizard Overview

The System Health Setup Wizard creates remote connections to the servers which System Health needs to monitor. If remote connections are not created, many of the monitors do not work.

Access the System Health Setup Wizard

The System Health Setup Wizard is accessible in one of the following ways:

- Through the first run of the System Health application on the machine running HP Business Availability Center.
-  Clicking the **Full Model Synchronization** button on the System Health Dashboard Toolbar or the Inventory Tab Toolbar.
-  Clicking the **Soft Sync** button on the System Health Dashboard Toolbar or the Inventory Tab Toolbar.

Note:

- Clicking the Soft Sync button displays only the portion of the wizard relevant to changes made in the HP Business Availability Center system. If no changes were made, clicking this button does not generate the System Health Setup Wizard.
- The user whose remote connection information you enter into the System Health Setup Wizard can perform only those actions for which they have permissions.

Sample Status and Description

When creating remote connections through the System Health Setup Wizard, the connection status is indicated by a colored icon.

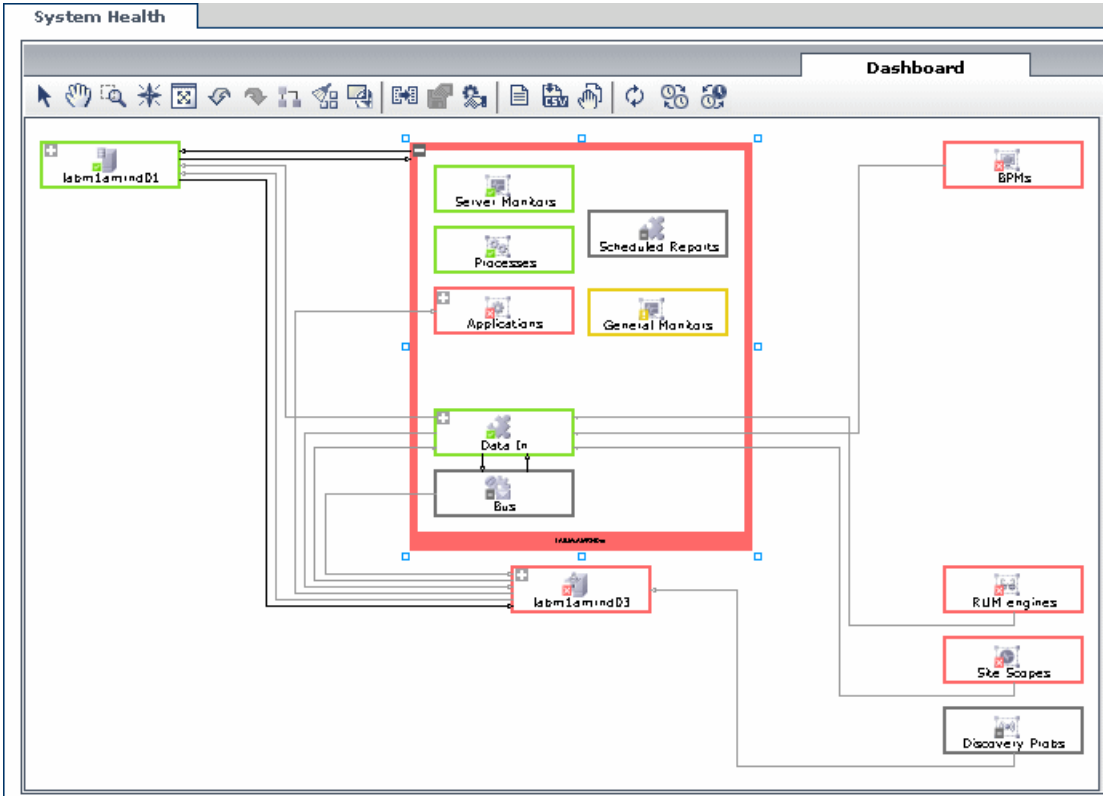
The following table describes each color and its status:

Status	Description
	A green icon indicates that remote connectivity between System Health and the component has been established, and that all of the component's monitors are enabled to run.
	A red icon indicates that remote connectivity between System Health and the component has failed, and therefore, the monitors on the component do not communicate with the server, rendering their information unavailable. A red icon is accompanied by an "x" symbol inside a red square.
	A gray icon indicates that remote connectivity between System Health and the component was not attempted to be established, and therefore, the monitors on the component do not receive an answer from the server. A gray icon is accompanied by a "-" symbol inside a gray square.

System Health Displays

The HP Business Availability Center components and their statuses are displayed in the following formats:

➤ **System Health Dashboard.** Displays a map of all HP Business Availability Center components. The color of the component boxes' outline indicates the components' status.



You can click the expand button to expand components and view the subcomponents contained therein. You can also double click a monitor in the **Monitors** table to open the parent component in the System Health Dashboard.

You can click the collapse button to collapse components and hide the subcomponents contained therein.

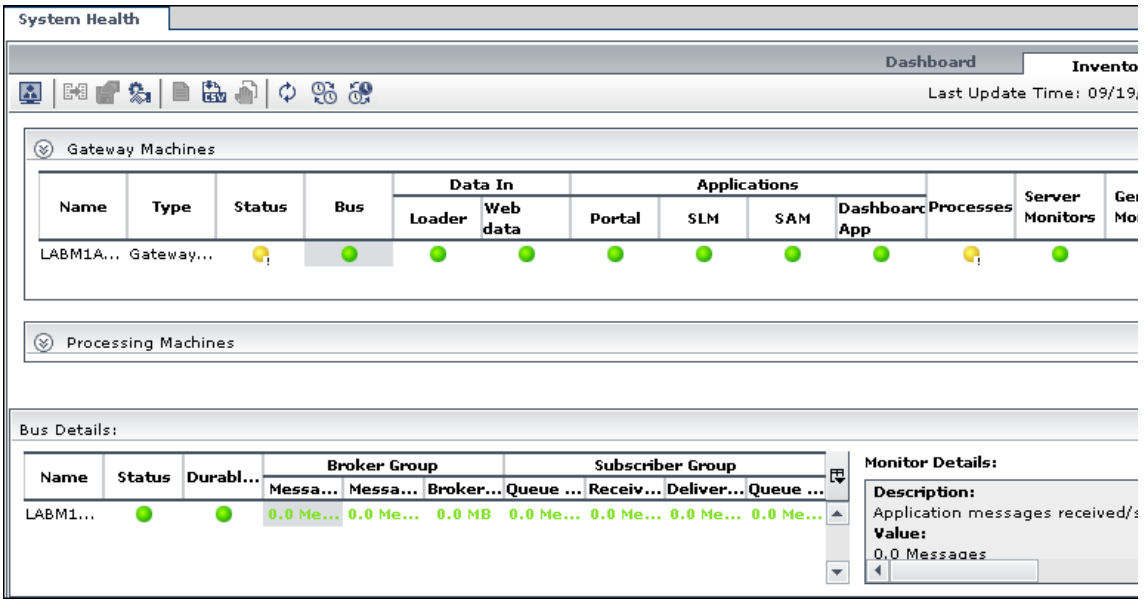
Important: You must select the cursor button on the System Health Dashboard Toolbar to operate the expand and collapse buttons. The cursor is the default selection when you enter the System Health Dashboard.

The Monitors Table in the Right Pane displays information about the monitors running on the highlighted component or subcomponent. The General Table in the Right Pane displays information about the properties associated with the highlighted server.

Note: The General Table is only visible when highlighting a server on the Map of HP Business Availability Center System and Components.

➤ **Inventory Tab.** Displays information on Gateway Server and Data Processing Server components, and their subcomponents, in table form. The Inventory Tab enables you to compare the performance of the subcomponents and monitors on multiple servers by presenting their statuses in a single view.

The **<Subcomponent Name> Details** table displays information on the highlighted subcomponent, and the **Monitor Details** area provides additional information on the subcomponent's monitors, if applicable.



Component Status and Description

The following table displays a sample icon and a description of its outlined color and status:

Status	Description
	A component enclosed by a green outline indicates that the component is working properly. The component's icon is accompanied by a **check** symbol inside a green square.
	A component enclosed by a red outline indicates that a critical problem exists in the component, in one of its subcomponents, or both. The component's icon is accompanied by an **x** symbol inside a red square.
	A component enclosed by a yellow outline indicates one of the following: ➤ A non-critical problem exists either in the component, in one or more of its subcomponents, or both. ➤ The component's monitors were unable to retrieve an answer from the server. The component's icon is accompanied by a **!** symbol inside a yellow square.
	A component enclosed by a gray outline indicates that there are currently no monitors scheduled to run for the component. The component's icon is accompanied by a - sign inside a gray square.
	A component enclosed by a jagged blue outline together with the component's color indicates the highlighted component.

Note: The color of all component outlines reflects the lowest functioning level subcomponent or monitor contained in the component, known as the **worst child rule**. The exception to this rule is the gray outlined components, which do not automatically cause their parent components to be outlined in gray.

Monitor Status and Description

The following table displays a colored indicator and a description of its status, as appearing on both the Inventory Tab and the Monitors table in the Right Pane:

Status	Description
	The component and all subcomponents are working properly (status is **good**).
	The component or a sub component has a critical problem (status is **error**). A red indicator is accompanied by an **x** symbol.
	The component or a sub component has a non-critical problem, or didn't receive an answer from the server (status is **warning**). The yellow indicator is accompanied by a **!** symbol.
	There is no data for the monitors. Monitors did not run yet. The gray indicator is accompanied by a - symbol.

Note: After deploying System Health, the monitor colors appear gradually as each monitor runs according to its schedule.

Understanding Service Reassignment

HP Business Availability Center can be deployed either through the recommended deployment configuration, or legacy deployment configuration.

Recommended Deployment

The recommended deployment consists of a Gateway Server (or two Gateway Servers behind a load balancer) and a Data Processing Server. The Data Processing server can also have a backup server.

If a certain Data Processing Server machine is not functioning properly or requires downtime for servicing, administrators can manually reassign the services running on that machine to a different Data Processing Server machine. Administrators can also preconfigure a specific Data Processing Server to automatically fail over to a specific backup machine.

The reassignment process can take up to 25 minutes, during which time the system is in downtime.

Legacy Deployment

In legacy enterprise environments, the Data Processing Server is split into three standalone servers:

- Modeling Data Processing Server
- Online Data Processing Server
- Offline Data Processing Server

Each server is installed on a separate machine. Each server might also have one backup machine defined for it.

If a certain Data Processing Server machine is not functioning properly or requires downtime for servicing, administrators can manually reassign the services running on that machine to a different Data Processing Server machine. Administrators can also preconfigure a specific Data Processing Server to automatically fail over to a specific backup machine.

The reassignment process can take up to 25 minutes, during which time the system is in downtime.

There are several theoretical scenarios for reassigning services among machines, to manage resource issues or enable server administration. The table below illustrates these scenarios by indicating the paths along which services can be reassigned.

Flow Table

	To Full Data Processing Server (Backup server in recommended deployment)	**To Modeling Data Processing Server**	**To Online Data Processing Server**	**To Offline Data Processing Server**
From Full Data Processing Server	Yes **Note:** This is the recommended sever deployment	Yes - for modeling services	Yes - for online services	Yes - for offline services
From Modeling Data Processing Server	Yes	Yes	No	No

From Online Data Processing Server	Yes	No	Yes	No
From Offline Data Processing Server	Yes	No	No	Yes

Deploy and Access System Health

You deploy System Health either on a machine with access to HP Business Availability Center (recommended so that System Health continues to run if HP Business Availability Center servers are down) or on any HP Business Availability Center Gateway Server (if an additional machine is not available).

You can access System Health:

- directly, via a Web browser using the syntax: **http://<server_name>:18080/SiteScope/SH/Main.do**
- as an application embedded in HP Business Availability Center, after configuring the appropriate URL in the Infrastructure Settings section of Platform Administration. For details, see the procedure below.

Deploying System Health

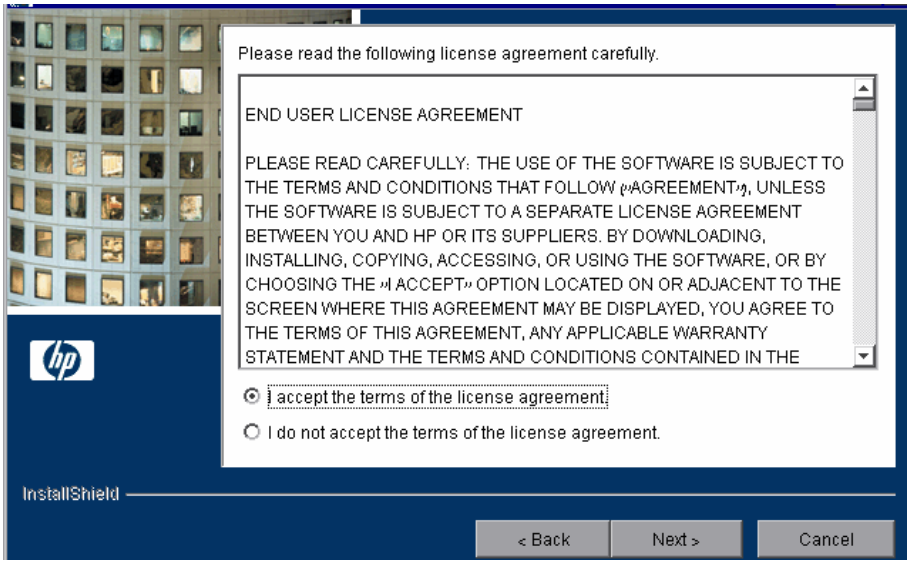
You must ensure that the Gateway server and the management database are up and running before deploying System Health. System Health must be deployed in the same domain as HP Business Availability Center, and any firewalls must be open.

To deploy System Health:

1 Insert the SiteScope installation disk into your machine.

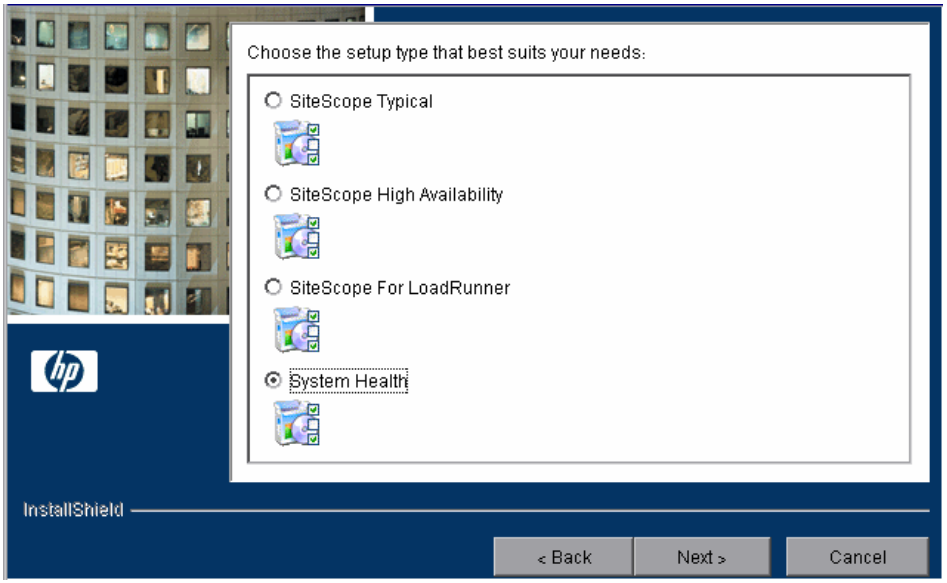
2 Select the **setup.exe** option. The HP SiteScope installation wizard is displayed.

3 Click **I accept the terms of the license agreement** and click **Next**.

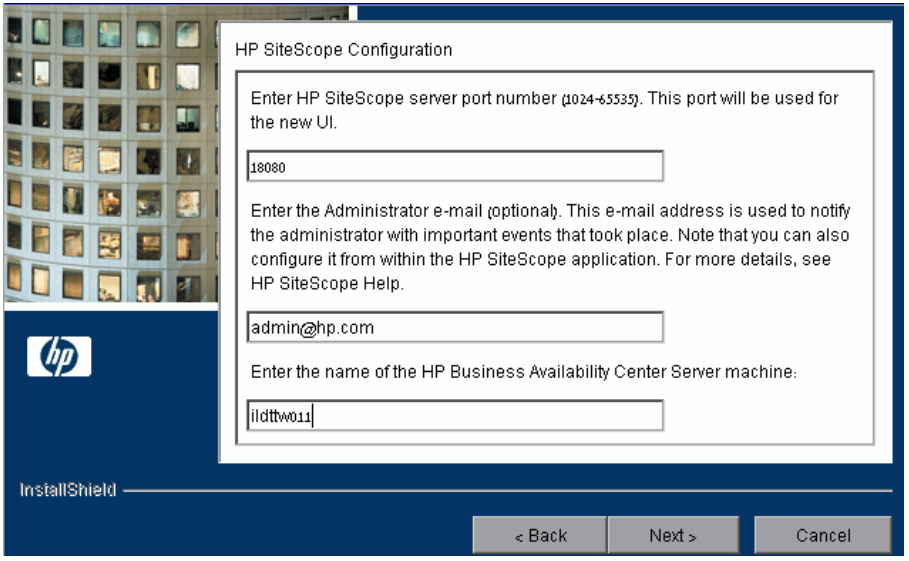


4 Enter a directory to install SiteScope on, or accept the default **C:\SiteScope**, and click **Next**.

5 Select the **System Health** setup type, and click **Next**.



6 Enter the following information in the HP SiteScope Configuration window:



- The HP SiteScope server port number. Accept the default port number of 18080, or choose another port that is free.
- The administrator e-mail address, used to notify the administrator of important events that took place.

Note: This setting is optional.

- The name of the HP Business Availability Center Gateway Server.

7 Check the summary information in the resulting window and click **Next**. The HP SiteScope installation process runs.

8 Click **Next** when the installation process finishes.

9 Restart your computer for the HP SiteScope installation to take effect. Click **Yes** to restart your computer, or **No** if you want to restart your computer later.

10 Click **Finish** to exit the HP SiteScope installation wizard.

System Health is now deployed in your HP Business Availability Center environment.

Note: If System Health is deployed on a Solaris machine, it can only monitor other Solaris machines. You can configure general properties on the System Health setup wizard, but advanced properties must be configured via SiteScope.

Accessing System Health

You access System Health either as an embedded part of HP Business Availability Center, or directly in a Web browser:

To access System Health in HP Business Availability Center:

1 Ensure that System Health has been installed, either on your dedicated server or on your Gateway Server. This must be done before you can access the System Health interface.

2 Log into your HP Business Availability Center machine. For details, see "Logging into HP Business Availability Center" on page 17.

3 Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, select **System Health**, and locate the **URL** entry in the System Health table. Modify the value to the following URL:

http://<machine name>:<port number>/SiteScope/Main.do

Where the following values are true:

<machine name> = The machine System Health is installed on.

<port number> = 18080 by default, or you can choose another port that is free.

4 Click **Save** to register the URL for accessing System Health in HP Business Availability Center.

Note: Steps 3 - 4 are performed the first time you access the System Health interface.

---

5 Select **Admin** > **Platform** > **Setup and Maintenance** > **System Health** to access the System Health interface.

To access System Health directly in a Web browser:

1 Ensure that System Health has been installed, either on your dedicated server or on your Gateway Server. This must be done before you can access the System Health interface.

2 Enter the following link into your browser window:

http://<machine name>:<port number>

Where the following values are true:

<machine name> = The machine System Health is installed on.

<**port number**> = 18080 by default, or you can choose another port that is free.

Note: It can take several minutes for the System Health application to appear on your screen.

---

3 Enter your login name and password in the appropriate boxes to log into System Health.

Initial access can be gained using the default login parameters:

Login Name=**systemhealth**, Password=**systemhealth**

It is recommended that you change this password immediately to prevent unauthorized entry. To change the password, click the **Change Password** link on the System Health login page.

Note: After changing your password on the System Health login page, you must enter your System Health username and password when accessing System Health in HP Business Availability Center. Once you have done this, HP Business Availability Center does not require you to re-enter this information to access System Health until the next time your password is changed on the System Health login screen.

Deploying System Health in a Secured Environment

When deploying System Health in a secured HP Business Availability Center environment, note the following:

- On the System Health Dashboard, Reverse Proxy components are depicted together with the Load Balancer components, called **mediators**.
- The WDE URL monitor appears red until you enter the monitor's username and password in SiteScope.
- When accessing System Health via HP Business Availability Center, you must enter a username and password to view the System Health interface.
- You must supply the name of the Gateway server, and not the reverse proxy.

Ensure the Health of Your HP Business Availability Center System

System Health enables you to monitor the components of your HP Business Availability Center system and ensure they are functioning properly. In addition to monitoring the performance of your components, you can map HP Business Availability Center to recognize your infrastructure deployment, move services from one server to another, configure backup servers, manage BAC processes, and generate a Quick Report on component performance.

Configure Remote Connection Details for HP Business Availability Center Monitors

You optionally provide the server's remote connection details for the HP Business Availability Center monitors (such as cpu) that require it. You also configure recipients to receive System Health alerts via e-mail. For details, see "System Health Setup Wizard" on page 154.

Monitor Performance of HP Business Availability Center Components

You can monitor the performance of the servers, databases, and data collectors running on your HP Business Availability Center system and view the results via either the System Health Dashboard tab or the Inventory tab. For details, see "System Health Displays" on page 101.

Example

➤ **System Health Dashboard**

The System Health Dashboard components are presented with an icon surrounded by a colored box. You can navigate these components by clicking on the toolbar on the System Health Dashboard. For details on the System Health Dashboard Toolbar, see "Toolbar" on page 169.

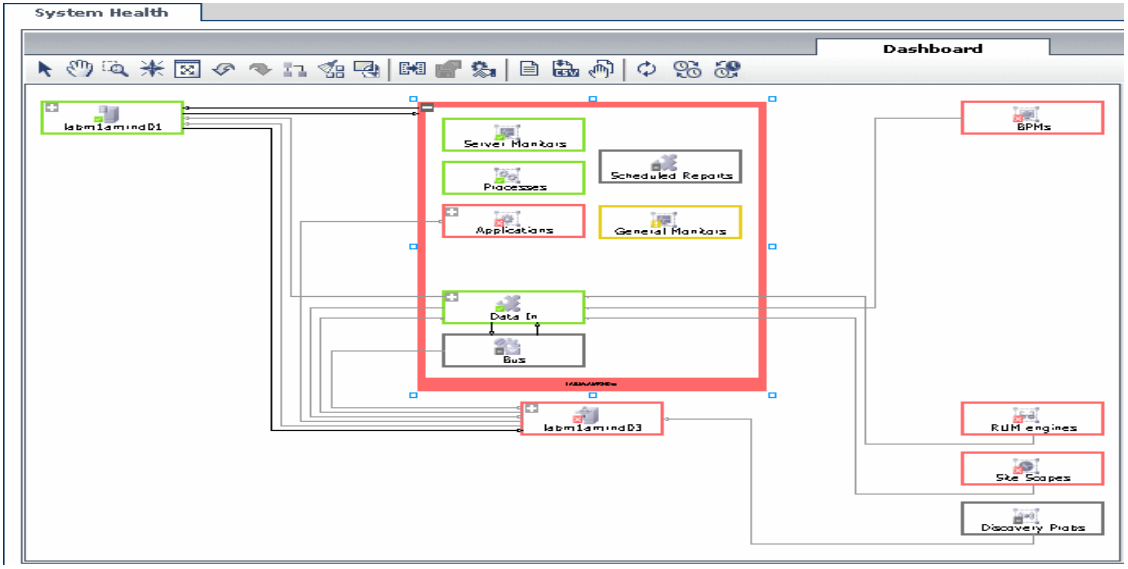
A component's status is indicated by both its outlined color and status icon color.

For details on the components' outlined colors, see "Map of HP Business Availability Center System and Components" on page 181.

Click the expand icon on a component to view its subcomponents.

Click the collapse icon on a component to hide its subcomponents.

You can also retrieve information on HP Business Availability Center servers via the General Table, and information on the server's components on the Monitors Table in the Right Pane of the System Health Dashboard.

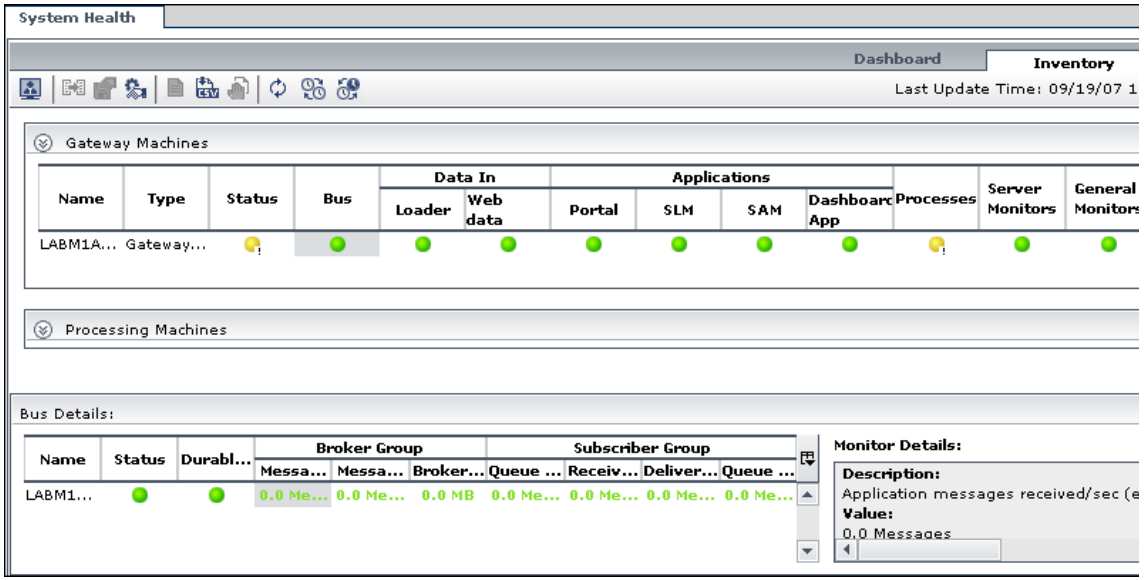


➤ **Inventory Tab**

The Inventory Tab enables you to compare the performance of the subcomponents and monitors on multiple servers by presenting their statuses in table format. Statuses are indicated by color icons in the components' cells. The Inventory Tab is helpful for getting a flat view of your monitored environment.

For details on the components' color icons, see "System Health Displays" on page 101.

You can also retrieve information about the monitors running on the various subcomponents via the <Subcomponent Name> Details Table.



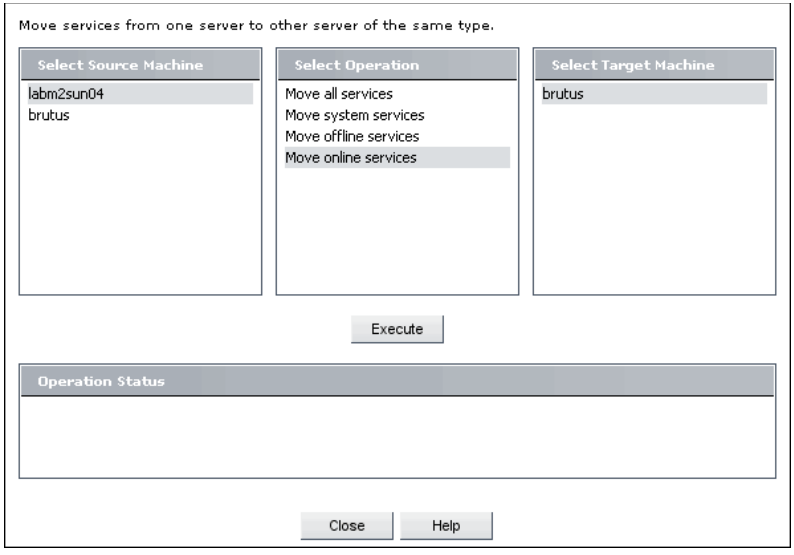
Move Backend Services

In the Service Manager Dialog Box, you move backend services from one server to another of the same type, in case the server machine is not functioning properly or requires downtime for servicing.

For details, see “Service Manager Dialog Box” on page 174.

Example

1. Click the **Service Manager button** on the Toolbar on either the System Health Dashboard or the Inventory Tab.
2. Select the machine that you want to move services from in the **Select Source Machine** window.
3. Select the operation you want to perform in the **Select Operation** window.
4. Select the machine you want to move services to in the **Select Target Machine** window.
5. Click the **Execute** button. The operation status appears in the **Operation Status** window.

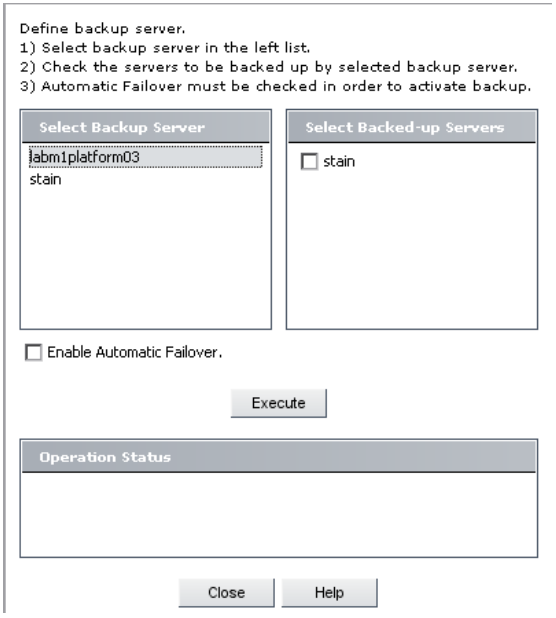


Configure Backup Servers

In the Configure Backup Servers Dialog Box, you define a backup server, in case the server machine is not functioning properly or requires downtime for servicing. For details, see “Backup Server Setup Window” on page 175.

Example

1. Click the **Backup Server Configuration** button on the Toolbar on either the System Health Dashboard or the Inventory Tab.
2. Select a backup server from the left pane.
3. Select a server to be backed-up from the right pane.
4. Click the **Enable Automatic Failover** checkbox.
5. Click **Execute** to register your backup server.



Note: You must perform step 4 to activate your selection as the backup server.

Manage BAC Processes

In the Manage BAC Processes Dialog Box, you stop or start Business Availability Center Processes on specific servers. For details, see "Process Manager Dialog Box" on page 176.

Example

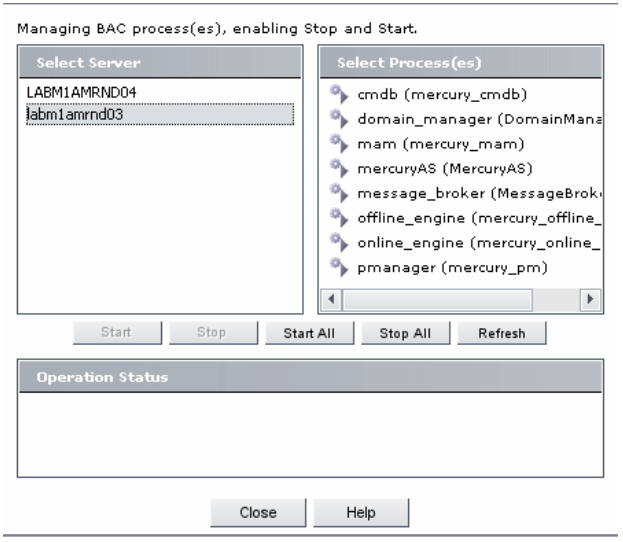
1 Click the **Process Manager** button on the Toolbar on either the System Health Dashboard or the Inventory Tab.

2 Select the server you want to start or stop processes on in the **Select Server** window.

3 Select the process you want to start or stop in the **Select Process(es)** window. You can select multiple processes in one of the following ways:

- Press the CTRL key while selecting additional processes.
- Press and hold the SHIFT key while pressing the up or down cursor buttons on the keyboard.

4 Click **Start** to start the selected processes, **Stop** to stop the selected processes, or **Refresh** to refresh the processes' status. You can also start all processes by clicking the **Start All** button, and stop all processes by clicking the **Stop All** button. The Operation Status appears in the **Operation Status** window.



Display a Quick Report

Click the Quick Report button to display a Quick Report displaying information on monitors deployed on HP Business Availability Center components. For details, see "Quick Report Screen" on page 180.

Example

Table Format
Error List
Warning List
Good List

Close Window

Summary for Multiple Monitors

(information from 8:58 AM 7/9/07 to 12:18 PM 7/9/07)

Uptime Summary

Name	Uptime %	Error %	Warnin
Durable Subscriber Group	94.73	0	
Monitor Broker Group	94.73	0	
Monitor Subscriber Group	94.73	0	
Monitor Container Group	94.73	0	
Log Level for D$\HPBAC\conf\core\Tools\log4j\mercury_online_engine	100	0	
Log Level for D$\HPBAC\conf\core\Tools\log4j\mercury_offline_engine	100	0	
Log Level for D$\HPBAC\conf\core\Tools\log4j\mercury_data_upgrade	100	0	
Log Level for D$\HPBAC\conf\core\Tools\log4j\mam	100	0	
Log Level for D$\HPBAC\conf\core\Tools\log4j\mercury_upgrade_wizard	100	0	
Log Level for D$\HPBAC\conf\core\Tools\log4j\cmdb	100	0	
Log Level for D$\HPBAC\conf\core\Tools\log4j\common	100	0	
Log Level for D$\HPBAC\conf\core\Tools\log4j\mercury_wde	100	0	
Log Level for D$\HPBAC\conf\core\Tools\log4j\data_marking	100	0	
Log Level for D$\HPBAC\conf\core\Tools\log4j\PlainJava	100	0	
Log Level for D$\HPBAC\conf\core\Tools\log4j\EJB	100	0	
Log Level for D$\HPBAC\conf\core\Tools\log4j\mercury_pm	100	0	
Log Level for D$\HPBAC\conf\core\Tools\log4j\Servlets	100	0	

HP Business Availability Center Components

The System Health interface displays the following HP Business Availability Center components:

- **Data Collectors.** Tools that collect availability and performance data. Data collectors include:
  - **BPMs.** Business Process Monitors, which run scripts simulating user actions and collect resulting data.
  - **RUM Engines.** Real User Monitors, which monitor actual user traffic and activity and collect resulting data.
  - **SiteScopes.** Monitor performance of IT infrastructure.

- **Discovery Probes.** Discover all the components of your IT infrastructure, create CIs for them, and send the data to the UCMDB.
- **Gateway Machines.** One of the servers on which HP Business Availability Center runs. The Gateway Server is responsible for running HP Business Availability Center applications, producing reports, operating the Administration Console, receiving data samples from the data collectors and distributing this data to the relevant HP Business Availability Center components, and supporting the Bus.
- **Load Balancing Machines.** Displayed only if deployed. Load balancers ensure that the data flow is evenly distributed among all HP Business Availability Center Gateway Servers so that no one particular server becomes overloaded.
- **Processing Machines.** One of the servers on which HP Business Availability Center runs. The Data Processing Server is responsible for aggregating and partitioning data, running the Business Logic Engines, and controlling the HP Universal CMDB-related services.

  Components are displayed on both the System Health Dashboard and the Inventory tab.
- **Databases.** Monitors the databases HP Business Availability Center is using.
- **UCMDB.** Displayed only if deployed separately. The UCMDB serves as a central repository for configuration information.
- **Reverse Proxy Server.** Displayed only when System Health is configured in a secure environment. For details on Reverse Proxies, see "Using a Reverse Proxy in HP Business Availability Center" in the *HP Business Availability Center Hardening Guide* PDF.

Troubleshooting

The following table illustrates potential problems that can occur on the System Health interface, and suggested solutions:

Problem	Solution
Interface does not display any HP Business Availability Center components	Click the **Refresh** button on your browser. **Note:** This problem is most common when first logging into System Health on Internet Explorer 7.0.
All components and monitors are displayed in gray	 Click the Full Model Synchronization button on the Toolbar in either the System Health Dashboard or the Inventory Tab. The Full Model Synchronization button resets the System Health configuration and erases all of the monitors' history in HP Business Availability Center. You then reconfigure System Health from the System Health Setup Wizard.
Monitors are not displayed on a component	

System Health Monitors

System Health uses SiteScope monitors to measure the performance of your HP Business Availability Center components. Some of the monitors are monitors that are available in the SiteScope application and some are configured specifically for System Health.

This section describes the following groups of monitors:

- "Machine Hardware Monitors" on page 124
- "Database Monitors" on page 125
- "HP Business Availability Center Server Monitors" on page 126
- "Gateway Server Monitors" on page 129
- "Processing Server Monitors" on page 137
- "Data Collectors" on page 148

Machine Hardware Monitors

The following group of monitors monitor the hardware on which the Business Availability Center applications run and, where indicated, some of them monitor databases as well:

Machine Hardware Monitors

Monitor Name	Description
Ping	Checks the availability of the host via the network. Runs on HP Business Availability Center and Database servers. If Business Availability Center includes a proxy server or load balancer, this monitor runs on the mediator or load balancer. **Included Measurements:** ➤ **Round Trip Time** ➤ **Loss Percentage** **Threshold Configured In:** SiteScope For details, see "Ping Monitor Overview" in *Using System Availability Management*.
Server Virtual Memory	Tracks how much virtual memory is currently in use on the server. Runs on HP Business Availability Center and Database servers. **Threshold Configured In:** SiteScope For details, see "Memory Monitor Overview" in *Using System Availability Management*.
Server CPU	Tracks how much CPU is currently in use on the server. Runs on HP Business Availability Center and Database servers. **Threshold Configured in:** SiteScope For details, see "CPU Utilization Monitor Overview" in *Using System Availability Management*.

Monitor Name	Description
Server Disk Space	Tracks how much disk space is currently in use on the hard disk drive where HP Business Availability Center is installed. Runs only on the HP Business Availability Center server. **Threshold Configured In:** SiteScope For details, see "Disk Space Monitor Overview" in *Using System Availability Management*.

Database Monitors

The following monitors monitor each database running on the HP Business Availability Center database servers. There can be multiple databases running on a server and there is a monitor instance for each database:

Monitor Display Name	Purpose
DB Statistics	Verifies that database statistics have been collected for all tables created more than 24 hours ago.
Database Connectivity	Verifies the connection between HP Business Availability Center and the database.

HP Business Availability Center Server Monitors

The following monitors run on the Gateway server, the Processing server, or both (if not otherwise indicated, the monitor runs on both):

General Monitors

Monitor Name	Description
Out of Memory in Log	Searches for unexpected behavior due to out of memory, displayed as instances of Out of Memory in **topaz_all.ejb.log**. For details, see "Log File Monitor Overview" in *Using System Availability Management*.
Nanny Manager Process	Monitors whether HP Business Availability Center server processes are up and running. **Threshold Configured In:** SiteScope For details, see "Service Monitor Overview" in *Using System Availability Management*.
Log Level for <configuration directory>	Checks if any of the log files in the specified directory are configured to debug log level (i.e. - searches for the string **loglevel=debug**). **Threshold Configured In:** SiteScope
BAC Application Server Response	Checks that the BAC Application server is responsive. Information goes straight to the application server and not via the web server. This monitor runs only on the Gateway Server. **Threshold Configured In:** SiteScope For details, see "URL Monitor Overview" in *Using System Availability Management*.
Logged In Users	Displays the percentage and number of total users logged into HP Business Availability Center.
Web Server Status	Displays the current status of the Web server indicating its availability.

Process Monitors

For descriptions of the processes, see “Process Manager Dialog Box” on page 176.

The two JVM monitors listed monitor only the Java processes, which include:

- cmdb;
- DataUpgrade;
- mercury_db_loader;
- MercuryAS;
- MessageBroker;
- mercury_offline_engine;
- mercury_online_engine;
- topaz_pm_process;
- mercury_wde;
- MercuryWSGuard;

The <process name> monitor monitors all processes.

Monitor Display Name	Description
<Process Name> JVM Statistics Memory Monitors	Monitors the memory measurements for a Java process. **Included Measurements:** ➤ **Heap Free.** Displays the amount of Heap Free space in JVM. ➤ **Permanent Heap Free Memory.** Displays the amount of Permanent Heap Free space in JVM.
<Process Name> JVM Statistics Threads Monitors	Monitors the threads measurements for a Java process. The process name is in the name of the monitor. **Included Measurements:** ➤ **Current Thread Count.** Current number of threads used by the process ➤ **Peak Thread Count.** Maximum number of threads used by the process ➤ **Dead Locked Threads.** Number of deadlocked threads in the process
<process name>	Verifies whether the **<process name>** process is running, its CPU, and virtual memory utilization. For details, see "Service Monitor Overview" in *Using System Availability Management*.

Gateway Server Monitors

The following monitors run on the Gateway Server:

Data In/Web Data Entry

Monitor Name	Description
Web Data Entry Status	Determines the overall status of the Web Data Entry component. **Included Measurements:** ➤ **Bus Status.** Determines Web Data Entry connection to the Bus. ➤ **Gateway Status.** Determines Gateway availability. ➤ **Failures to Publish.** Indicates number of samples which failed to publish. ➤ **Output EPS.** Determines the number of published samples per second.
Out of Memory Exception in Log	Searches for unexpected behavior, displayed as instances of the string OutofMemoryExceptionInLog in the **wde.log** file. For details, see "Log File Monitor Overview" in *Using System Availability Management*.
Class Not Found Exception in Log	Searches for unexpected behavior, displayed as instances of the string ClassNotFoundException in the **wde.log** file. For details, see "Log File Monitor Overview" in *Using System Availability Management*.
Web Data Entry Availability	Determines if Web Data Entry is up and running. For details, see "URL Monitor Settings" in *Using System Availability Management*.

Data In/Loader

Monitor Name	Description
Main Flow	Measures flow of data in component. **Included Measurements:** ➤ **Number of Samples in Queues.** Used to control memory usage of the loader. ➤ **Bus Connection Status.** Checks loader connectivity to the Bus. **Threshold Configured In:** JMX of Infrastructure Settings. To access, go to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** and search under **System Health** or the applicable component application.
EPS ratio in main flow	Enables you to evaluate the ratio of the average insert rate to the loader with the average data insert rate to the database from the loader. **Threshold Configured In:** Infrastructure Settings. To access, go to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** and search under **System Health** or the applicable component application.
Connection to DB	Checks connection to database from loader process.
Average Insert Rate to DB (Recovery Flow)	Monitors the average insert rate to the database from the recovery persistency folder. **Threshold Configured In:** Infrastructure Settings. To access, go to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** and search under **System Health** or the applicable component application.
Out of Memory Exception in Log	Searches for the string Out of Memory in **Loader.log**. For details, see "Log File Monitor Overview" in *Using System Availability Management*.

Monitor Name	Description
Class Not Found Exception in Log	Searches for errors in **Loader.log**. For details, see "Log File Monitor Overview" in *Using System Availability Management*.
Max Files in Queue in Recovery Persister	Displays the number of files in the longest queue in the recovery persister directory. **Threshold Configured In:** Infrastructure Settings. To access, go to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** and search under **System Health** or the applicable component application.

Dashboard Application

Monitor Name	Description
Dashboard Admin	Searches for unexpected behavior, displayed as instances of ERROR, in **bam.admin.log.** **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.
Dashboard Application	Searches for unexpected behavior, displayed as instances of ERROR, in **bam.app.log.** **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.
Dashboard Application Front-end	Searches for unexpected behavior, displayed as instances of ERROR, in **bam.app.frontend.log.** **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.

Monitor Name	Description
Dashboard Front-end Actions	Searches for unexpected behavior, displayed as instances of ERROR, in **bam.actionbase.log.** **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.
Dashboard BLE Plug-in	Searches for unexpected behavior, displayed as instances of ERROR, in **bam.ble.plugin.log.** **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.
Dashboard Rules	Searches for unexpected behavior, displayed as instances of ERROR, in **bam.app.rules.log.** **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.
Dashboard Business Reports	Searches for unexpected behavior, displayed as instances of ERROR, in **bzd.log.** **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.
Dashboard Open API	Searches for unexpected behavior, displayed as instances of ERROR, in **bam.open.api.log.** **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.
Repositories	Searches for unexpected behavior, displayed as instances of ERROR, in **repositories.log.** **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.

Monitor Name	Description
Repositories UI	Searches for unexpected behavior, displayed as instances of ERROR, in **repositories.ui.log.** **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.
Repositories Upgrade	Searches for unexpected behavior, displayed as instances of ERROR, in **repositories.upgrade.log.** **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.
Repositories Context Menu UI	Searches for unexpected behavior, displayed as instances of ERROR, in **context.menu.log.** **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.
Center High Availability	Searches for unexpected behavior, displayed as instances of ERROR, in **bac.ha.centers.log.** **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.

Portal Application

Monitor Display Name	Description
MyBAC	Searches for unexpected behavior, displayed as instances of ERROR, in **portal.log.** **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.

Verticals Application

Monitor Display Name	Description
Verticals Core	Searches for unexpected behavior, displayed as instances of ERROR, in **vertical.ejb.log.** **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.
BAC for Siebel	Searches for unexpected behavior, displayed as instances of ERROR, in **siebel.ejb.log.** **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.
BAC for SAP	Searches for unexpected behavior, displayed as instances of ERROR, in **sap.ejb.log.** **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.

System Availability Management Application

Monitor Display Name	Purpose
SAM Admin Fatal	Searches for unexpected behavior, displayed as instances of FATAL, in **sam-admin.log**. **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.

Monitor Display Name	Purpose
SAM Admin SiteScope Profiles on DB	Searches for unexpected behavior, displayed as instances of ERROR-Unable to get SiteScope profiles from DB, in **sam-admin.log**. **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.
SAM Admin SiteScope Profiles List	Searches for unexpected behavior, displayed as instances of Failed retrieve SiteScope profiles list, in **sam-admin.log**. **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.

Service Level Management Application

Monitor Display Name	Purpose
SLAs Monitor Leaf Validator	Indicates that the SLM hierarchy does not detect its monitors, due to removed or replaced transactions or CIs.
SLM Logic	Searches for unexpected behavior, displayed as instances of unexpected result, in **slm.rules.log**. For details, see "Log File Monitor Overview" in *Using System Availability Management*.

Monitor Display Name	Purpose
SLM Reports	Searches for unexpected behavior, displayed as instances of unexpected result, in **slm_reports.ejb.log**. For details, see "Log File Monitor Overview" in *Using System Availability Management*.
SLM Snapshot	Searches for unexpected behavior, displayed as instances of unexpected result, in **slm_snapshot.ejb.log**. For details, see "Log File Monitor Overview" in *Using System Availability Management*.

Bus

Monitor Display Name	Purpose
Subscriber Group	Monitors subscriber-related measurements. **Threshold Configured In:** Infrastructure Settings. To access, go to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** and search under **System Health** or the applicable component application.
Broker Group	Monitors broker measurements. **Threshold Configured In:** Infrastructure Settings. To access, go to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** and search under **System Health** or the applicable component application.
Durable Subscriber Group	Provides information about durable subscribers in the broker. **Threshold Configured In:** Infrastructure Settings. To access, go to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** and search under **System Health** or the applicable component application.

Processing Server Monitors

The following component monitors run on the Processing Server:

Alerts Engine

Monitor Display Name	Purpose
BLE-BUS Connection Monitor	Monitors connection between the BLE Offline Engine and the Bus.
queue/alert_engine_alert	Measures the size of the queue between the BLE and the Alerts Listener. **Threshold Configured In:** Infrastructure Settings. To access, go to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** and search under **System Health** or the applicable component application.
queue/alert_engine_notification	Measures the size of the queue between the Alerts Listener and the Notification Listener. **Threshold Configured In:** Infrastructure Settings. To access, go to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** and search under **System Health** or the applicable component application.

Bus

Monitor Display Name	Purpose
Subscriber Group	Monitors subscriber related measurements. **Threshold Configured In:** Infrastructure Settings. To access, go to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** and search under **System Health** or the applicable component application.
Broker Group	Monitors broker measurements. **Threshold Configured In:** Infrastructure Settings. To access, go to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** and search under **System Health** or the applicable component application.
Durable Subscriber Group	Provides information about durable subscribers in the broker. **Threshold Configured In:** Infrastructure Settings. To access, go to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** and search under **System Health** or the applicable component application.

Database Services/Partition Manager

Monitor Display Name	Purpose
Partition Timely Creation	Verifies that partitions are created according to partitioning policy.
Oversized Partitions	Finds partitions with more than the allotted number of rows specified in threshold settings. **Threshold Configured In:** <HP Business Availability Center Root Directory>\conf\pmconfig.properties You can edit these settings in the properties file: ➤ **MAX_ROWS_PER_PARTITION.** The optimal number of rows per partition that PM strives to create. ➤ **WARN_ROWS_PER_PARTITION.** The number of rows in the partition that generate a warning. ➤ **ERROR_ROWS_PER_PARTITION.** The number of rows in the partition that generate an error.

Application Engines/Dashboard Engine

Monitor Display Name	Purpose
BLE Online Monitor	Monitors BLE Online calculations. **Included Measurements:** ➤ **Size of Model.** Percentage of model size relative to the maximum capacity. ➤ **DB Availability.** Verifies connection to the database ➤ **Bus Connectivity.** Verifies connection to the Bus. ➤ **Persistency.** Indicates the number of failures in saving persistency data. ➤ **Calculation Duration.** Average calculation time. **Threshold Configured In:** Infrastructure Settings. To access, go to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** and search under **System Health** or the applicable component application.
Dashboard BLE Plug-in	Searches for unexpected behavior, displayed as instances of ERROR, in **bam.ble.plugin.log.** **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.
Dashboard Rules	Searches for unexpected behavior, displayed as instances of ERROR, in **bam.app.rules.log**. **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.

Monitor Display Name	Purpose
Repositories	Searches for unexpected behavior, displayed as instances of ERROR, in **repositories.log**. **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.
Repositories Upgrade	Searches for unexpected behavior, displayed as instances of ERROR, in **repositories.upgrade.log**. **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.

Application Engines/SLM Engine

Monitor Display Name	Purpose
BLE Offline Tasks	Indicates whether the time taken to perform the SLM tasks took longer than the time allotted in Infrastructure Settings. **Included Measurements:** ➤ **Delayed Tasks.** Shows whether there are delayed or failed SLM calculation tasks. ➤ **Cycle Time.** Shows the percentage of the overall measurement period used to complete calculation of ongoing SLM tasks. **Threshold Configured In:** Infrastructure Settings. To access, go to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** and search under **System Health** or the applicable component application.

Monitor Display Name	Purpose
BLE Offline Monitor	Monitors BLE Offline calculations. **Included Measurements:** ➤ **DB Availability.** Verifies connection to the database. ➤ **Bus Connectivity.** Verifies connection to the Bus. ➤ **Persistency.** Indicates the number of failures in saving persistency data. ➤ **Max Task Duration.** Displays the duration of the longest task over the time configured in the Infrastructure Settings, indicating whether or not the SLM calculation is too slow. ➤ **Data Stream Fuse Violations.** Indicates performance problems due to the amount of data queried for SLM calculations. **Threshold Configured In:** Infrastructure Settings. To access, go to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** and search under **System Health** or the applicable component application.
SLM Logic Monitor	Searches for unexpected behavior, displayed as instances of unexpected result, in **slm.rules.log**. **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.

Application Engines/Reports DB Aggregator

Monitor Display Name	Purpose
DB Aggregator	Indicates whether the time to perform the DB Aggregation task took longer than the time configured in Infrastructure Settings. **Included Measurements:** ➤ **Delayed Tasks.** Displays whether delayed or failed tasks are found. ➤ **Cycle Time.** Shows the percentage of the overall measurement period used to complete aggregation calculations. **Threshold Configured In:** Infrastructure Settings. To access, go to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** and search under **System Health** or the applicable component application.
Validator	Responsible for the creation of DB Aggregation and SLM tasks. **Included Measurements:** ➤ **Validation Time.** Checks whether validation ran within the time frame defined in the Offline Aggregation settings. **Threshold Configured In:** Infrastructure Settings. To access, go to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** and search under **System Health** or the applicable component application.
Scheduler	Schedules when the DB Aggregator and SLM tasks are performed. **Included Measurements:** ➤ **Threads Alive.** Checks for active threads in the offline aggregation scheduler.

Application Engines/CDM

Monitor Display Name	Purpose
Adapters Framework	Searches for unexpected behavior, displayed as instances of ERROR, in **bam.shared.log.** **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.

Modeling/CMDB

Monitor Display Name	Purpose
Model Objects Quota and Count	Compares current CI count with the CI quota. **Threshold Configured In:** Infrastructure Settings. To access, go to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** and search under **System Health** or the applicable component application.
TQL Quota and Count	Compares current TQL count with the TQL quota. **Threshold Configured In:** Infrastructure Settings. To access, go to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** and search under **System Health** or the applicable component application.
Oversized TQLs	Displays TQLs that are larger than the size permitted by the configured threshold. **Threshold Configured In:** Infrastructure Settings. To access, go to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** and search under **System Health** or the applicable component application.

Monitor Display Name	Purpose
Availability and Performance	Checks system availability and response time. **Included Measurements:** ➤ **Run AdHoc TQL.** Checks how long the Run AdHoc TQL operation takes. ➤ **Load ClassModel.** Checks how long the Load ClassModel operation takes. **Threshold Configured In:** Infrastructure Settings. To access, go to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** and search under **System Health** or the applicable component application.
DB - Could not reset timeout because the object is not monitored	Searches for Couldn't reset timeout because the object isn't monitored in **cmdb.log.** **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.
DB - Failed to borrow object from pool	Searches for Failed to borrow object from pool in **cmdb.log.** **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.
DB - Failed to create a connection	Searches for Failed to create a connection for in **cmdb.log.** **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.
Notification - Cannot Publish	Searches for cannot publish in **cmdb.log.** **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.

Monitor Display Name	Purpose
Notification - Cannot get notifications from the BUS	Searches for error occurred during receive of JMS message in **cmdb.log.** **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.
Performance - Request Timeout	Searches for Request Timeout in **cmdb.log.** **Threshold Configured In:** SiteScope For details, see "Log File Monitor Overview" in *Using System Availability Management*.

Modeling/Viewing System

Monitor Display Name	Purpose
All Symbols Quota and Count	Compares current symbols count with symbols quota. **Threshold Configured In:** Infrastructure Settings. To access, go to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** and search under **System Health** or the applicable component application.

Monitor Display Name	Purpose
Views Quota and Count	Compares current views count with views quota. **Threshold Configured In:** Infrastructure Settings. To access, go to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** and search under **System Health** or the applicable component application.
Oversized Views	Checks for views that are larger than threshold configured in Infrastructure Settings. **Threshold Configured In:** Infrastructure Settings. To access, go to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** and search under **System Health** or the applicable component application.

Data Collectors

BPM Data Collector

Monitor Display Name	Purpose
BPM Last Ping Time	Reports time of most recent ping performed from BPM data collectors. **Threshold Configured In:** Infrastructure Settings. To access, go to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** and search under **System Health** or the applicable component application.
BPM Last Reported Data Time	Measures last reported time of data received from BPM data collectors. **Threshold Configured In:** Infrastructure Settings. To access, go to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** and search under **System Health** or the applicable component application.

SiteScope Data Collector

Monitor Display Name	Purpose
SiteScope status on <SiteScope instance>	Measures the overall status of the SiteScope data collector. **Included Measurements:** ➤ **Last Heartbeat.** Indicates the time of the most recent sample received from SiteScope that indicates the basic availability (i.e. - heartbeat) of the system. ➤ **Health Status.** Indicates the status of the SiteScope Health group, and number of monitors in the group with **error** status. **Note:** Both measurements are monitored only if using SiteScope version 9.0 or higher. If a previous version is installed, only the **Last Heartbeat** measurement is monitored. **Threshold Configured In:** Infrastructure Settings. To access, go to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** and search under **System Health** or the applicable component application.

Discovery Probe Data Collector

Monitor Display Name	Purpose
Discovery Probe status on <Discovery Probe instance>	Receives Discovery tasks from the server, dispatches them, and sends the results back to the CMDB through the server. **Included Measurements:** ➤ **Last Report Time.** The most recent report time. ➤ **Amount of Reported CIs.** The number of CIs reported by the probe. ➤ **Last Access Time.** The most recent time the probe was accessed.

RUM Data Collector

Monitor Display Name	Purpose
RUM Status on <RUM Engine Instance Name>	Displays the aggregated status of the Real User Monitor data collector. **Included Measurements:** ➤ **RUM Engine**. Aggregated status of the Real User Monitor engine monitors. ➤ **RUM Probe IP**. Aggregated status of the Real User Monitor probe with the specified IP address. Each probe has its own entry. ➤ **Database.** Aggregated status of Real User Monitor internal DB monitors. ➤ **Samples to Business Availability Center server.** Aggregated status of the Real User Monitor samples sent to HP Business Availability Center. **Threshold Configured In:** Real User Monitor internal configuration. **Note:** If the Real User Monitor data collector's status is problematic, refer to the Real User Monitor web console for troubleshooting. For details, see "Monitoring the Health of HP Real User Monitor Components" in the *Real User Monitor Administration* PDF.

7

System Health User Interface

This chapter includes the screens and dialog boxes that are part of the System Health user interface.

Important: If you do not deploy the new System Health interface, your system defaults to the Legacy System Health application. For details on Legacy System Health, see "Legacy System Health" on page 187.

System Health Setup Wizard

Description	Enables you to establish remote connectivity to the HP Business Availability Center and database servers for full monitoring. **To Access:** Click **Admin** > **Platform** > **Setup and Maintenance** > **System Health.** **Notes:** ➤ To enable configuring the System Health application, the System Health Setup Wizard opens automatically upon the first access to the application after it has been installed. For subsequent users and user instances the wizard does not open automatically. ➤ You can also access the System Health Setup Wizard by performing either Full Model Synchronization or Soft Synchronization. Soft Synchronization only generates the Wizard if changes were made to the System Health model.
Important Information	If you do not enter remote connection details for the server, System Health only retrieves information on monitors that do not require remote connectivity. The left pane of the System Health Setup Wizard indicates which stage of the wizard you are currently working with.
Additional Links	"System Health Setup Wizard Overview" on page 99, "Deploy and Access System Health" on page 108, "System Health Monitors" on page 123.
Wizard Map	The System Health Setup wizard contains: Servers Remote Setup Page > Databases Remote Setup Page > Recipients Setup Dialog Box

Servers Remote Setup Page

Description	The first step of the System Health Setup Wizard. Enables you to create a remote connection to HP Business Availability Center servers for System Health to monitor.
Important Information	You can configure different settings for each server, or apply the same settings to all servers. You must configure the remote connection details for the server in order for System Health to run all of the server's available monitors. If you do not provide remote connection details for the server, the monitors do not communicate with the server, rendering their information unavailable.
Additional Links	"System Health Setup Wizard Overview" on page 99
Wizard Map	The System Health Setup Wizard contains: **Servers Remote Setup Page** > Databases Remote Setup Page > Recipients Setup Dialog Box

The Servers Remote Setup Page includes the following elements (listed alphabetically):

GUI Element	Description
	Click to show descriptions of the Remote connection details fields.
	Click to select all, clear all, or invert your selection in the server list.
Apply	Click to apply configurations for the selected server.
Encoding	Indicates the encoding used by the server. **Example:** Cp1252, UTF-8

GUI Element	Description
Login	Enter login name used when accessing the operating system running on the server. The user whose login name is entered must have the appropriate permission level for the monitors to run on the server. The format for entering information into this cell is **DOMAINNAME\login**.
Method	Select the method of communication for how to connect to the HP Business Availability Center components. **Example:** NetBIOS, SSH
OS Type	Enter the Operating System running on the server. **Example:** Windows, UNIX **Note:** This field is only visible if System Health does not identify an operating system on the server.
Password	Enter password used when accessing the operating system running on the server. The user whose password is entered must have the appropriate permission level for the monitors to run on the server.

Databases Remote Setup Page

Description	The second step of the System Health Setup Wizard. Enables you to create a remote connection to databases for System Health to monitor.
Important Information	You can configure different settings for each server, or apply the same settings to all servers. You must configure the remote connection details for the server in order for System Health to run all of the server's available monitors. If you do not provide remote connection details for the server, the monitors do not communicate with the server, rendering their information unavailable.

Additional Links	"System Health Setup Wizard Overview" on page 99
Wizard Map	The System Health Setup Wizard contains: Servers Remote Setup Page > **Databases Remote Setup Page** > Recipients Setup Dialog Box

The Databases Remote Setup Page includes the following elements (listed alphabetically):

GUI Element	Description
	Click to show descriptions of the Remote connection details fields.
	Click to select all, clear all, or invert your selection in the server list.
Apply	Click to apply configurations for the selected database.
Encoding	Indicate the encoding used by the server running the database. **Example:** Cp1252, UTF-8
Initialize Shell Environment	Optionally, enter any shell commands to be executed at the beginning of the session. Separate multiple commands with a semicolon (;). This option specifies shell commands to be executed on the remote machine directly after a Telnet or SSH session has been initiated.
Login	Enter login name used when accessing the operating system running on the server on which the database is installed. **Note:** The format for entering information into this cell is **DOMAINNAME\login**.
Login Prompt	The prompt output when the system is waiting for the login to be entered. **Default:** login:

GUI Element	Description
Method	Select the method of communication for how System Health speaks to the database. **Example:** NetBIOS, SSH
OS Type	Enter the Operating System running on the server. **Example:** Windows, UNIX **Note:** This field is only visible if System Health does not identify an operating system on the server.
Password	Enter password used when accessing the operating system running on the server on which the database is installed.
Password Prompt	The prompt output when the system is waiting for the password to be entered. **Default:** password:
Prompt	The prompt output when the remote system is ready to handle a command. **Default: #**
Secondary Prompt	Optionally, enter the secondary prompts if the telnet connection to the remote server causes the remote server to prompt for more information about the connection. Separate multiple prompt string by commas (,).
Secondary Response	Optionally, enter the responses to any secondary prompts required to establish connections with this remote server. Separate multiple responses with commas (,).

Recipients Setup Dialog Box

Description	The third and final step of the System Health Setup Wizard. Enables you to configure recipients to receive predefined System Health alerts via e-mail.
Important Information	You can click a recipient's name in the recipient list pane to edit their details.
Wizard Map	The System Health Setup Wizard contains: Servers Remote Setup Page > Databases Remote Setup Page > **Recipients Setup Dialog Box**

The Recipients Setup Dialog Box contains the following elements:

GUI Element	Description
	Click to display descriptions of the Recipient Details fields.
BAC Databases	Select to receive alerts on status of HP Business Availability Center Databases.
BAC servers, services, and applications	Select to receive alerts on status of HP Business Availability Center servers, services, and applications.
Create	Adds the specified recipient to the recipient list pane.
Email	Enter the recipient's email address.
Mediators	Select to receive alerts on status of HP Business Availability Center Mediators and Load Balancers.
Name	Enter the recipient's name.

System Health Dashboard

Description	Enables you to view, in a dashboard view, HP Business Availability Center components and their status, including information on the properties and monitors associated with the components. **To Access:** Click **Admin** > **Platform** > **Setup and Maintenance** > **System Health.**
Important Information	This is the default display in the System Health interface. The Dashboard consists of the Left Pane and the Right Pane.
Additional Links	"Deploy and Access System Health" on page 108 "System Health Setup Wizard" on page 154 "System Health Displays" on page 101

Left Pane

Description	Displays a map of the databases, servers, data collectors, and mediators and load balancers (if they exist for your deployment) on HP Business Availability Center, and a toolbar of action buttons. **To Access:** Click the **Dashboard** tab on the System Health interface. This is the default view when accessing System Health.
Important Information	The status of the components is indicated by the color of the box surrounding the icon and the accompanying symbol.
Useful Links	"System Health Displays" on page 101

Right Pane

Description	Displays information on components selected in the Left Pane. **To Access:** Click the Dashboard tab on the System Health interface.
Important Information	The Right Pane consists of the Monitors Table and the General Table. The Monitors table contains information about the monitors and subcomponents on the highlighted component in the Left Pane. The General table contains information about the properties of the highlighted server in the Left Pane.
Useful Links	"System Health Displays" on page 101

Monitors Table

Description	Contains information on the monitors running on the selected component in the System Health Dashboard. Click the arrows in the header to expand or collapse.
Important Information	Monitors are listed either individually or in groups. The groups correspond to the components that are within the highlighted object in the left pane. You can choose which columns are to be visible by clicking on the table options button  above the vertical scrollbar in the table. The displayed monitors correspond to the component or subcomponent selected in the Map of HP Business Availability Center System and Components. The monitors are described in the table's other columns and in the **Monitor Details** pane. You can view more details about the System Health monitors on the SiteScope application by clicking the **SiteScope** link at the top of the System Health interface.
Useful Links	"HP Business Availability Center Components" on page 121

The Monitors Table includes the following elements (listed alphabetically):

GUI Element	Description
	Click to select GUI Elements to be visible in the table, enable horizontal scrolling in the table, and pack all columns to return columns to their default width in the table.
	Click to disable the selected monitor.
	Click to reactivate the selected monitor's schedule.

GUI Element	Description
	Click to run the selected enabled monitor immediately.
	Click to expand the list of monitors to list all monitors and measurements for that object. This is the default view.
	Click to collapse the list of monitors to display only the monitors and hide the monitor measurements.
	Click to refresh the list of monitors to display the latest status for the monitors.
	Indicates an individual monitor that is running on the selected component.
	Indicates a group of monitors that are running on the selected component.
Last Updated	Indicates the last time that the monitor ran.
Monitor Details	Lists the **Description** and result of the selected monitor. A monitor instance could produce a text string or a numerical value as its result, or both. Depending on the result of the monitor, that result is displayed in either the **Additional Information** field for a text string result or **Value** field for numerical results, or both.
Monitor/Group Name	Lists the name of the monitor or subcomponent running on the component.
Status	Indicates the monitor or monitor group's status. The monitor or monitor group's status is indicated by a colored ball icon.

General Table

Description	Contains information about the selected server in the System Health Dashboard. Click the arrows in the header to collapse and expand.
Important Information	You can choose which GUI Elements are to be visible by clicking on the table options button  above the vertical scrollbar in the table. This table appears only when a server is selected.

The General Table includes the following elements (listed alphabetically):

GUI Element	Description
	Click to select GUI Elements to be visible in the table, enable horizontal scrolling in the table, and pack all columns to return columns to their default width in the table.
Property Name	Lists the properties associated with the selected component, such as the IP Address, build number, and operating system type.
Value	Lists the value of the specified property.

Inventory Tab

Description	Displays the status of the servers and their respective components that appear on the System Health Dashboard in table format. Enables you to compare the performance of servers of the same type and to view a status in a flat view versus the hierarchal view in the Dashboard. **To Access:** Click the Inventory tab on the System Health interface.
Important Information	In addition to the monitors and components displayed on the System Health Dashboard, the tables contain the following fields: ➤ **Name.** The name of the server. ➤ **Type.** The type of server (appears only for Gateway and Processing server tables). ➤ **Status.** The overall status of the machine, indicated by a colored icon. The monitors are described in the **Monitor Details** pane.

Gateway Machines Table

Description	Contains information about the Gateway machines being monitored by System Health, and their subcomponents.
Important Information	Click the arrows in the header to expand or collapse the table. The subcomponents' status is indicated by a colored ball icon. You can choose which components and subcomponents you want to appear in the table by clicking on the table options button  above the vertical scrollbar in the table. You can also use the table options button to enable horizontal scrolling and to pack all columns, returning the columns to their default width in the table. The subcomponents' details appear in the <Subcomponent Name> Details Table. **Note:** The cell names indicate the component or subcomponent depicted on the System Health Dashboard.
Useful Links	"System Health Displays" on page 101 "HP Business Availability Center Components" on page 121

Processing Machines Table

Description	Contains information about the processing machines being monitored by System Health, as well as the subcomponents contained therein.
Important Information	Click the arrows in the header to expand or collapse the table. The subcomponents' status is indicated by a colored ball icon. You can choose which components and subcomponents you want to appear in the table by clicking on the table options button  above the vertical scrollbar in the table. You can also use the table options button to enable horizontal scrolling and to pack all columns, returning the columns to their default width in the table. The subcomponents' details appear in the <Subcomponent Name> Details Table. **Note:** The cell names indicate the component or subcomponent depicted on the System Health Dashboard.
Useful Links	"HP Business Availability Center Components" on page 121

<Subcomponent Name> Details Table

Description	Contains information about the specific component or subcomponent highlighted in the Gateway Machines Table or the Processing Machines Table.
Important Information	The subcomponents' details are indicated by a either a colored icon, or, where applicable, the subcomponent's value in the color indicating its status. The cell headings correspond to the monitors running on the selected component, in addition to the Name and Status headings, which connote the name of the machine and its overall status, respectively. You can choose which monitors you want to appear in the table by clicking on the table options button  above the vertical scrollbar in the table. The **Monitor Details** pane provides additional information on the selected monitor in the <Subcomponent Name> Details Table.
Useful Links	"Monitors Table" on page 162

Toolbar

Description	Enables you to: ➤ Customize the display of the HP Business Availability Center components. ➤ Perform actions on the HP Business Availability Center components. ➤ Perform management operations on the HP Business Availability Center components. ➤ Synchronize the status and model of the HP Business Availability Center components.
Important Information	Buttons that customize the display of the HP Business Availability Center components appear only on the System Health Dashboard. All other buttons appear on both the System Health Dashboard and the Inventory Tab.
Useful Links	"Service Manager Dialog Box" on page 174; "Backup Server Setup Window" on page 175; "Process Manager Dialog Box" on page 176; "Quick Report Screen" on page 180

Dashboard Customization Buttons

The Dashboard Customization Buttons enable you to customize the appearance of the components on the System Health Dashboard. They appear only on the System Health Dashboard.

The Dashboard Customization Buttons are:

GUI Element	Description
	Click to highlight a component in the System Health Dashboard. **Note:** This is the default setting upon entering the System Health Dashboard.
	Click to pan the System Health Dashboard.

GUI Element	Description
	Click to zoom on a specific area of the System Health Dashboard. You zoom by holding down the left click button on your pointer. Move the pointer down to zoom in; move the pointer up to zoom out.
	Click to navigate between components of the dashboard. You click the Navigation button and then click a line connecting two components or subcomponents. Depending on where on the line you click, the cursor is led to either the original or endpoint component, whichever is further.
	Click to fit all open components and subcomponents into the visible area.
	Click to undo your previous action and go back to the previous Left Pane display. **Note:** This button is enabled only if you have generated more than one view within the Left Pane.
	Click to redo an action that has been undone with the undo  button. **Note:** This button is only enabled if you have generated more than one view within the Left Pane, and are not currently resting on the most recent view.
	Click to realign Left Pane components.

GUI Element	Description
	Click to return the System Health Dashboard to its default view. This includes closing open components and realigning component boxes to their original state.
	Click for an overview map of all the component boxes in the Left Pane. The Overview Map appears in a separate window, with blue lines denoting the boundaries of the Left Pane. **Note:** You cannot perform other functions on the System Health Dashboard while the Overview Map is open.

Action Buttons

The Action Buttons enable you to perform actions on your HP Business Availability Center components. They appear on both the System Health Dashboard and the Inventory Tab.

The Action Buttons are:

GUI Element	Description
	Click to open the Service Manager window. This option enables you to move backend services from one server to another of the same type, if the server machine is not functioning properly, requires downtime for servicing, or is overloaded. **Note:** You must have more than one server of the same type configured in your HP Business Availability Center environment for this button to be enabled.

GUI Element	Description
	Click to define a backup server in case the current server is not functioning properly or requires downtime for servicing. **Note:** You must have more than one server of the same type configured in your HP Business Availability Center environment for this button to be enabled.
	Click to stop or start processes on specific servers, for maintenance purposes or in case these processes display a problematic status on the System Health Dashboard or the Inventory Tab.

Information Buttons

The Information Buttons enable you to retrieve information on your HP Business Availability Center components. They appear on both the System Health Dashboard and the Inventory Tab.

The Information Buttons are:

GUI Element	Description
	Click to receive quick reports on data over the past 24 hours in the selected component.
	Click to export a report containing a snapshot of the System Health monitors and HP Business Availability Center components' current status to a .csv file.
	Click to receive a .zip file containing log files on a specific server. **Note:** You must select a server component on the dashboard for this button to be enabled.

Synchronization Buttons

The Synchronization Buttons enable you to synchronize the status and model of the HP Business Availability Center components. They appear on both the System Health Dashboard and the Inventory Tab.

Important: If an HP Business Availability Center component was down while synchronization was performed during the System Health Setup Wizard, System Health may not have configured the full monitoring solution onto any component that was down during the wizard process. To ensure that this does not happen, it is recommended that all components are up and running during the System Health configuration and while performing a Soft or Full Model Synchronization.

The Synchronization Buttons are:

GUI Element	Description
	Click to refresh and retrieve the current status of the component without running the component's monitors.
	Click to update System Health with any changes in the System Health model. If required, the System Health Setup Wizard is generated for the area of System Health to which the changes apply.
	Click to reset the System Health configuration, including reset of all monitors. Full Model Synchronization resets the System Health configuration and erases all of the monitors' history either in SiteScope or HP Business Availability Center, depending on the System Health deployment method you chose. For details on deploying System Health, see "Deploy and Access System Health" on page 108. **Note:** Clicking this button returns you to the System Health Setup Wizard.

Service Manager Dialog Box

Description	Enables you to move backend services from one server to another of the same type, in case the server machine is not functioning properly, requires downtime for servicing, or is overloaded. **To Access:** Click the **Service Manager** button on the toolbar in either the System Health Dashboard or the Inventory Tab.
Important Information	You can move services from a server only to another server of the same HP Business Availability Center type. You cannot move services from or to an external machine (such as UCMDB). When automatic failover moves processes to the backup machine, it may only move part of a service group, causing System Health to display the same service group on two different servers.
Useful Links	"Understanding Service Reassignment" on page 106

The Service Manager Dialog Box includes the following elements (listed alphabetically):

GUI Element	Description
Execute	Click to move the customer service from one server to another.
Operation Status	Displays the status of the performed operation.
Select Operation	Select the service you want to move.
Select Source Machine	Select the machine from which you want to move the service.
Select Target Machine	Select the machine to which you want to move the service.

Backup Server Setup Window

Description	Enables you to define a Backup server to run your HP Business Availability Center server components in case the server machine is not functioning properly or requires downtime for servicing. **To Access:** Click the **Backup Server Setup** button on the System Health Dashboard toolbar.
Important Information	This button is enabled only if you have configured more than one server of the same HP Business Availability Center type. You must click the **Enable Automatic Failover** box for the backup server to take effect. External machines, such as UCMDB, cannot be defined as a backup machine.
Useful Links	"Move Backend Services" on page 116

The Backup Server Setup Window includes the following elements (listed alphabetically):

GUI Element	Description
Enable Automatic Failover	Select to activate the selected server as the backup server.
Execute	Click to define the selected server as the backup server.
Operation Status	Displays the status of the operation performed.
Select Backed-up Server	Select the server to be backed up.
Select Backup Server	Select the backup server.

Process Manager Dialog Box

Description	Enables you to stop or start processes on specific servers, in case these processes display a problematic status on the System Health Dashboard or the Inventory Tab, or the processes require maintenance. **To Access:** Click the **Process Manager** button on the toolbar on either the System Health Dashboard or the Inventory Tab.
Important Information	You can select multiple processes in one of the following ways: ➤ Press the CTRL key while selecting additional processes. ➤ Press and hold the SHIFT key while pressing the up or down cursor buttons on the keyboard.
Useful Links	"Manage BAC Processes" on page 119

The Process Manager Dialog Box includes the following elements (listed alphabetically):

GUI Element	Description
	Icon displayed next to the process to indicate the selected process is running.
	Icon displayed next to the process to indicate the selected process was started and is not yet running.
	Icon displayed next to the process to indicate the selected process was stopped.
	Icon displayed next to the process to indicate the selected process is currently being stopped.
	Icon displayed next to the process to indicate the selected process was launched.
	Icon displayed next to the process to indicate the selected process' status is unknown.
Operation Status	Displays the status of the operation performed.

GUI Element	Description
Refresh	Click to refresh process statuses. **Note:** A stopped process appears in red.
Select Process(es)	Select the process you want to stop or start. **Note:** You can select multiple processes by holding down the CTRL button while selecting processes.
Select Server	Select the server on which you want to start or stop the processes.
Start	Click to start the selected processes.
Start All	Click to start all of the processes in the **Select Process(es)** window.
Stop	Click to stop the selected processes.
Stop All	Click to stop all of the processes in the **Select Process(es)** window.

HP Business Availability Center Processes

The following table includes the processes that run on the HP Business Availability Center servers (listed alphabetically):

GUI Element	Description
CMDB Process	A process that runs on the CMDB database that stores all the configuration item data. It does not always run and depends on your HP Business Availability Center deployment. **Process name:** cmdb
Data Upgrade	Enables transferring of data from a previous version of HP Business Availability Center to a newer version. **Process name:** DataUpgrade
Database Loader	Runs the component on the server which loads the data into the database. **Process name:** mercury_db_loader

GUI Element	Description
E-mail Reports	Sends HP Business Availability Center reports via e-mail to specified recipients. **Process name:** EmailReportsMdrv
HP Domain Manager	Runs the process which is responsible for all the bus processes in all HP Business Availability Center servers. **Process name:** DomainManager
LDAP	Runs queries and modifications for directory services. **Process name:** slapd
MercuryAS	Runs the JBoss Application Server, which runs the access to all HP Business Availability Center applications. **Process name:** MercuryAS
Message Broker	Enables the transference of a message from the formal messaging protocol of the sending machine to the formal messaging protocol of the receiving machine. **Process name:** MessageBroker
Offline Engine	Runs the engine which controls the offline components of the HP Business Availability Center system. **Process name:** mercury_offline_engine
Online Engine	Runs the engine which controls the online components of the HP Business Availability Center system. **Process name:** mercury_online_engine
Partition Manager	Runs the Partition Manager to create new or purge old partitions in the profile database, as necessary. **Process name:** topaz_pm_process

GUI Element	Description
TMU	Checks the HP Business Availability Center license every five minutes and updates the database accordingly. **Note:** This process can only be run on a Windows server. **Process name:** TMU
WDE	Runs the Web Data Entry component of the Gateway Server, which receives data from all registered data collectors and publishes the data to all HP Business Availability Center engines. **Process name:** mercury_wde
Webserver Guard	Ensures that the webserver is continually running. **Process name:** MercuryWSGuard
IIS Web Server	IIS Web server process. This process runs if the server is running on IIS. **Process name:** inetinfo
IPlanet Web Server	IPlanet Web server process. This process runs if the server is running on IPlanet. **Process name:** webservd
Apache Web Server	Apache Web server process. This process runs if the server is running on Apache. **Process name:** httpd

Quick Report Screen

Description	Displays reports on data from all monitors which monitor the component selected on the Dashboard Tab. **To Access:** Click the **Quick Report** button on the toolbar on either the System Health Dashboard or the Inventory Tab.
Important Information	This is a display of historical information from the past 24 hours on monitors deployed on HP Business Availability Center components. The following links appear in the window, which enable the user to view specific information on the monitors: ➤ Table Format: ➤ Error List: ➤ Warning List: ➤ Good List: For details on the information these links display, see below.
Useful Links	"Display a Quick Report" on page 120; "SiteScope Quick Report" on page 1263 in *System Availability Management*.

The Quick Report Dialog Box includes the following elements (listed alphabetically):

GUI Element	Description
<Error List>	Lists the monitor runs that retrieved an **error** status based on the thresholds configured for the monitor.
<Good List>	Lists the monitor runs that retrieved a **good** status based on the thresholds configured for the monitor.
<Graphs>	Displays the monitor groups' output in graph format.
<Table>	Displays the monitor groups' output in table format.

GUI Element	Description
<**Warning List**>	Lists the monitor runs that retrieved a **warning** status based on the thresholds configured for the monitor.
Measurement Summary Table	Explains the measurements that are displayed on each HP Business Availability Center monitor.
Uptime Summary Table	Displays the percentage of uptime each HP Business Availability Center monitor experienced over a select time period.

Map of HP Business Availability Center System and Components

Description	Depicts the various HP Business Availability Center components measured by System Health. **To Access:** Click the **Dashboard** tab on the System Health interface.

Important Information	**Database** components appear on the left side of the pane. **HP Business Availability Center Server** components appear in the left-middle of the pane. **Load Balancer** components appear in the right-middle of the pane. **Note:** When System Health is deployed in a secured environment, Reverse Proxy components appear with the Load Balancer components. **Data collector** components appear on the right side of the pane. The components' status is indicated by a colored icon and indicator sign. The monitors that run on components and subcomponents appear in the Monitors Table in the Right Pane.
Useful Links	"System Health Displays" on page 101 "Monitors Table" on page 162

Icons and Buttons

The following are the icons and buttons on the Map of HP Business Availability Center System and Components:

GUI Element	Description
	Click to expand the component and view its subcomponents.
	Click to hide the subcomponents contained within the selected component.
	Icon indicating a Database Server.
	Icon indicating a Database.

GUI Element	Description
	Icon indicating a Gateway Server.
	Icon indicating a Processing Server.
	Icon indicating a group of processes.
	Icon indicating a group of server monitors.
	Icon indicating a Bus component.
	Icon indicating a logical group. **Example:** Alerts Engine
	Icon indicating an application. **Example:** Dashboard
	Icon indicating a group of applications.
	Icon indicating a service. **Example:** Service Level Management Engine
	Icon indicating a group of Business Process Monitor data collectors.
	Icon indicating a group of SiteScopes.
	Icon indicating a group of Discovery Probes.

GUI Element	Description
	Icon indicating a group of Real User Monitor data collectors.
	Icon indicating the flow of data. **Note:** Click the Navigation button  and then click anywhere on an arrow to find the arrow's destination or origin. For details, see "Toolbar" on page 113.

Database Components

The Map of HP Business Availability Center System and Components includes the following HP Business Availability Center database elements (listed alphabetically):

GUI Element	Description
CMDB Database	A central repository for configuration information.
History Database	Used for storage of data, over time, of the CMDB configuration items (CIs).
Management Database	Used to store system-wide and management-related metadata for the HP Business Availability Center environment.
Profile Database	Used to store raw and aggregated measurement data obtained from the HP Business Availability Center data collectors.

HP Business Availability Center Server Components and Processes

The Map of HP Business Availability Center System and Components includes the following HP Business Availability Center server elements (listed alphabetically):

- Alerts Engine
- Applications (Dashboard application, Service Level Management, System Availability Management, and Portal components)

- Applications Engines
- BPMs (Business Process Monitors)
- bus
- CMDB
- CDM
- Dashboard Engine
- Discovery Probes
- modeling
- Portal application (My BAC)
- Processes (for details, see "HP Business Availability Center Processes" on page 177)
- Real User Monitor Engines
- Reports database aggregator
- SAM (System Availability Management - Management of SiteScopes)
- Scheduler (NOA service scheduler)
- Server monitors
- SiteScopes
- SLM (Service Level Management) Engine
- Validator (NOA service validator)
- Verticals (SAP service and Siebel service)

Data Collector Components

The Map of HP Business Availability Center System and Components includes the following HP Business Availability Center data collector elements (listed alphabetically):

GUI Element	Description
BPMs	Displays status of the Business Process Monitor data collectors.
Discovery Probes	Displays status of the Discovery Probes.
RUM Engines	Displays status of the Real User Monitor engines.
SiteScopes	Displays status of the SiteScopes.

8

Legacy System Health

Note to HP Managed Software Solutions customers: HP Operations administers these pages and the interface is hidden from your view.

The System Health page enables high-level HP Business Availability Center administrators to manage the workload of the Data Processing Servers and the services they are running by setting up Automatic Failover or manually reassigning services among servers in response to resource issues or for maintenance purposes.

Important: Legacy System Health is available only if you have not deployed the new System Health interface, either as a stand-alone application or as an embedded part of HP Business Availability Center. For details on deploying the new System Health interface, see "Deploy and Access System Health" on page 108.

Working with the System Health Page

The System Health page enables high-level HP Business Availability Center administrators to monitor the load on the Data Processing Servers in the HP Business Availability Center server architecture and manage the Data Processing Servers—by setting up Automatic Failover or by manually reassigning services from one server to another —to prevent downtime due to insufficient resources on a particular machine or due to required server machine maintenance.

Administrators can also view static information about the machines on which the Gateway Servers are running.

Note:

- For complete details on setting up a high availability deployment of HP Business Availability Center servers, as well as descriptions of all services that run on the Data Processing Server, see "High Availability for HP Business Availability Center" in the *HP Business Availability Center Deployment Guide* PDF.
- Reassigning services from one server to another can also be done using the JMX Console. It is recommended that the JMX Console only be used to reassign services that cannot be reassigned via the System Health page. For details, see "Manually Reassigning Services" in the *HP Business Availability Center Deployment Guide* PDF.

Permissions Required to Access the System Health Page

The System Health page can be accessed by users with Superuser or Administrator permissions.

System Health Page Layout

The System Health page can be viewed by selecting **Admin** > **Platform** > **Setup and Maintenance** > **System Health**. The System Health page is divided into three panes:

- **Servers.** The Servers pane is located on the top left of the page and lists:
  - in the All tab, the names and types of all the installed servers
  - in the Data Processing tab, the names of all the Data Processing Servers, the service configuration for each, and the status of the worst monitored server resource
- **Services.** The Services pane is located on the top right of the page and displays the statuses of all the monitored server resources for the server currently selected in the Servers pane.
- **Management.** The Management pane is located across the bottom of the page and displays the status of tasks that are running or were run during the course of the current Web session.

Understanding Service Reassignment

In typical enterprise environments, the Data Processing Server is split into three standalone servers:

- Modeling Data Processing Server
- Online Data Processing Server
- Offline Data Processing Server

Each server is installed on a separate machine. Each server might also be installed on one or more backup machines.

If a certain Data Processing Server machine is not functioning properly or requires downtime for servicing, administrators can manually reassign the services running on that machine to a different Data Processing Server machine. Administrators can also preconfigure a specific Data Processing Server to automatically fail over to a specific backup machine.

Important: Before manually reassigning services to another server or configuring a server as a backup server for Automatic Failover, ensure that the HP Business Availability Center service is running on that server.

When a service is reassigned via the System Health interface from an active Data Processing Server to a different Data Processing Server, for example a backup server, HP Business Availability Center modifies the setting in the management database that defines the active Data Processing Server. The newly defined server setting in the management database is read by the high availability controller running on the Data Processing Servers. At that point, a process begins whereby HP Business Availability Center stops using the services on the previously active server and begins using the services on the newly active server. This process can take up to several minutes, during which time the system is in downtime.

There are several theoretical scenarios for reassigning services among machines, to manage resource issues or enable server administration. The table that follows illustrates these scenarios by indicating the paths along which services can be reassigned.

Flow Table

	To Full Data Processing Server	To Modeling Data Processing Server	To Online Data Processing Server	To Offline Data Processing Server
From Full Data Processing Server	Yes	Yes	Yes	Yes
From Modeling Data Processing Server	Yes	Yes	No	No
From Online Data Processing Server	Yes	No	Yes	No
From Offline Data Processing Server	Yes	No	No	Yes

Monitoring System Resources on the System Health Page

High-level HP Business Availability Center administrators can use the System Health page to monitor system resource status to identify potential resource issues and take action before the system is adversely affected.

This section includes the following topics:

Viewing Server Architecture

From the All tab in the Servers pane, you can view the names of all the servers that are deployed in the HP Business Availability Center server architecture, and their type (Gateway or Data Processing).

Viewing Data Processing Server Configuration

From the Data Processing tab in the Servers pane, you can view the names of all the Data Processing Servers that are deployed in the HP Business Availability Center server architecture, and their configuration (All services, Modeling, Online, Offline). For details on Data Processing Server configurations, see "High Availability for the Data Processing Server" in the *HP Business Availability Center Deployment Guide* PDF.

In addition, the status of the worst-performing monitored resource is displayed in the Worst Resource column. For details on resource status, see "Understanding Data Processing Server Resource Status" on page 193.

Viewing Data Processing Server Properties

When a specific server is selected from the Data Processing tab in the Servers pane, you can view properties for that server by clicking the **Show Properties** button in the Services pane. The Properties dialog box displays the following properties:

- **Name.** The server name.
- **IP.** The server IP address.
- **Backup server for this server.** If a backup server is configured for the server, the name of the backup server is displayed. Note that this information is displayed even if Automatic Failover has been disabled.
- **This server is a backup for servers.** If the server is configured as a backup server, the names of the severs the server is backing up are displayed. Note that this information is displayed even if Automatic Failover has been disabled.

Understanding Data Processing Server Resource Status

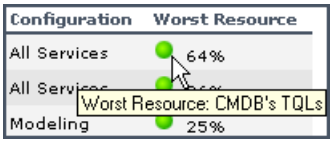
The resource status information that is displayed on the System Health page is based on capacity limit and threshold settings that are preconfigured by HP. These settings can be viewed in the Infrastructure Settings Manager (select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, and select **System Health**).

Warning: Do not modify Capacity Limit settings, as doing so can adversely affect the performance of HP Business Availability Center. If your organization requires modification of these settings, it should be done in coordination with your HP representative.

Types of Resource Status Information

Two types of resource status information are displayed:

- **percentage of capacity limit.** Represents the actual usage of the resource relative to its configured capacity limit. In the example below, the CMDB's TQLs are at 64% of capacity (in this case, 77 TQLs out of a limit of 120).



- **threshold representation of the percentage of capacity limit**. Uses a color-coded icon to express the percentage of the capacity limit, based on the following ranges:

Range	Color Code
<=70% of capacity limit	Green
>70% but <=90% of capacity limit	Yellow
> 90% of capacity limit	Red
No data/No services running	Gray

Resource Status Information in the Servers Pane

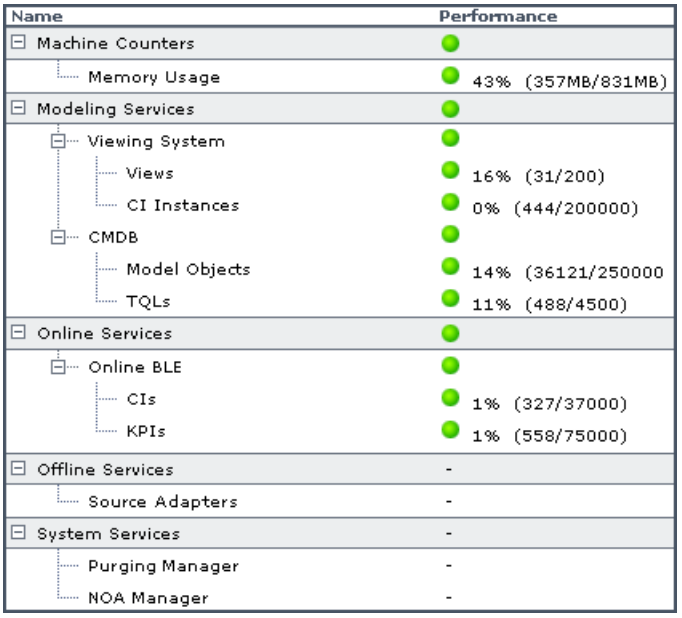
In the Servers pane, you can see the following resource status information:

- for each active server in the list, the percentage of capacity limit and its threshold representation, in the Worst Resource column, indicating the status of the worst-performing resource among all the resources being monitored on that server.
- a tooltip with resource details. Place your mouse pointer over a threshold icon to view information on the specific resource whose status is being reported.

Note: The offline server configuration does not report any resource status information as there are currently no monitored resources for the Offline Data Processing Server.

Resource Status Information in the Services Pane

In the Services pane, you can see a detailed display of all monitored server resources for the server selected in the Servers pane.



Name	Performance
Machine Counters	
Memory Usage	43% (357MB/831MB)
Modeling Services	
Viewing System	
Views	16% (31/200)
CI Instances	0% (444/200000)
CMDB	
Model Objects	14% (36121/250000
TQLs	11% (488/4500)
Online Services	
Online BLE	
CIs	1% (327/37000)
KPIs	1% (558/75000)
Offline Services	-
Source Adapters	-
System Services	-
Purging Manager	-
NOA Manager	-

- The **Name** column displays, per resource group, the services and their monitored resources.
- The **Performance** column displays:
  - for each resource group, a threshold icon indicating the status of the resource group, based on the worst child rule (the parent node inherits the status of its worst child)
  - for each service, a threshold icon indicating the status of the service, based on the worst child rule (the parent node inherits the status of its worst child)

- for each monitored resource, a threshold icon and accompanying percentage indicating the status of the resource, and the numerical representation of the percentage, based on the preset capacity limit for the resource. Note that the capacity limits differ depending on the specific deployment architecture. For example, the capacity limit for CMDB TQLs is lower in a three-server deployment (the CMDB service runs on a Data Processing Server running all services) than it is in a five-server deployment (the CMDB service runs on a dedicated Modeling Data Processing Server).

The table below describes the different resource groups, services, and monitored resources whose status can be monitored from the System Health page. Note that the offline server configuration—which includes offline services and system services—does not report any resource status information as there are currently no monitored resources for the Offline Data Processing Server.

Resource Group	Service	Monitored Resource	Description
Machine Counters (all servers)		Memory Usage	The percentage of memory usage by the **mercury_as** process. In addition, the absolute memory usage and total memory capacity values are displayed. These are taken from the server's operating system.

Resource Group	Service	Monitored Resource	Description
Modeling Services (Modeling Data Processing Server)	**Viewing System**	CI Instances	The number of configuration item (CI) instances in service views that the server can handle simultaneously
		Views	The number of views that the server can handle simultaneously
	CMDB	Model Objects	The number of CMDB model objects (CIs, KPIs, and so forth) that the server can handle simultaneously
		TQLs	The number of Topology Query Language (TQL) queries that the server can handle simultaneously
Online Services (Online Data Processing Server)	**Online BLE**	CIs	The number of configuration items (CIs) with associated KPIs that the server can handle simultaneously
		KPIs	The number of Key Performance Indicator (KPI) objects that the server can handle simultaneously
Offline Services (Offline Data Processing Server)	**Source Adapters**	Resource not monitored. If service is running, the "-" character appears. If service is not running, it does not appear in the table.	Service responsible for adding data collector entities to the CMDB

Resource Group	Service	Monitored Resource	Description
System Services (Offline Data Processing Server)	**Purging Manager**	Resource not monitored. If service is running, the "-" character appears. If service is not running, it does not appear in the table.	Service that handles data purging and partitioning
	New Offline Aggregation Manager	Resource not monitored. If service is running, the "-" character appears. If service is not running, it does not appear in the table.	Service that validates and synchronizes new tasks for the offline aggregator on an hourly or daily basis

Configuring Service Reassignment

High-level HP Business Availability Center administrators can use the System Health page to:

- configure Automatic Failover for the Data Processing Server. For details, see "Configuring Automatic Failover for the Data Processing Server" on page 200.
- manually reassign services to accommodate the need for server machine maintenance. For details, see "Procedure for Manually Reassigning Services" on page 205.

Configuring Automatic Failover for the Data Processing Server

The process of automatically moving services from a primary server to another server is called **Automatic Failover**.

This section includes the following topics:

Automatic Failover Configuration

Automatic Failover for a Data Processing Server to a backup server must be configured. It is not enabled by default.

There are two steps in enabling the Automatic Failover mechanism:

- enable Automatic Failover of primary servers
- configure the backup server for primary servers

To enable Automatic Failover of primary servers:

1 Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, select **High Availability Controller**, and locate the **Automatic Failover Enabled** entry in the High Availability Controller - General Properties table.

2 Click the **Edit** button for **Automatic Failover Enabled.** The Automatic Failover Enabled dialog box opens.

3 Select **true** and click **Save**. The change takes effect immediately.

Note: It is recommended to keep the **Keep Alive Timeout (minutes)** default value of **20.** A lower value may give a false failure alert.

To configure the backup server for primary servers:

1 Select **Admin** > **Platform** > **Setup and Maintenance** > **System Health**.

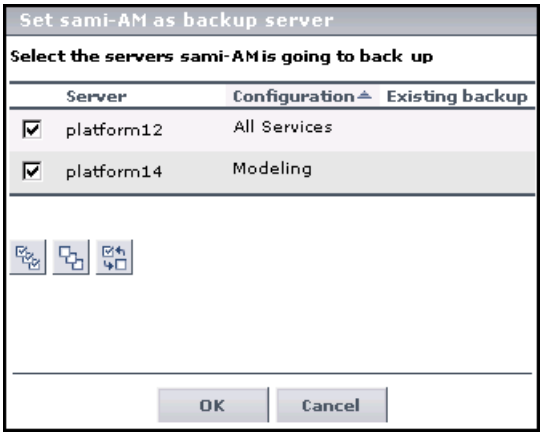
2 In the Servers pane, choose the Data Processing tab. Click the server to be the backup server. Information about the selected server is displayed in the Services pane.

3 In the Services pane, click the Set as **Backup Server** button to define the server as a backup server. The Set as Backup Server dialog box opens with a list of Data Processing Servers.

For each listed server, the following information is displayed:

- **Server.** The server name.
- **Configuration.** The server configuration (All services, Modeling, Online, or Offline)
- **Existing backup.** Lists the backup server currently defined for the servers in the Server list.

4 Select the primary servers that the backup server is to back up and click **OK** to save your selections.



When a primary server exceeds the **Keep Alive Timeout** with no response, Automatic Failover automatically reassigns the services to the predefined backup server. The primary server automatically shuts down its services in order to prevent duplicate services from running.

Note: While Automatic Failover is moving services, a brief period of high CPU usage on the backup server may occur while those services start. CPU usage returns to normal once all services are running.

When the primary server becomes operational, you must manually reassign services to it from the backup server. For details on manually reassigning services, see “Procedure for Manually Reassigning Services” on page 205.

Removing Automatic Failover

Follow the procedure below to stop a server from acting as a backup server for some or all of the servers it is backing up.

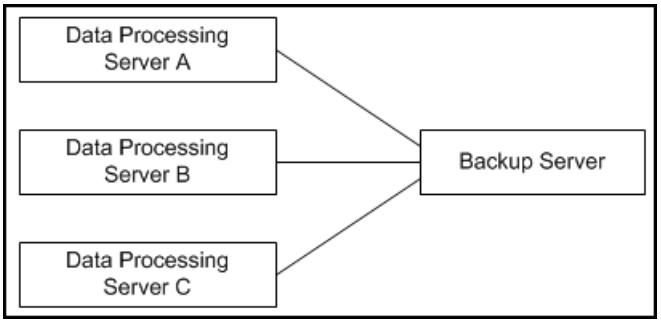
To stop a server from acting as a backup server:

1. Select **Admin** > **Platform** > **Setup and Maintenance** > **System Health**.
2. Choose the **Data Processing** tab In the Servers pane. Click the server that you no longer want to serve as a backup server. Information about the selected server is displayed in the Services pane.
3.  Click the **Set as Backup Server** button in the Services pane to open the Set as Backup Server dialog box.
4. Clear the check boxes beside some or all of the listed servers, as required.
5. Click **OK** to save the settings.

Notes and Limitations

- Automatic Failover is only supported in Data Processing Servers.
- By default, Automatic Failover is not enabled.
- A primary server does not have a default backup server. A backup server must be explicitly defined. If no backup server is defined, Automatic Failover does not try to locate a suitable backup server, even if one is available.
- Each server can have only one backup server.
- Several primary servers can be assigned to the same backup server. Keep in mind, however, that if several primary servers fail simultaneously, the backup server may also fail if it exceeds its performance capacity.
- The backup server cannot have a defined backup server.

- After a primary fails and its services move to a backup, the primary, after it restarts, acts as a backup to the backup server for its original services.



- For the above diagram, when Data Processing Server A fails, its services automatically move to Backup Server. When it returns online, it acts as a backup for its services which are now running on Backup Server. Data Processing Server A, however, is not defined as a backup for Backup Server.
- The Source Adapters service (also known as the CDM service) on the Offline Data Processing Server uses the **<HP Business Availability Center root directory>\CMDB** directory. The CMDB directory must be moved to a separate machine for high availability purposes (that is, configured as a shared directory) to enable success of the Automatic Failover mechanism when backing up the Offline Data Processing Server. For details on configuring the CMDB directory as a shared directory, see "High Availability for the CDM" in the *HP Business Availability Center Deployment Guide* PDF.
- The backup server must have the same operating system as the Data Processing server it backs up. In other words, the active server and its backup server must both be either Solaris or Windows.
- The active server and its backup server must both have the same version of HP Business Availability Center.
- The HP Business Availability Center service must be running on the backup server so that it can poll the database intermittently to know when it receives service assignments.

- If, after enabling Automatic Failover and configuring backup servers, you then disable Automatic Failover, the backup server assignments remain visible in the System Health page.
- When a designated backup server becomes the active server (i.e. - starts running the services of the server it was backing up), an asterisk (*) appears beside the server name in the Servers pane. When the server ceases to act as a backup server (i.e. - no longer runs the services of the server it was backing up), the asterisk is removed.

Procedure for Manually Reassigning Services

When there is a need to manually reassign services from one machine to another (for example, due to a resource issue on a given machine, required server maintenance, or to reassign services to a primary server after its services were automatically moved to a backup server using the Automatic Failover mechanism), follow the procedure below to create and apply server reassignment tasks.

Note: The Source Adapters service (also known as the CDM service) on the Offline Data Processing Server uses the **<HP Business Availability Center root directory>\CMDB** directory. If the CMDB directory has not been moved to a separate machine for high availability purposes (that is, configured as a shared directory), when the Offline Data Processing Server services are manually reassigned to a different server, the CDM service will not function properly until the CMDB directory is manually copied to the new Offline Data Processing Server. For details on configuring the CMDB directory as a shared directory, see "High Availability for the CDM" in the *HP Business Availability Center Deployment Guide* PDF.

To reassign services:

1. In the Servers pane, select the server whose services you want to reassign.
2.  In the Services pane (right pane), click the **Move services as group** button to view the **Move services** context menu.

3 Select one of the below options. The Move Services dialog box opens.

- **Move all services.** Select to move all services from the server to a different server.
- **Move modeling services.** Select to move modeling services from the server to a different server.
- **Move offline services.** Select to move offline services from the server to a different server.
- **Move online services.** Select to move online services from the server to a different server.
- **Move system services.** Select to move system services from the server to a different server.

4 In the Move Services dialog box, select the server to which you want to reassign the selected group of services. Only servers to which the services can be moved are listed.

5 Click **OK** to move the services.

6 Monitor the status of the running tasks from the Status tab.

The Status tab displays all tasks currently running, or that have completed running during the current Web session.

Limitation: If a task does not complete (that is, the reassigned services do not start successfully), the Status tab will continue to display a status message indicating that the task is in progress. Successful reassignment can be verified in the System Health log file, **systemConsole.log**, if the log file is configured to record messages at the INFO level. For details on the log file, see "Log File" on page 207.

System Health Logging and Troubleshooting

Use the following information to troubleshoot issues, as required.

System Health Logging

All server reassignments performed via the System Health page are written to the Audit Log. In addition, messages are written to a log file.

Audit Log

All services reassignments are written to the Audit Log (**Admin** > **Platform** > **Setup and Maintenance** > **Audit Log**).

To view the history of services reassignments, in the Audit Log select the **System Console** context. If required, use the up and down arrows to scroll through the entries.

Log File

Log messages are written to the log file **<HP Business Availability Center root directory>\log\systemConsole.log**. The type of messages is dependent on the level of logging enabled. By default, only errors are written to this log. For details on changing log level, see "Changing Log Levels" in *Reference Information*.

System Health Troubleshooting

Problem: HP Business Availability Center servers installed and running in a distributed architecture appear as unavailable in the Servers pane.

Problem Cause: To determine server availability, HP Business Availability Center pings the servers according to the name registered in the SERVERS table in the database. In certain environments, the host machine performing the ping requires the target machine's IP (and not its machine name), but does not know the IP. Thus, the ping fails and the machine is reported as unavailable.

Solution: Map the names of all HP Business Availability Center server machines (Gateway and Data Processing) to their corresponding IPs in the **C:\WINNT\system32\drivers\etc\hosts** file (path may vary depending on Windows installation) on the Gateway Server machine. If there are multiple Gateway Server machines and/or Gateway Server machines behind a load balancer, perform the above procedure on all machines. Note that the left column is for IP addresses and the right column is for machine names.

9

Audit Log

HP Business Availability Center enables you to view a log of all the actions performed by different users accessing the platform.

Understanding the Audit Log

You use the audit log to keep track of different actions performed by users in the system. You can track according to the following contexts in the audit log:

- **Alert Administration.** Displays actions related to adding, modifying, deleting, enabling and disabling alerts, as well as registering and unregistering alert recipients.
- **CI Status Alert Administration.** Displays actions related to creating alert schemes for a configuration item (CI) status alert.
- **Customer Package Management.** For HP Managed Software Solutions only. Displays actions related to modifying package information such as: package location information, general package properties, Business Process Monitor package properties or SiteScope package properties.
- **Dashboard Administration.** Displays actions related to configurations made in the Dashboard Administration.

- **Data Collector Maintenance.** Displays actions related to removing Business Process Monitors and SiteScopes.
- **Database Management.** Displays actions related to creating, deleting, and modifying users and passwords for profile databases, as well as modifying the status of the Purging Manager.
- **Deleted Entities.** Displays actions related to adding and deleting data collectors from End User Management Administration. These are Business Process profiles, Real User Monitor engines, and SiteScope monitors.
- **Downtime/Event Scheduling.** Displays actions related to creating and modifying downtime and scheduled events.
- **IT World (IT Universe) Configuration.** Displays actions, including editing, updating, and removing CIs and relationship, performed in the IT Universe Manager application.
- **Monitor Administration (Business Process Monitor).** Displays actions related to profile management and configuration, including starting and stopping profiles, adding and deleting transaction monitors, modifying scheduling, defining and modifying hosts, adding and deleting WebTrace addresses, and modifying transaction thresholds.
- **Monitor Administration (Real User Monitor).** Displays actions related to Real User Monitor management and configuration, including the addition and deletion of Real User Monitor probes, servers, and host groups, and the configuration and deletion of pages, transactions, and end users.
- **Monitor Administration (SiteScope).** Displays actions related to profile management and configuration, including starting and stopping profiles, adding and deleting monitors, modifying monitors and groups, editing preferences, and configuring alerts.
- **Notification Template Administration.** Displays actions related to modifying open ticket information, ticket settings, closed tickets, ticket templates, and subscription information: notification types (locations or general messages), and recipients.
- **Permissions Management.** Displays all actions related to assigning permissions, roles, and permissions operations for resources onto users and user groups.

- **Recipient Administration.** Displays actions related to modifying information about the recipients of audit logs.
- **Scheduled Report Administration.** Displays actions related to modifying the reporting method and schedule of reported events.
- **Script Repository.** For HP Managed Software Solutions only. Displays actions related to modifying the type of verification of Business Process Monitor scripts, and verification of subscription information.
- **Service Level Management Configuration.** Displays actions related to service level agreements performed in the Service Level Management application. For a list of the audited actions, see "Using the Audit Log" on page 212.
- **SLA Alert Administration.** Displays actions related to creating, modifying, or deleting SLA alerts.
- **System Console.** Displays all services reassignments performed in the System Health interface to resolve system resource issues.
- **User Defined Reports.** For HP Managed Software Solutions only. Displays actions related to the creation and modification of custom reports.
- **User/Group Management.** Displays actions related to adding, modifying, and deleting users and user groups.
- **View Manager.** Displays actions related to KPIs such as adding a KPI, editing a KPI, and deleting a KPI. Additionally, it displays actions related to changing the **Save KPI data over time for this CI** and the **Monitor changes** options.

Using Filters in the Audit Log

When you select one of the above categories from the Context list, the following information is displayed in the Audit Log table:

- **Modification Date.** Displays the date of the listed action
- **Modified By.** Displays the user who performed the listed action
- **Actions.** Displays a detailed description of the action

Using the Audit Log

You access the audit log from the Audit Log page, available from the Setup and Maintenance menu of Platform Administration.

To use the audit log:

1. Select **Admin** > **Platform** > **Setup and Maintenance** > **Audit Log**. The Audit Log page opens.
2. Select a context using the **Context** filter.
3. Where relevant, select a profile from the list. HP Business Availability Center updates the table with the relevant information.
4. Optionally, click the **Auditing Filters** link and specify filter criteria. The following filters are available:
   - **User.** Specify a user in the system to view actions performed by only that user.
   - **Containing text.** Specify a text string that the action must contain to be displayed.
   - **Start after and End before.** Specify a starting and ending time period to view actions for only that period. Click the **more** button to open the Calendar dialog box where you can select a date.

   Click **OK**. HP Business Availability Center updates the table with the relevant information.
5. If required, use the **Previous Page** and **Next Page** arrows to move through the audit log.

Part III

Data Collection

10

Data Collector Maintenance

Note to HP Managed Software Solutions customers: HP Operations administers these pages and the interface is hidden from your view.

You can perform ongoing maintenance tasks on the data collectors installed with your platform to suit the changing requirements of your organization.

About Data Collector Maintenance

The HP Business Availability Center platform includes installable components that provide data collection capabilities. The Data Collector Maintenance page enables you to manage and maintain the data collectors in your platform.

Note: Data collectors can be installed from the Downloads page in Platform Administration. For details on downloading, see "Downloads" on page 43.

The Data Collector Maintenance page is available in the Data Collection tab of Platform Administration and displays the current data collector instances registered in the management database for each data collector type. The page is divided into tabs representing the following types of data collectors:

- SiteScope
- Business Process Monitor
- Real User Monitor

You use the Data Collector Maintenance page to:

- view a detailed list of all data collectors in your platform
- remove a Business Process Monitor instance
- view a data collector's current properties

You can also link to the administration site of the data collector.

Understanding the Data Collector Maintenance Page

The Data Collector Maintenance page includes the following information, depending on which data collector tab is selected:

- a location filter at the top of the page, which enables you to filter the list of data collectors by host location
- a check box beside each data collector, which must be checked to select the data collector, container, or group for various host management options.
- a list, by host name, of all data collectors registered in the management database for the type selected.

Note: A Business Process Monitor instance is identified by the combination of the **Host Name** and **Location Name**. Both the host name and location name are defined by the user when setting up a Business Process Monitor instance. For details, see "Business Process Monitor Host Page" in the *Business Process Monitor Administration* PDF.

- IP address of the data collector
- the location defined for the SiteScopes and Business Process Monitor instances
- the version, including build number for SiteScope, of the data collector software installed
- the last time the data collector pinged the management database
- a column indicating whether the data collector is removable (for details, see "Removing a Business Process Monitor" on page 218)

- a details button which opens the data collector's information page
- a link to the data collector's administration site, enabling you to perform administrative tasks on the data collector directly from this page

- clear all, select all, and invert selection buttons to clear all selections, select all data collectors, and to invert selection (clear data collectors that were selected and select data collectors that were not selected)

- a **Refresh** button
- an **Export BPM Information** button on the Business Process Monitor tab, which enables you to export information from the Business Process Monitor data collector to a text file.
- a **remove** button, which enables you to remove selected data collectors.

Note: A data collector which has pinged in the last 24 hours is not removable.

Removing a Business Process Monitor

Using the Data Collector Maintenance page to remove a data collector removes it from the management database. This may be required if a specific data collector instance becomes obsolete.

Removing a data collector deletes it only from the management database, not from the profile database. For example, a removed Business Process Monitor instance that was added to a profile at least once, no longer appears in the list of available hosts that is displayed when creating profiles. However, the location of the removed host still appears in different areas of HP Business Availability Center (for example, in reports and filters). If you do not want a removed Business Process Monitor instance to appear in reports, use report filters to remove the location associated with the data collector. For details on configuring report filters, see "Report Filters" in End User Management, and "Configuring Report Filters Globally" on page 229.

HP Business Availability Center enables you to remove only those Business Process Monitor data collectors that are no longer in use if one of the following criteria is met:

- The Business Process Monitor is not associated with any profiles.
- The Business Process Monitor has not pinged the database server hosting the management database for at least 24 hours.

To stop the Business Process Monitor from pinging the database server, you must shut down the Business Process Monitor.

To remove a Business Process Monitor instance:

1 Select **Admin** > **Platform** > **Data Collection**. Choose **Data Collector Maintenance**. The Data Collector Maintenance page opens.

2 If required, filter the list using the **Location** filters to view specific locations from which you want to remove data collector instances.

3 Select the check box for the data collector instance you want to remove, checking the removable column to see if it is removable.

If the Removable column has **No** listed for this instance, you can click the **Information** button to see why the data collector is not removable. A dialog box displaying information on the data collector opens. For details, see "Viewing Data Collector Information" on page 220.

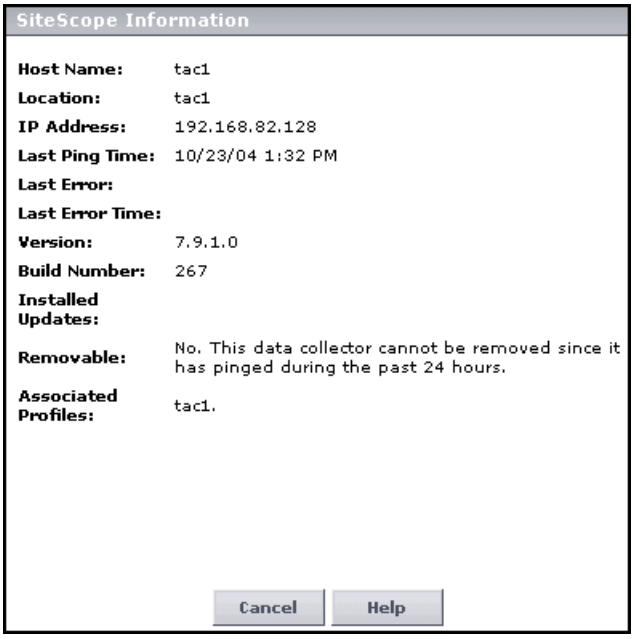
4 Click **Remove**, and confirm that you want to remove the instance(s).

To refresh the list of services:

Click the **Refresh** button at the bottom of the page.

Viewing Data Collector Information

To view more information on a data collector, including an explanation of why the instance is or is not removable, click the **Information** button to open the data collector's Information dialog box.



On the data collector's Information page, the following is displayed:

- The type of data collector.
- The name of the host machine on which the selected data collector is installed.
- The location of the host machine on which the data collector is installed.
- The IP address of the host machine on which the data collector is installed.
- The last time the service pinged the management database.
- The last reported error message, if one exists.
- The time of the last reported error message, if one exists.

- The version number, including build number, of the data collector software.
- A list of the updates that have been installed on the data collector software.
- An indication of whether or not the data collector instance is removable, and if not, why.
- The profiles currently associated with the data collector.

11

Downtime/Event Scheduling

Downtime or other scheduled events can sometimes skew the results of system availability and performance reports. You may want to exclude these periods of time from reports and alerts.

Defining Downtime and Other Influencing Events

You define downtime or a scheduled event that will occur in the future, and HP Business Availability Center excludes data collected during this time interval from its reports. For example, you might want to exclude a recurring maintenance event or a holiday.

Using the Downtime/Event Scheduling page, you can apply a downtime event to multiple profiles. For the defined time interval, you select whether HP Business Availability Center stops sending alerts, stops running the associated profiles, or both.

To define downtime or a scheduled event:

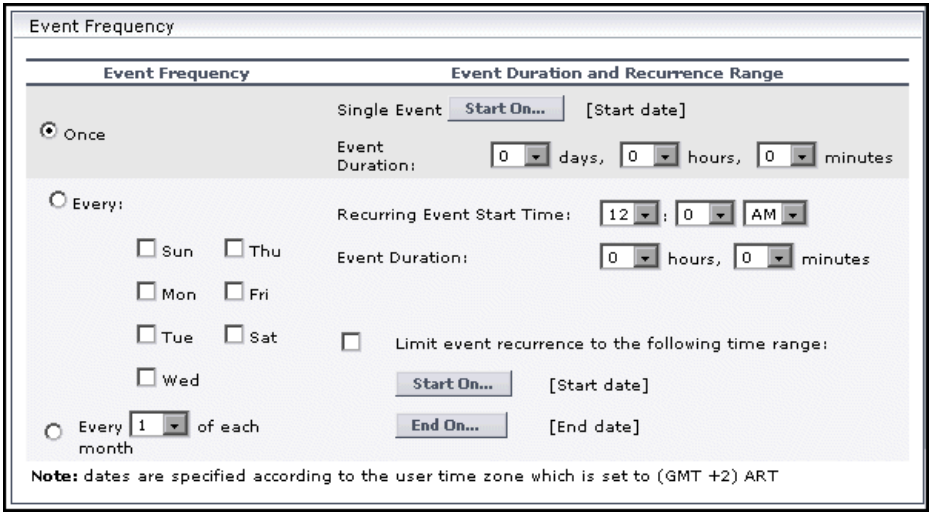
1 Select **Admin** > **Platform** > **Data Collection** > **Downtime/Event Scheduling**. The Downtime/Event Scheduling page opens.

Click the **New Event** button. The Downtime/Event Scheduling dialog box opens and is divided into three sections:

- Event Schedule General Properties
- Event Frequency
- Event Schedule Action

2 In the Event Schedule General Properties area, enter a name and a description of the downtime or scheduled event in the appropriate boxes.

3 In the Event Frequency area, define the time period for the event. You can define a one-time event or a recurring event.



Important: The time period that you define here should be according to the time at the HP Business Availability Center server, and not according to the time on the client on which you are working (if the server and client are in different time zones).

Choose from the following alternatives:

- **Once.** To define a one-time event, select **Once** in the Event Frequency column. Click **Start On** to choose the start date and time of the event. Choose the duration of the event in days, hours, and minutes.
- **Every.** To define a recurring event that occurs on specific days of the week, select **Every** and select the days on which the event occurs. Enter the start time for the event, and its duration.

  To limit the event's duration to a particular time range, select the **Limit event recurrence to the following time range** check box, click **Start On** and **End On**, and choose the dates from the calendar.

  For example, you have defined an open-ended event frequency for every Sunday at 1 AM for 2 hours. You could limit the event so that it occurs every Sunday for a period of two hours.

4 In the Event Schedule Action area, you can prevent alerts from being generated and profiles from being run during defined downtime or scheduled events.

- To prevent alerts from being generated during the time the event is scheduled to occur, select **Stop sending legacy alerts during the event occurrence**.
- To stop running the selected Business Process profile and collecting data during the time the event is scheduled to occur, select **Stop running the profile during the event occurrence**.

Note: These settings do not affect the generation of alerts defined in SiteScope and cannot stop SiteScope from running during downtime or scheduled events.

---

5 In the Event Schedule Action area, select which profiles to associate with this event.

Highlight a profile in the **Available profiles** list and click the right arrow to move it to the **Selected profiles** list. If you do not want a profile that is listed under **Selected profiles** to be associated with this event, highlight the profile and click the left arrow to move it to the **Available profiles** list.

Note: Only those profiles for which the user has full permissions appear in the **Available** or **Selected profiles** list. Additional profiles for which the user does not have permissions may be defined in the platform, but they will not appear for this user.

---

6 Click **OK**. The event you defined is now listed in the Downtime/Event Scheduling page.

To edit an existing downtime or scheduled event:

1 In the Downtime/Event Scheduling page, select the check box next to the event you want to edit. The Downtime/Event Scheduling dialog box opens.

2 Make any changes to the event parameters.

3 Click **OK** to save your changes.

Note: You can edit only those events for which you have full permissions on all the profiles associated with the event. For details on permissions, see “Permissions Management” on page 311.

To delete an existing downtime or scheduled event:

1 In the Downtime/Event Scheduling page, select the event you want to delete. To make selections, use the buttons at the bottom of the page for **Select All**, **Clear All**, and **Invert Selection**.

2 Click the delete button. The event is removed from the Downtime / Event Schedule page.

Note: You can delete only those events for which you have full permissions on all the profiles associated with the event. For details on permissions, see “Permissions Management” on page 311.

12

Profile Entity Maintenance

Platform Administration includes a tool for filtering transactions, locations, and groups from reports. It can also delete obsolete transactions, locations, and groups from the database.

Configuring Report Filters Globally

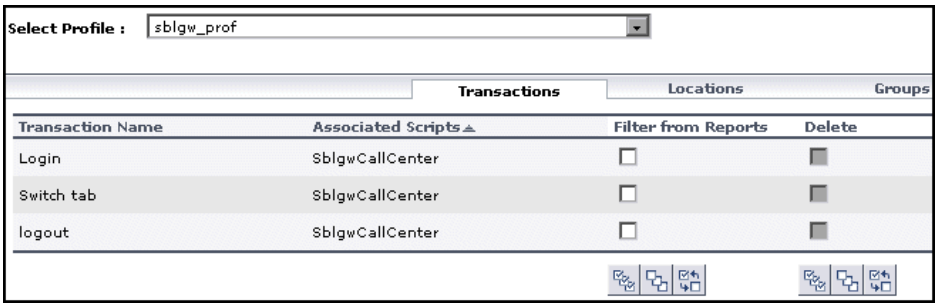
Global report filters enable administrators to exclude - per profile - specific transactions, locations, and groups from all HP Business Availability Center reports for the current and future profile sessions.

Global report filters affect all users. Any transaction, location, or group that is filtered out using global report filters is unavailable in the user-level report filters. For details on specifying report filters per user, see “Report Filters” in *Using End User Management*.

You configure report filters globally in the Profile Entity Maintenance page, accessed in the Data Collection tab of Platform Administration.

To configure global report filters:

1 Select **Admin** > **Platform** > **Data Collection** > **Profile Entity Maintenance**. The Profile Entity Maintenance page opens.



2 From the **Select profile** list, select the profile from which you want to select transactions, locations, or groups to exclude from reports.

3 Select the tab for the type of entity you want to filter from all reports: **Transactions**, **Locations**, or **Groups**.

4 Select the check box under the **Filter from Reports** column beside the transaction(s), location(s), or group(s) you want to exclude from reports for all users in the system.

To make your selections, you can also use the buttons at the bottom of the page for **Select All**, **Clear All**, and **Invert Selection**.

5 Click **Apply** to save your settings.

Note: To activate global filter settings for the current user, log out of HP Business Availability Center and log in again.

Filtered values still appear in user-defined (Custom and Trend) reports that were created before configuring the filter. To remove newly filtered values from existing user-defined reports, you must remove and re-add the components containing the elements for which filters have been set, and save the report.

Deleting Entities from the Database

HP Business Availability Center enables you to delete obsolete entities that are no longer associated with Business Process profiles. These entity types include transactions, locations, and groups.

When you add a transaction monitor to a Business Process profile, the transaction and the transaction's location and group are added to the profile database. Even when a transaction monitor is deleted from the Business Process profile, the transaction and its location and group are still listed in the profile database. Until they are deleted in the Profile Entity Maintenance page, they appear in reports and filter lists for the profile.

Note: You use the End User Management page to create Business Process profiles and add transaction monitors to those profiles. You also delete transaction monitors from profiles in End User Management Administration. For details, see "Managing Business Process Profiles" in *Using End User Management*.

Deleting transactions, locations, and groups affects all users. You delete only those transactions, locations, and groups that are no longer associated with the selected profile. You do this in the Profile Entity Maintenance page, accessed in the Data Collection tab of Platform Administration.

To delete transactions, locations, and groups that are not associated with selected profiles:

1. In Platform Administration, select **Data Collection** > **Profile Entity Maintenance**. The Profile Entity Maintenance page opens.
2. From the **Select profile** list, select the profile from which you want to delete transactions, locations, or groups.
3. Select the tab for the type of entity you want to delete: **Transactions**, **Locations**, or **Groups**.

4 Select the check box under the **Delete** column beside the transaction(s), location(s), or group(s) you want to delete for the selected profile.

You can delete only those transactions, locations, or groups which are no longer associated with the selected profile (i.e. - not in use). Only the check boxes for those entities are enabled for deletion. If an entity is still associated with the selected profile, the deletion check box is disabled for that entity.

To make your selections, you can also use the buttons at the bottom of the page for **Select All**, **Clear All**, and **Invert Selection**.

5 Click **Apply** to save your settings.

13

Working with Measurement Filters

Note to HP Managed Software Solutions customers: HP Operations administers this page and the interface is hidden from your view.

This chapter explains how to define measurement filters that enable you to filter data being sent to HP Business Availability Center from its data collectors, or from external systems or data sources.

Measurement Filters Overview

Measurement filters enable you to harvest significant data from the quantities of data sent to the HP Business Availability Center database from various data sources (including HP data collectors and third-party data sources) by creating filters that only display the most relevant data required.

You can create measurement filters for all data samples for which HP Business Availability Center uses the Universal Data Exchange (UDX) framework. These include Real User Monitor data samples, SiteScope Integration Monitor data samples, and Business Logic Engine data samples. For details on the samples used in HP Business Availability Center, see "Data Samples" in *Reference Information*.

Once you set up measurement filters, you can use them in various contexts in HP Business Availability Center, including:

- when defining trend reports using the Custom monitor type
- when creating views in CMDB Administration (all defined measurement filters are automatically added as CIs to the UDX Measurement Filters view)
- when creating service level agreements (by adding measurement filter CIs to the SLA)

Note: In certain contexts in the HP Business Availability Center Web interface, the term "custom" data is used to categorize the data samples for which HP Business Availability Center uses the Universal Data Exchange (UDX) framework.

Defining Measurement Filters

You define measurement filters from the Measurement Filters page, which you access from the **Admin** > **Platform** > **Data Collection** tab.

For details on the data types listed on the Measurement Filters page, see "Data Samples" in *Reference Information*.

When creating a measurement filter keep the following guidelines in mind:

- You build an expression by working in the following order: Field, Operator, Value.
- The values you enter in the Value box are case sensitive and you must enter them precisely as they are used in the samples.

To define a measurement filter:

1. Select **Admin** > **Platform** > **Data Collection** > **Measurement Filter** to open the Measurement Filters page.
2. From the Data Type list, select the data type for which you want to define a filter. For details on the data types listed on the Measurement Filters page, see "Data Samples" in *Reference Information*.

   Filters previously defined for the data type are displayed by name. If no filters exist for the data type, HP Business Availability Center displays a message.

   To display existing filters by category, select **Category**. (You create categories to organize your filters. For details on creating a category, see "Creating a Category" on page 237.)
3. Click **New Filter** to open the Filter dialog box.
4. Enter a name for the filter. This is the name that you will see when building reports or in the UDX Measurement Filters view.
5. Build a Boolean expression, using the **And** and **Add 'OR' Expression** buttons.

   For each statement, define the following:

   - **Field.** Choose fields by which to filter the sample. For a list of fields associated with each sample, see "Data Samples" in *Reference Information*.
   - **Operator.** The list of operators displayed depends on the selected field.

➤ **Value.** Enter a value that the expression compares with the value in the data sample.

Note that:

➤ During the process of building the expression, you can view the results accumulated so far in the **Boolean Expression** box.

➤ If you select a numeric operator, the value must be in the same numeric format as appears in the database.

➤ If you select a text operator, you can enter a single value without quotation marks, as they are added automatically when HP Business Availability Center builds the expression. To add two values, add quotation marks around each value, and separate them by a comma. For example, to define a filter that searches for a transaction name that is either **HP** or **OVO**, enter **"HP","OVO"**.

➤ You should not use a field and operator combination twice in the same **And** phrase.

➤ If you are building a measurement filter for certain Real User Monitor data types, you can choose the value from a list (instead of typing it in the field). This is true for the following data types:

Data Type	Field	Operator
RUM Pages	Page Name End User Name	in/not in
RUM End Users	End User Name	in/not in
RUM Transactions	Transaction Name End User Name	in/not in

6 Click **OK**. The filter appears in the list of filters.

You can assign one or more categories to a filter to help you organize the filters. For details, see "Assigning a Category to a Measurement Filter" on page 237.

Creating a Category

You define categories that help to organize your filters in a meaningful manner.

To create a category:

1. Select **Admin** > **Platform** > **Data Collection** > **Measurement Filter** to open the Measurement Filters page.
2. Select the **View By Category** option to display the filters by category.
3. Click the **Category Manager** button to open the Category Manager dialog box.
4. Click **New Category** to open the New Category dialog box.
5. Enter a name for the category, and click **OK**. You are returned to the Category Manager dialog box. The new category appears in the list of categories.
6. Click **OK** to return to the Measurement Filters page.

Assigning a Category to a Measurement Filter

You can assign one or more categories to a filter.

To assign a category to a filter:

1. Select **Admin** > **Platform** > **Data Collection** > **Measurement Filters** to open the Measurement Filters page. Select **View By Name**.
2. Locate the measurement filter in the list, or enter the complete or partial filter name in the Search box, and click **Go**.

   When searching, you can type an asterisk to replace characters. For example, to search for the filter **probe on cats machine**, enter ***cat***.
3. Click the **Category** button to open the Filter Categories dialog box.

4 Select or clear categories to include or exclude them in the filter. Click **All** to select all choices. Click **None** to clear all selections. To invert your selection (clear filters that were selected and select filters that were not selected), click **Invert**.

5 Click **OK**.

Editing a Measurement Filter

You can edit a measurement filter only if it is not being used by any HP Business Availability Center entity. If the filter is being used, you can view its properties, but you must first remove the filter before you can edit it.

To edit a measurement filter:

1 Select **Admin** > **Platform** > **Data Collection** > **Measurement Filter** to open the Measurement Filters page. Select **View By Name**.

2 Locate the measurement filter in the list, or enter the complete or partial filter name in the Search box, and click **Go**.

When searching, you can type an asterisk to replace characters. For example, to search for the filter **probe on cats machine**, enter ***cat***.

3 Click the filter name to open the Filter dialog box.

4 Make any necessary changes. For details, see step 4 on page 235 in "Defining Measurement Filters".

5 Click **OK**.

To edit a measurement filter being used by an HP Business Availability Center entity:

1 Select **Admin** > **Platform** > **Data Collection** > **Measurement Filter** to open the Measurement Filters page. Select **View By Name**.

2 Locate the measurement filter in the list, or enter the complete or partial filter name in the Search box, and click **Go**.

When searching, you can type an asterisk to replace characters. For example, to search for the filter **probe on cats machine**, enter ***cat***.

3 Hold the cursor over **See Details** to view a list of entities that are using the filter.

   Click **See Details** to display the Filter dialog box in read-only mode.

4 Access each entity and remove the filter.

5 Return to the Measurement Filters page and edit the filter.

Duplicating a Measurement Filter

You can create a measurement filter by duplicating an existing filter, and making any necessary changes.

Note: If categories were assigned to the duplicated filter, they are also assigned to the new filter. If necessary, you can change these assignments. For details, see "Assigning a Category to a Measurement Filter" on page 237.

To duplicate an existing filter:

1 Select **Admin** > **Platform** > **Data Collection** > **Measurement Filter** to open the Measurement Filters page. Select **View By Name**.

2 Locate the measurement filter in the list, or enter the complete or partial filter name in the **Search** box, and click **Go**.

   When searching, you can type an asterisk to replace characters. For example, to search for the filter **probe on cats machine**, enter ***cat***.

3 Click the **Duplicate** button to open the Filter dialog box.

4 Change the name of the filter, and make any other changes as necessary.

5 Click **OK**. The new filter is listed with **(Duplicated)** next to its name.

Deleting a Measurement Filter

You can delete measurement filters, as long as they are not being used by any HP Business Availability Center entity. If the filter is being used, the Delete button is disabled.

To delete a filter:

1 Select **Admin** > **Platform** > **Data Collection** > **Measurement Filter** to open the Measurement Filters page. Select **View By Name**.

2 Locate the measurement filter in the list, or enter the complete or partial filter name in the Search box, and click **Go**.

When searching, you can type an asterisk to replace characters. For example, to search for the filter **probe on cats machine**, enter ***cat***.

3 Click the **Delete** button. Note that no warning message is displayed before HP Business Availability Center deletes the filter.

14

Central Repository Service

Note to HP Managed Software Solutions customers: The repository for HP Managed Software Solutions scripts functions differently from the repository described here. For details on working with scripts, see "HP Managed Software Solutions Script Repository" on page 268.

The Central Repository Service allows you to manage and maintain your scripts in one central location and enables version control of those scripts.

About the Central Repository Service

The Central Repository Service is the central storage in which all your organization's Business Process Monitor scripts are stored. The repository enables you to organize your scripts into logical groups and to view and manage the properties of those scripts. The repository also enables version control and version updates.

The Central Repository Service enables you to:

- create and manage user-defined folders for organizing your scripts (for details, see "Working with Central Repository Service Folders" on page 243)
- upload scripts to a repository folder for use when creating monitors
- manage the scripts that have been uploaded to the repository
- control the versions of the file sets with check in and check out functionality, including downloading script content onto your local system for editing

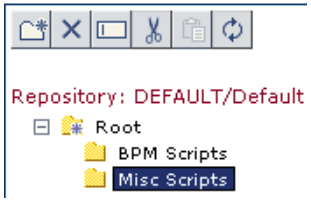
The Central Repository Service is installed during HP Business Availability Center deployment and resides along with the management database configured for your HP Business Availability Center installation.

To generate business process data, you must create profiles and transaction monitors to run scripts that include those processes you want monitored. When you add a transaction monitor to a profile in End User Management Administration, you can add only those scripts that have been stored in the Central Repository Service. For details on adding profiles and transaction monitors, see "Creating Business Process Profiles" and "Managing Business Process Profiles" in *Using End User Management*.

Note: If your HP Business Availability Center management database is running on an Oracle Server: For the Central Repository Service to function correctly, the management user schema requires execution permissions (the default) for the DBMS_LOB package. If these permissions have been revoked, the Central Repository Service is unable to access the database. Before using the Central Repository Service, confirm with your database administrator that these permissions are in place.

Working with Central Repository Service Folders

Scripts are organized into folders that you create and maintain in the Central Repository Service. Scripts can be added to the repository only within a user-defined folder. The folders are organized in a tree hierarchy that appears in the left pane of the Central Repository Service page.



The top level folder is the **Root** level. You create folders below the **Root** level folder. You manage the folders using the buttons that appear above the folder tree.

The Folder Content area in the right pane of the page lists all the scripts that have been uploaded to the folder that is highlighted in the folder tree hierarchy.

This chapter includes the following topics:

➤ "Moving a Folder" on page 245

➤ "Refreshing the Folder Tree" on page 246

Creating New Folders

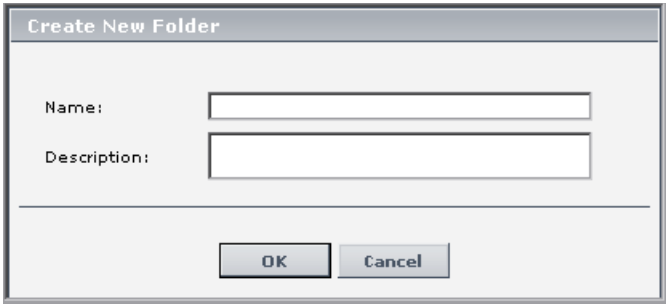
You can create a new folder under the **Root** folder or any other folder in the folder tree hierarchy.

To create a new folder:

1 Access the Central Repository Service page from Platform Administration by selecting **Admin** > **Platform** > **Data Collection** > **Central Repository Service**.

2 Click to highlight the **Root** or other parent folder under which you want to create the new folder.

3 Click the **New Folder** button. The Create New Folder dialog box opens.



4 Enter a folder name and description. The description is optional.

5 Click **OK** to create the new folder.

Deleting Folders

When you delete a folder, all sub folders and scripts under that folder are permanently erased from the repository. The only exception is if a script is checked out at the time that the folder containing it is deleted. In this case, the repository deletes all folders and scripts until it reaches the checked out file set and its folder, which cannot be deleted, and ceases the delete process.

To delete a folder:

1 Select the folder that you want to delete.

2 Click the **Delete Folder** button. The Delete Folder dialog box opens.

3 Click **Yes** to delete the folder.

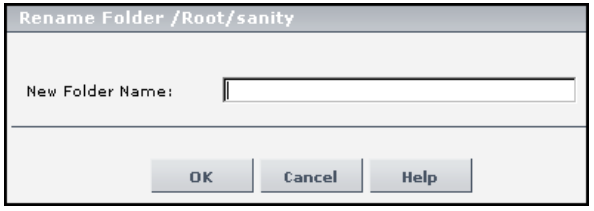
Renaming Folders

You can rename a folder in the tree hierarchy. This will not change any of the contents of the folder.

To rename a folder:

1 In the tree hierarchy, select the folder that you want to rename. It can be a parent folder or a sub folder.

2 Click the **Rename Folder** button. The Rename Folder dialog box opens.



3 Enter a new folder name.

4 Click **OK** to change the folder name.

Moving a Folder

You can move a folder from one location to another location within the tree hierarchy using cut and paste functions. You cannot paste a folder into the same folder from which it was cut.

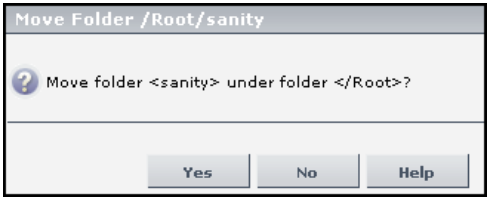
To move a folder:

1 In the tree hierarchy, select the folder that you want to move. It can be a parent folder or a sub folder.

2 Click the **Cut** button.

3 Select the target folder to be the new location for your folder.

4 Click the **Paste** button. The Move Folder dialog box opens.



5 Click **Yes** to move the folder.

Refreshing the Folder Tree

The **Refresh Tree** button enables you manually refresh the navigation tree in the Central Repository Service. You refresh the tree to load the folder data that may have been modified by other users using the Central Repository Service.

When you perform any of the folder operations, the tree refreshes automatically, so it is not necessary to refresh it manually.

Uploading Scripts and Creating File Sets

You create file sets that contain the scripts you upload to the Central Repository Service. File sets are the collection of files that make up the script and enable the transactions to be run by the Business Process Monitor. These file sets must be created within an existing folder in the Central Repository Service. For details on creating folders, see "Working with Central Repository Service Folders" on page 243.

To create scripts for use in HP Business Availability Center, you must record Business Process Monitor scripts using the HP Virtual User Generator recording tool. For details, see "VuGen Recording Tips" in Using End User Management.:

Once these scripts are recorded and saved as .zip files, you upload them to the Central Repository Service.

Note: When zipping a script in Virtual User Generator for upload to the Central Repository Service, it is recommended that you zip only the script's run-time files.

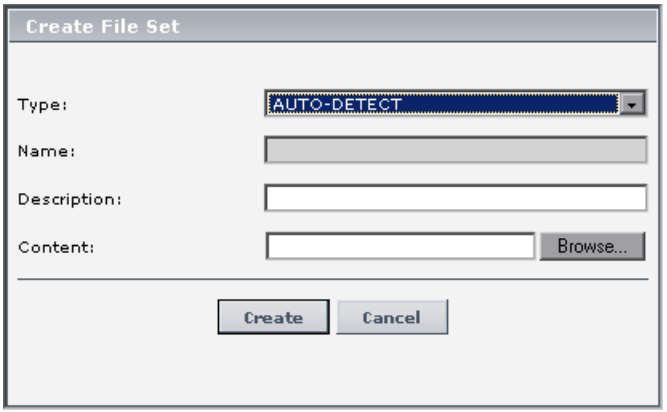
You must upload scripts to the repository to access them when creating profiles in End User Management Administration. You create profiles and transaction monitors to collect performance data on the transactions within the scripts. For details on creating profiles, see "Creating Business Process Profiles" in *Using End User Management*.

To create file sets and upload scripts to the Central Repository Service**:**

1 Access the Central Repository Service page by selecting **Admin** > **Platform** > **Data Collection** > **Central Repository Service**.

2 In the folder tree in the left pane, highlight the folder into which you want to add the script.

3 In the right pane, click the **New** button on the bottom right corner of the Folder Content area. The Create File Set dialog box opens.



4 Choose the type of file set you want to add to the Central Repository Service from the **Type** list. If you select **AUTO-DETECT**, the script type is determined during the upload.

Note: Currently, the following types are supported in HP Business Availability Center: **AUTO-DETECT**, **VUGEN SCRIPT**, and **QTP SCRIPT**.

---

5 The name of the content or .zip file you specify in step 7 on page 249 becomes the name of the file set. The name appears in the file set table in the right pane and when viewing the file set properties.

This is also the name that appears in the list of available scripts when creating transaction monitors in End User Management Administration. For details, see "Adding Transaction Monitors" in *Using End User Management*.

6 Optionally, add a description for the new file set. This description appears in the file set properties.

7 In the **Content** box, enter the path of the .zip file containing the script. You can also click **Browse** to locate the .zip file in your file system.

8 Click **Create** to add the new file set.

The file set is added to the table in the right pane. This may take a few moments depending on the size of the file's content.

For details on editing or deleting the script and file set properties, see "Managing File Sets" on page 249.

For details on file set versions, see "Working with File Set Versions" on page 253.

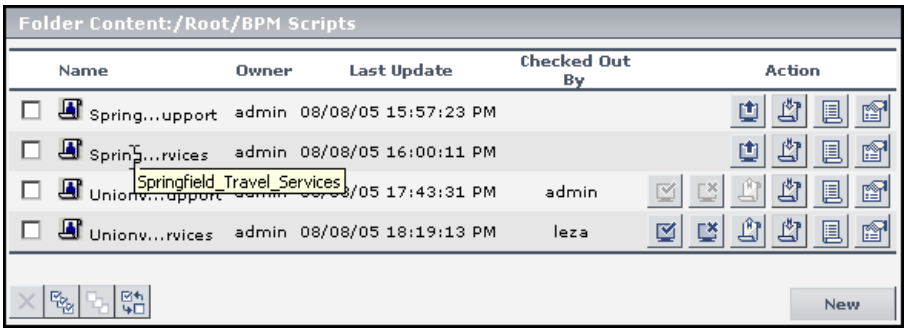
Managing File Sets

HP Business Availability Center enables you to manage the file sets that are stored within the Central Repository Service folders. The right pane of the Central Repository Service page lists in table format all the file sets that have been created within the folder that is highlighted in the folder tree. For details on the folder tree and folders, see "Working with Central Repository Service Folders" on page 243.

This chapter includes the following topics:

Understanding the File Set Table

When you select a folder in the tree view, the Central Repository Service displays a list of the available file sets for that folder.



Each line represents a file set for the selected folder and the actions that can be performed on the file set.

You can view the following:

- Type of script – Script type is indicated by these icons that appears next to the file set name:
  - Virtual User Generator (VUGen) script
  - QuickTest Professional script
- **Name.** The name given to the file set when it was created and the script was uploaded. In the case of a long name, the name is truncated in the table. To view the entire name, hover over the name as it appears and a tooltip opens displaying the full name of the file set as in the above diagram.
- **Owner.** The user who created the file set by uploading the script.
- **Last Update.** The date when the file set was last checked into the repository. This could be the date it was first created.
- **Checked Out By.** The user who has the file set currently checked out. If the file set is not checked out, this column is blank.

- **Action.** You can perform the following actions on each file set:
  -  Check out the file set to ensure version control. For details, see "Checking out a Version" on page 253.
  -  Check in the file set, cancel the check out, or upload without checking in. These buttons are displayed only for those file sets that have been checked out and are enabled only for the user who performed the check out. For details, see "Working with File Set Versions" on page 253.
  -  Download file set contents for editing. For details, see "Downloading File Set Content" on page 254.
  -  Show versions. For details, see "Viewing File Set Versions" on page 260.
  -  View file set properties. For details, see "Viewing File Set Properties" on page 252.

Deleting File Sets from a Central Repository Service Folder

When deleting file sets from a selected repository folder, keep in mind:

- All files within the deleted file set are permanently erased from the repository.
- If you delete a file set that is currently running in a transaction monitor, the transaction monitor continues running the file set's script, but the properties of the transaction monitor cannot be edited in End User Management Administration until the file set is added back to the Central Repository Service.
- A file set that is currently checked out cannot be deleted by another user and can be deleted only by the user who checked it out.

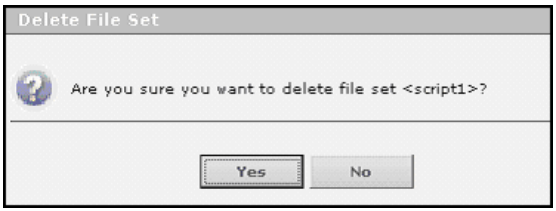
To delete a file set:

1. In the folder tree in the left pane of the Central Repository Service, highlight the folder that contains the file set that you want to delete.
2. Select the check box for the file set you want to delete.

To make your selections, use the buttons at the bottom of the page for **Select All**, **Clear All**, and **Invert Selection**.

3 Click the **Delete File Set** button at the bottom of the table. The delete button is enabled only if at least one file set is selected.

The Delete File Set dialog box opens.



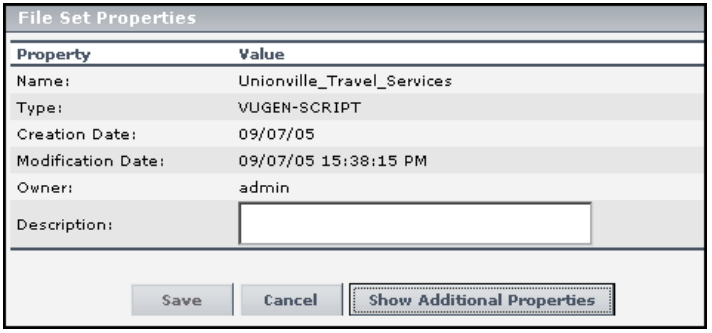
4 Click **Yes** to confirm that you want to delete the file set.

Viewing File Set Properties

You can view the properties of the current version of the file set. All the fields are view only and cannot be edited while viewing the properties.

To view file set properties:

1 Click the **File Set Properties** button on the line of the file set whose properties you want to view. The File Set Properties window of the working version of the file set opens.



2 Optionally, you can click **Show Additional Properties** to view the properties related to the script itself.

Note: When a file is checked in, none of the fields in the File Set Properties dialog box are editable. When a file set is checked out, the description property can be edited only by the user who checked out the file set.

Working with File Set Versions

The Central Repository Service enables you to control the versions of your file sets. The procedure when working within the Central Repository Service for editing a script is to check out the file set, download the script for editing, and then check in the file set. When the file set is checked in, the Central Repository Service automatically assigns the script a new version number.

You can also view version properties and restore previous versions of file sets. For details, see "Viewing File Set Versions" on page 260.

This chapter includes the following topics:

Checking out a Version

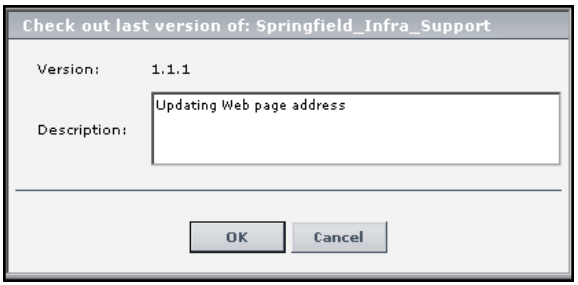
You can check out a file set to ensure that no other user makes changes to this version of the script while you are editing it. Only one user at a time can check out a file set. Once that file set is checked out, only that user can check it in, delete it, or create a new version.

Note: When a file set is checked out, the script can still be added as a transaction monitor while working in End User Management Administration. If the file set is checked in with a newer version, the transaction monitor includes a message to the user indicating that a newer version of the script is available in the repository.

To check out a file set:

1 Click the **Check Out** button on the line of the file set you want to check out.

The Check Out Last Version dialog box opens.



2 Optionally, enter a description for the version. This is recommended so that all users have access to the information regarding why different versions have been created in the repository.

3 Click **OK**. The file set is checked out.

You can now download the file set, knowing that the version cannot be edited by another user.

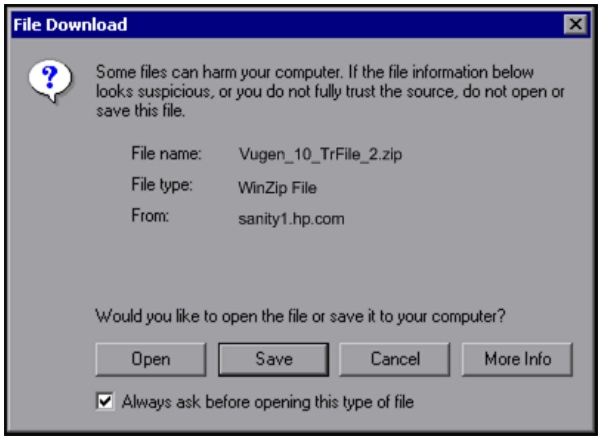
Downloading File Set Content

When you download a file set, the current working version of the file set is downloaded. It is good practice to check out the file set before downloading it to ensure that another user is not simultaneously editing the same file set's script.

To download the content of a file set's current working version:

1 Click the **Download File Set Content** button on the line of the file set that you want to download.

If the file set has content, the File Download dialog box opens.



If the selected file set is empty, the Central Repository Service issues a warning indicating that the file set has no content.

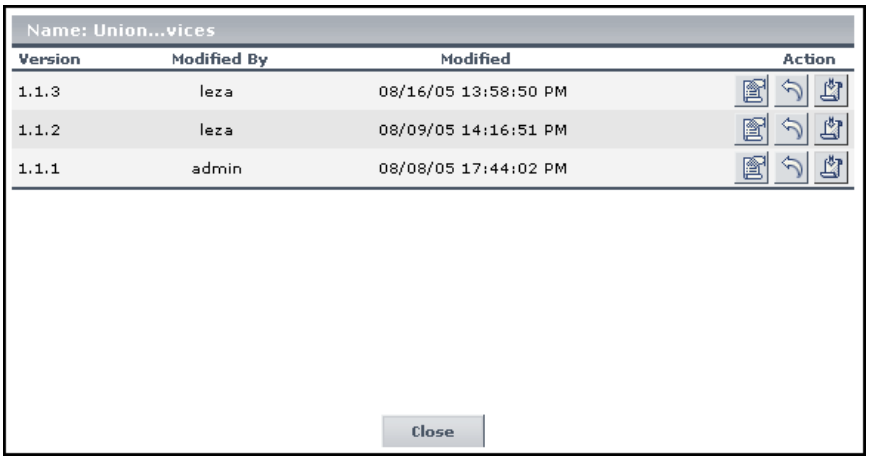
2 Click **Save** to save the .zip file that contains the script to your local file system. The Save As dialog box opens.

3 Specify a location in your file system for saving the zipped file of the script and click **Save**.

You can now use your recording tool to open and edit the downloaded script.

To download the specified version of a file set:

1 Click the **Show Versions** button on the line of the file set whose content you want to download. The File Set Versions dialog box opens.



2 Click the **Download File Set Content** button on the line of the file set version that you want to download. Select from the list of checked in file set versions.

You cannot download the version of a file set version that is checked out. For details, see "Viewing File Set Versions" on page 260.

3 Continue with steps 2 on page 255 through 3 on page 255 in the procedure for downloading the current working version of a file set.

Checking in a Version

You check the file set back into the Central Repository Service once you have finished editing the script and saving the .zip file in your file system.

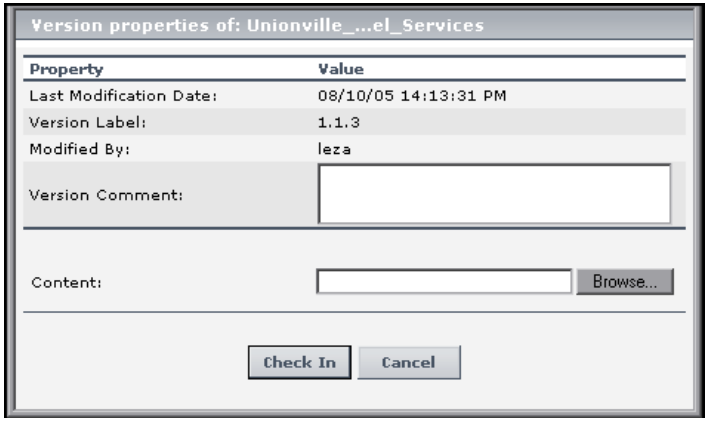
When you check in a file set, the Central Repository Service automatically creates a new version for the file set. For example, if you checked out version number 1.1.1 of a file set, the Central Repository Service creates version number 1.1.2 as a result of checking the file set back into the Central Repository Service. File set version 1.1.1 is still accessible and its script can be added to transaction monitors in End User Management Administration, but the latest version, file set version 1.1.2, becomes the default version.

To check in a version:

1 Click the **Check In** button on the line of the checked out version of the file set you want to check in.

Note: This button appears only for file sets that are checked out.

A check in version of the Version Properties dialog box opens.



2 Optionally, enter **Version comments** for this new version of the file set. This is recommended so that other users know what has been updated in the script.

3 Optionally, click **Browse** to locate and select the .zip file of the latest version of the script.

➤ If you specify a location for the file set content, the name of the uploaded .zip file must match identically to the name of the file set.

- If you do not specify a location for the file set content, and:
  - The file set content has been uploaded and not yet checked in, the most recently uploaded version of the content is checked in. No location has to be specified. For details, see "Uploading File Set Content" on page 259.
  - The file set content was not uploaded, the same content of the file set that was checked out is checked in again and given a new version number.

4 Click **Check In** to check in the version or **Cancel** to cancel the operation.

Cancelling Check Out

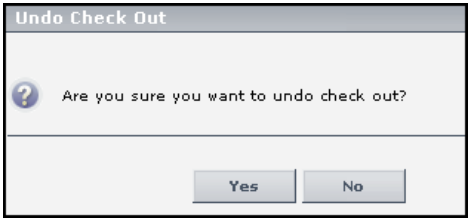
Cancelling a check out prevents the Central Repository Service from creating a new version number and leaves the file checked in with its current version number. If you have made modifications to the script that you do not want saved in the Central Repository Service file set, cancelling the check out ensures that those changes are not brought into the Central Repository Service.

To cancel a check out:

1 Click the **Undo Check Out** button on the line of the checked out file set.

Note: This button appears only for file sets that are checked out.

The Undo Check Out dialog box opens.



2 Click **Yes** to undo the check out or **No** to keep the file set checked out.

Uploading File Set Content

When a file set is checked out, you can upload a script without creating a new file set version. You upload scripts to save the recent modifications you have made in the script to the Central Repository Service. This is done only if you do not yet want to create a new version by checking in the file set. You may want to do this as an extra precaution when making many modifications to scripts so that the file set is saved to the repository. This is useful, for example, while you are testing the script in the recording tool.

When you upload a script without checking in the file set, the content of this version of the file set is not available to other users.

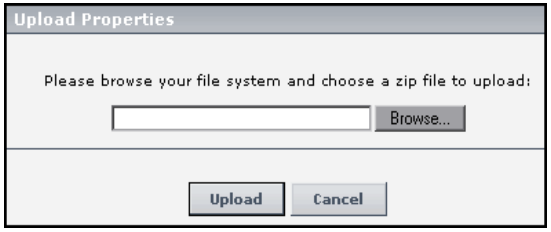
When you check in a file set that has been uploaded, you do not have to specify a location in your file system to locate the file set. The most recently uploaded file set is automatically checked in during the check in procedure.

To upload the content of a checked out file set:

1 Click the **Upload File Set Content** button on the line of the checked out file set.

Note: This button appears only for file sets that are checked out.

The Upload Properties dialog box opens.



2 Click **Browse** to locate and select the .zip file of the latest version of the script.

3 Click **Upload** to save the script to the Central Repository Service.

If, during check in, you do not specify a location for the .zip file, this content is used when checking in the file set.

Viewing File Set Versions

You can view the versions of a file set in the File Set Versions dialog box. It includes a listing of all the versions of a file set and the actions that can be performed on that file set version.

The versions list and available actions are different for a file set that is checked in from those for a file set that is checked out.

You can restore a previous version of a file set that is not checked out.

Viewing Checked in File Set Versions

When you view the file set versions of a file set that is not checked out, you see all the versions of the file set that have existed in the Central Repository Service. You can view the following:

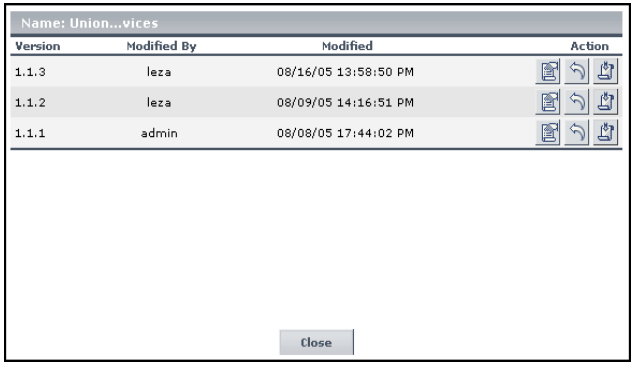
- **Version.** The number given to the file set when it was last checked into the Central Repository Service.
- **Modified by.** The user who last checked in the version of the file set.
- **Modified.** The date and time when the file set was last checked into the repository. If the file set has never been checked in, this is the date the script was first downloaded and the file set was first created.
- **Action.** You can perform the following actions on the version:
  -  **View version properties.** While viewing version properties, you can modify only the **Version Comments** field. All other fields are uneditable.
  -  **Restore version.** This enables you to restore a previous version of a file set and make it the current version. For details, see “Restoring Previous File Set Versions” on page 261.
  -  **Download file set contents for editing.** For details, see “Downloading File Set Content” on page 254.

Restoring Previous File Set Versions

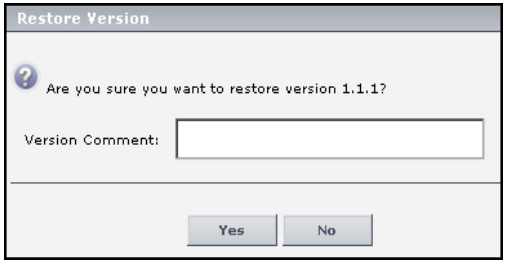
When you restore a file set version, the Central Repository Service automatically assigns that version the next available version number. For example, if you select version number 1.1.1 to restore, the Central Repository Service assigns that same file set content the next available version number which in the diagram below, would be version number 1.1.4. Thus, version 1.1.1 and version 1.1.4 are identical.

To restore a previous version of a file set:

1 Click the **Show Versions** button on the line of the file set whose previous version you want to restore. The File Set Versions dialog box opens.



2 Click the **Restore Version** button on the line of the version you want to restore. The Restore Version dialog box opens.



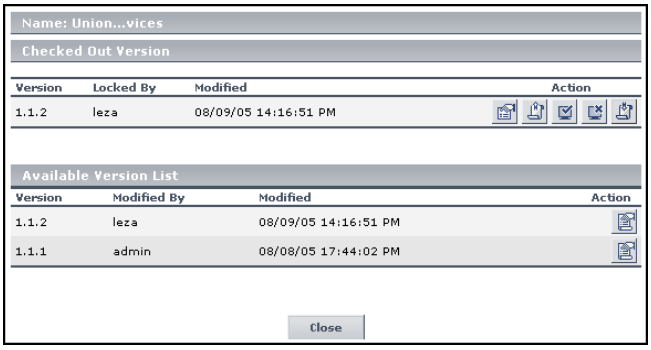
3 Optionally, enter the relevant information in the **Version Comments** field. Because the contents of the new version you are creating are identical to the old version, it is recommended that you include the version number that was restored in the comments.

4 Click **Yes** to confirm.

The new version now appears with its new version number in the File Set Versions dialog box.

Viewing Checked out File Set Versions

When you view the file set versions of a file set that has been checked out, you see the checked out version listed separately from the previous versions of the file set.



- In the Checked Out Version area, you can view the following for the checked out version:
  - **Version.** The version number of the file set that is checked out.
  - **Locked by.** The user who checked out the file set.
  - **Modified.** The date and time when the file set was last checked into the repository. If the file set has never been checked in, this is the date it was first created.

- **Action.** If you are the user who checked out the file set, you can perform the following actions on the version:
  -  **View file set properties.** For details, see "Viewing File Set Properties" on page 252.
  -  **Check in the file set, cancel the check out, or upload without checking in.** These buttons are enabled only for the user who performed the check out. For details, see "Working with File Set Versions" on page 253.
  -  **Download file set contents for editing.** For details, see "Downloading File Set Content" on page 254.

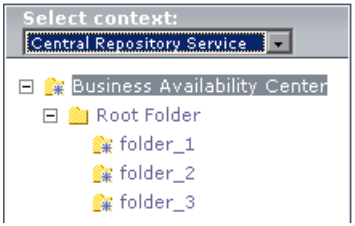
- In the Available Versions area, you can view the following for all the previous versions of the checked out file set:
  - **Version.** The number given to the file set when it was last checked into the Central Repository Service.
  - **Modified by.** The user who last checked in this version of the file set.
  - **Modified.** The date and time when this version of the file set was last checked into the repository.
  - **Action.** You can perform the following action on the version:
    -  **View version properties.** While viewing version properties, you can modify only the **Version Comments** field. All other fields are uneditable.

CRS Permissions

This section includes the following topics:

Prior to HP Business Availability Center 7.0, permissions could only be applied to the Central Repository Service as a whole.

Beginning in version 7.0, you can restrict a user's access to individual folders and all of its scripts and subfolders. In the example below, if a user has permission to access the folder_1 folder, he also has permission to access its scripts and its subfolders.



Setting Permission Mode

Permission management is in either of the following modes:

➤ **enforce permission.** This is the default mode. Users authenticated in HP Business Availability Center are allowed to perform actions on specific folders. Only those folders and scripts that the user has permission to access are displayed in the Folder Content area.

➤ **do not enforce permission.** Any user authenticated in HP Business Availability Center can perform any action on any folder. All folders and scripts are displayed in the Folder Content area.

You can change the permission mode from **enforce permission** to **do not enforce permission,** and vice versa.

The following procedure changes the mode from **enforce permission** to **do not enforce permission.**

To change permission mode:

1 Stop HP Business Availability Center on the Gateway server.

2 Using WinZip or WinRAR, extract and then open **<HP Business Availability Center root directory>/lib/crs_resources.jar**. Do the following:

   a rename **crs_common_config.xml** to **crs_common_config_tas.xml**

   b rename **crs_common_config_full_permissions.xml** to **crs_common_config.xml**

   c save and close **crs_resources.jar**

3 In the **<HP Business Availability Center root directory>/conf/tas** directory, do the following:

   a rename **crsContext.xml** to **crsContext.xml.old**

   b rename **crsContext.properties** to **crsContext.properties.old**

4 Restart HP Business Availability Center.

Assigning Permissions Operation

If Permission management is in **enforce permission** mode, you can assign the appropriate permissions operation. For details about permissions, see "Granting and Removing Permissions" on page 313.

To assign a permissions operation:

1 Select **Admin > Platform > Users and Permissions.** In the Resource Context list, select **Central Scripts Repository**. Select the appropriate folder underneath the Root folder. Operations assigned to a folder affect all folders contained beneath it.

2 In the Users and Groups area, select the user.

3 In the Roles and Operations area, select the **Operations** tab.

4 Check or clear either the **View** or the **Full Control** operation box:

- If **View** is checked, the user can view and download a script in the Central Scripts Repository.
- If **Full Control** is checked, the user can edit or delete any script in the selected folder or its subfolders.

  Giving Full Control on the Root folder grants the user permissions on all folders under Root. If he later adds a folder under the Root folder, Full Control is automatically granted on that folder.
- If neither **View** nor **Full Control** is checked, the user has no access to any script or subfolder in the selected folder. This is the default permissions operation.

5 Click **Apply Permissions** to save the settings.

If the user was logged in while you changed his permissions operation, he must log out and log in again for the changes to take effect.

Importing Application Performance Lifecycle Scripts to the CRS

You can import the Production Analysis Reports from Application Performance Lifecycle (APL) Scripts to the Central Repository Service. For details, see "Work with the Central Repository Service (CRS)" on page 487 in *Solutions and Integrations*.

15

Data Collection Administration for HP Managed Software Solutions

Note: The Location IP Ranges, Script Repository, and Package Information pages are available to HP Managed Software Solutions customers only.

Data Collection Administration for HP Managed Software Solutions allows you to view the customer's list of locations and related information, to maintain your scripts and view their verification information, as well as to view package location information.

Location IP Ranges

The Location IP Ranges page presents a list of locations defined in your package. This list includes the detailed IP address ranges.

In Platform Administration, click **Data Collection** > **Location IP Ranges** to open the **Location Info** area.

You can view the following information:

- **Location Name.** The physical location: city, county, state, or province, and the name of the location.
- **IP Address/Subnet Mask.** The range of IP addresses for the location. The first number is the IP Address (and the beginning of the range). The second number is the Subnet Mask. The Subnet Mask is used to calculate the number of addresses in the range by subtracting the last set of three numbers (in this example: 240) from the set of three numbers before last (in this example: 255). The result is: 255-240=15. This result is then added to the last set of three numbers in the IP Address (in this example 144+15=159) to provide the upper IP Address in the range: 195.193.104.159. The range of Amsterdam IP Addresses is then from the IP Address: 195.193.104.144 to the calculated upper IP address: 195.193.104.159.

HP Managed Software Solutions Script Repository

The script repository is a central database in which all your organization's Business Process Monitor scripts are stored.

When you add a monitor to a profile in End User Management Administration, you can add only those scripts that have been stored in the Script Repository and were manually verified ("Managing Business Process Profiles" in *Using End User Management*).

Once you have created and recorded the scripts (for details, see "Recording Business Process Monitor Scripts" on page 269), you upload them using the Script Repository page (for details, see "Uploading Scripts" on page 269). You can then view the scripts, edit them, and upload them again (for details, see "Understanding the Script Repository" on page 270). You can reload a previous version and make it the current version and you can view the results of the verification process performed by HP Business Availability Center (for details, see "Editing Scripts" on page 271). You can also specify the recipients to whom the results of the verification process should be sent (for details, see "Notifying Recipients of Script Verification" on page 277).

Recording Business Process Monitor Scripts

You record Business Process Monitor scripts using the HP Virtual User Generator recording tool. Once they are recorded, you zip the related files and upload them to the script repository (for details, see "VuGen Recording Tips" in *Using End User Management*). Business Process Monitor scripts are listed in the Business Process Monitor tab in the Script Repository page.

Note: When zipping a script in Virtual User Generator for upload to the script repository, it is recommended that you zip only the script's run-time files. Zipping all files may cause script verification to fail due to a limit in the file size allowed by the repository.

Uploading Scripts

You upload scripts from the Script Repository page.

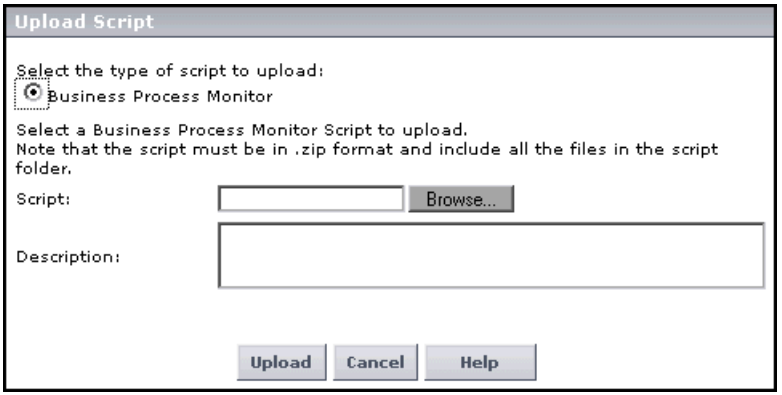
When the upload is finished, HP Business Availability Center displays the script in the appropriate list of uploaded scripts on the Script Repository page. For details, see "Understanding the Script Repository" on page 270. The version of the script that is stored is the active version. To use a newer version or to go back to an older version of the script you must upload the script corresponding to the version you want. That script then becomes the active version of the script.

After you upload a script, HP Business Availability Center runs the verification process. For details, see "Understanding the Script Verification Results" on page 274.

You must upload scripts to the repository to access them when creating profiles. For details on creating profiles, see "Managing Business Process Profiles" in *Using End User Management*.

To upload scripts from the Script Repository page:

1 In the Script Repository page, click **Upload** to open the Upload Script page.



2 Select the type of script you want to upload (if not already selected).

3 Click **Browse** to open the Choose File dialog box.

4 Browse to the location on your computer or network where the recorded script is located, select the file, and click **Open**.

Business Process Monitor scripts must be in **.zip** format.

5 Click **Upload** to upload the script.

Understanding the Script Repository

The Script Repository page lists the scripts that have been uploaded in the repository.

In Platform Administration, click **Data Collection** > **Script Repository** to open the **Script Repository** area with the **Business Process Monitor** tab selected.

You can view the following information – the same information is displayed in the **Business Process Monitor** tab:

- **Script Name.** The name of the script. Click the script name to open the **.zip** files or the **.obs** files that comprise the transaction. For details, see "Editing Scripts" on page 271.
- **Owner.** The name of the last user who updated the script.
- **Version.** The current version of the script. Double-click the version to modify it. For details, see "Displaying Script Versions" on page 272.
- **Status.** The status of the verification process for the script. Double-click the status to modify it. For details, see "Understanding the Script Verification Results" on page 274.
- **Last Update**. The date when the script was last updated.

You can:

- Download a special Virtual User Generator by clicking **Click to download HP Virtual User Generator**. For details, see "Recording Business Process Monitor Scripts" on page 269.
- 
Open the **.usz** file directly in the Virtual User Generator (if you have installed it) by clicking **Edit**. For details, see below.
- 
Manually verify the script by clicking **Manually Verify**. For details, see "Manually Verifying the Script" on page 274.
- Upload the script from the Script Repository page by clicking **Upload**. For details, see "Uploading Scripts" on page 269.
- 
Refresh the displayed information by clicking **Refresh**. The data is refreshed from the server (from the database that stores the list of scripts).

Editing Scripts

You can access Business Process Monitor scripts stored in the repository by clicking the script name link and saving the script to a local or network drive. You can then edit the file at a later time using the Virtual User Generator or you can open the file using any program that supports the **.zip** format.

You can view information about the script version (for details, see "Displaying Script Versions" on page 272).

You can view the conditions under which the script verification ran, and the actual result of each condition (for details, see "Manually Verifying the Script" on page 274 and "Understanding the Script Verification Results" on page 274).

After editing a script, you must upload it again to the repository. Business Process Monitor scripts must be zipped before being uploaded. After you upload the edited script, HP Business Availability Center reruns the verification process on the script.

HP Business Availability Center indicates the update date and time of editing in the Last Update column.

Displaying Script Versions

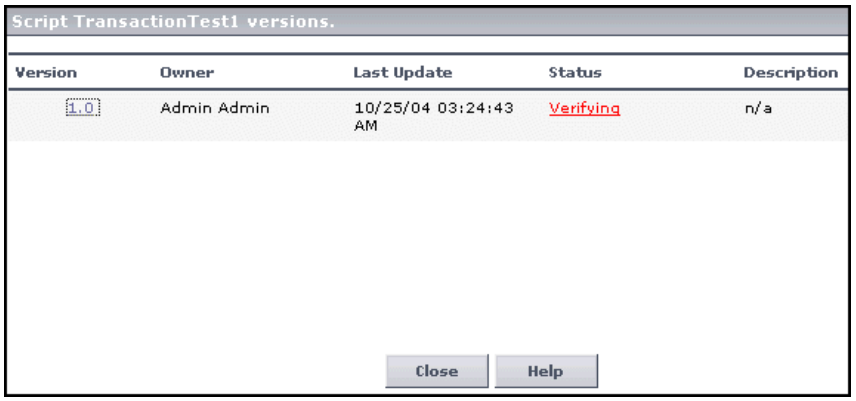
You can use the Script <script-name> versions page to track changes made to scripts and to access them to perform changes.

The Script <script-name> versions page displays the history of the script. Each time you upload the script, a new line is added to this list and the version is incremented.

To select a previous version of the script you must download it and upload it again; it then becomes the current version.

To display the list of versions of a script

1 In the **Script Repository** area, click the script version to open the Script <script-name> versions page.



2 View the following information:

Version – The version of the script. Click the version to open the scripts, which are stored in **.zip** format if they are Business Process Monitor scripts. The current version is underscored.

- **Owner.** The name of the last user who updated the script.
- **Last update.** The date when the script was last updated.
- **Status.** The status of the script. Click the status to open the Script Verification Results page. For details, see "Manually Verifying the Script" on page 274.
- **Description.** The description of the script. The description is useful for version control: you can describe why changes were made to this version of the script.

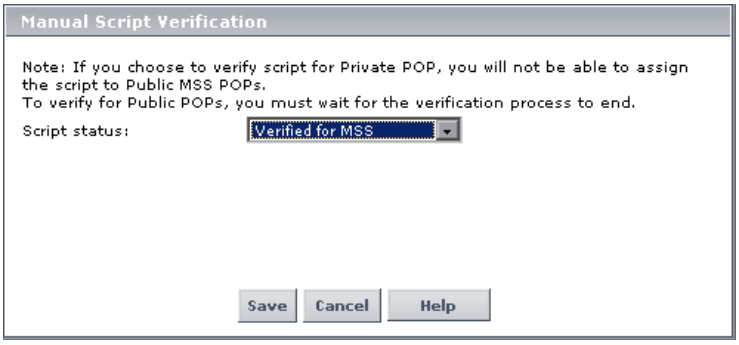
3 Click **Close** to close the page.

Manually Verifying the Script

You can use this page to change the verification status of a script and to remove a script from use.

To manually verify the script:

1 In the **Script Repository** area, click **Manually Verify** to open the Manual Script Verification page.



2 Select the appropriate **Script status**:

- **Verified for private POP.** Select this status for scripts that you want to verify for use on your private Business Process Monitor.
- **Verification failed.** Select this status to disable a transaction before running your profile.
- **Verified for MSS.** Select this status to enforce script to be verified for MSS (for operators and superusers only).

3 Click **Save** to save the changes.

Understanding the Script Verification Results

After you upload a script to the script repository, HP Business Availability Center runs a verification process to verify that the script executes properly when it is run in a profile. Once the script passes verification, HP Business Availability Center displays the **Passed** status in the Status column. You can add a script to a profile only after it passes verification.

You can check the verifications for which your transaction failed in the script <script-name> versions page.

The complete list of conditions is as follows:

Running Verifications	Rule	Actual Result
Disallowed function calls: system;lr_load_dll	Do not use the function calls that are listed.	Lists the actual function calls used in the script.
Download size must be less than 3000000 bytes	The maximum size of the download.	Indicates the actual download size.
Execution must be less than 300 seconds	The maximum execution time of the script.	Indicates the actual execution time of the script.
Expected protocol: QTWeb; NCA; WinSock; Sap_web; SapGui; Siebel_Web; HTTP; SOAP; PS8; PS8WebJS; WinSockWeb; Oracle_NCA; OracleWebJS; WebJS; WinSockWeb; Tulip; Citrix_ICA; OracleWebJS; General-vbs; General-Js SMTP; POP3; IMAP; Oracle; ODBC; FTP; EJB-Testing; MLDAP; Rmi-Java; Java_protocols	Only use the listed protocol types.	Indicates the actual protocol type used in the script.
Extra files with the following extensions are allowed: ini;h;tst	Only use extra files with the listed extensions.	Lists the actual extensions used in the script.
Failed transactions are disallowed	Do not use failed transactions.	Indicates whether there were failed transactions in the script.
Maximum number of dynamic transactions allowed:0	Do not use more dynamic transactions than the allowed maximum number.	Indicates the number of dynamic transactions in the script. Dynamic transactions are the transactions that are not defined in the USR file; meaning their name has been generated dynamically (for example: Transaction + i == Transaction 1,Transaction 2, and so forth).

Running Verifications	Rule	Actual Result
Maximum number of iterations allowed:1	Do not use more iterations than the allowed maximum number.	Indicates the number of time each action in a script is run. Every script is composed of actions (.c code files) which can be run more than once during one running of the script (a feature used mainly in LoadRunner and not in HP Business Availability Center). This iteration number must be limited so that duplicate transactions are not reported.
Maximum number of transaction instances allowed:1	Do not use more transaction instances than the allowed maximum number.	Indicates the number of transaction instances in the script.
Maximum number of transactions allowed:100	Do not use more transaction than the allowed maximum number.	Indicates the number of transactions in the script.
Total size must be less than 600000 bytes	The maximum total size of the script.	Indicates the actual total size of the script.

Note: The verification process differs depending on the contents of the script. Some scripts may go through a subset of the verifications listed above.

If any of these verification checks are not applicable to your organization, contact HP Managed Software Solutions Support.

To view the script verification results

1 In the Script <transaction-name> versions page, click the value in the **Status** column to open the Script Verification Results page.

2 You can view the following information:

- **Expected/Allowed Value Verifications.** Lists the conditions for the script verification.
- **Actual results.** The current results of the verification.
- **Description.** The description of the verification.
- **Status.** The status of the verification. Possible values are: Passed, Warning, or Failed.

3 Click **Close** to close the page.

Notifying Recipients of Script Verification

Note: This section applies only to Business Process Monitor scripts.

You can instruct HP Business Availability Center to send e-mail notification to specified recipients when Business Process Monitor script verification is complete.

To send e-mail notification when verification is complete:

1 In the **Verification Subscription** area, check the **Notify the following recipients when script verification is complete** check box.

2 Specify one or more e-mail addresses of the recipients in the **E-mail address(es)** box, separated by semi-colons.

3 Click **Apply**.

Package Information

Package information includes information about the customer package. This information is entered in the HP Business Availability Center application when the HP Managed Software Solutions contract is signed.

You can use the Package Information page for:

- Viewing Package Information (for details, see page 278)
- Selecting Locations for Business Process Monitors (for details, see page 279)
- Viewing and Modifying Package Properties Information (for details, see page 280)

Viewing Package Information

You can view information about the package name, expiration date, Business Process Monitor transactions, URLs, and POPs.

To view package information:

1. Select **Admin** > **Platform** > **Data Collection** > **Package Information** to open the **Package Information** area.
2. View the following information:
   - **Name.** The name of the package.
   - **Expiration.** The expiration date. The expiration date becomes red 14 days before the expiration date of a paying customer package, and 7 days before the expiration date of an evaluation customer package. For details, see "Viewing and Modifying Package Properties Information" on page 280.
   - **Business Process Monitor Transactions.** The total number of Business Process Monitor transactions that can be run as part of the package.
   - **URLs.** The total number of single URLs monitors that can be accessed as part of the package.

- **Global POPs.** The total number of global POPs that can be run as part of the package.
- **Private POPs.** The total number of private POPs that can be run as part of the package.

3 You can:

- Click **Package Location** to open the Package Locations page. For details, see "Selecting Locations for Business Process Monitors" on page 279.

- Click **Edit** to open the Package Properties page. For details, see "Viewing and Modifying Package Properties Information" on page 280.

Selecting Locations for Business Process Monitors

You can view the available Business Process Monitor locations on which to run the packages. You can also select, among all the possible locations, the appropriate Business Process Monitor locations up to the number specified by the customer package.

To view package location information or select locations for Business Process Monitors:

1 Select **Admin** > **Platform** > **Data Collection** > **Package Information** to open the **Package Information** area.

2 In the Package Information page, click **Package Location** to display the Package Locations page.

3 Select the appropriate locations, up to the number of locations allowed for your package.

4 Click **Save** to save the changes.

Viewing and Modifying Package Properties Information

The Package Properties page displays information about the customer package for specific applications (Business Process Monitor and SiteScope). This information is entered in HP Business Availability Center when the contract is signed with HP. You can modify only the subscribed recipients.

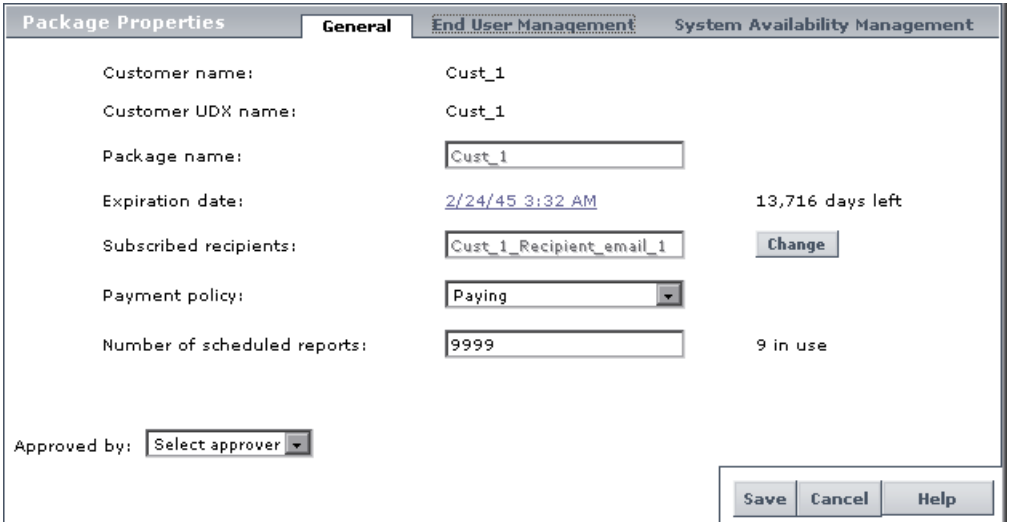
Modifying the Subscribed Recipients and Viewing the General Package Properties Information

The **General** tab in the Package Properties area displays general information about the package.

To modify the subscribed recipients and view the general package properties information:

1 Select **Admin** > **Platform** > **Data Collection** > **Package Information** to open the Package Information area.

2 In the Package Information page, click **Edit** to display the Package Properties page. Click the **General** tab:



3 You can view the names of the recipients who will receive package expiration notices via e-mail in the **Subscribed recipients** field. Click **Change** to open the Select Recipients page. For details, see "Assigning Recipients" on page 215.

- If you are a paying customer, the appropriate recipient will receive a package expiration notice via e-mail 14 days before the due date.
- If you are an evaluation customer, the appropriate recipient will receive a package expiration notice via e-mail 7 days before the due date.

4 You can also view the following information:

- **Customer name.** The name of the customer.
- **Package name.** The name of the package.
- **Expiration date.** The expiration date of the package. The number to the right of the box indicates the number of days left before the package expiration date.
- **Number of scheduled reports.** Number of scheduled reports included in the package. The number to the right of the box indicates the number of scheduled reports that have already been configured.

5 Click **Save** to save your changes.

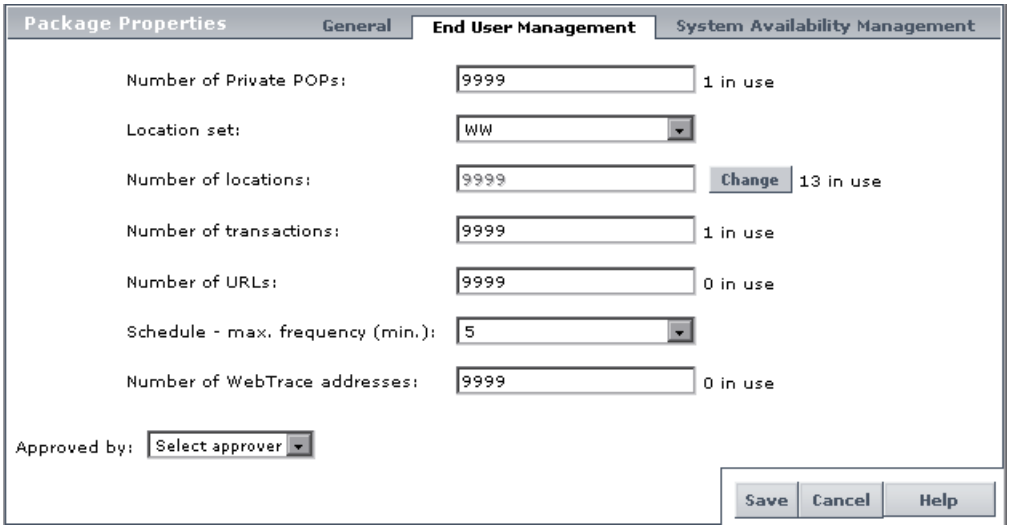
Viewing End User Management Package Properties Information

The **End User Management** tab in the Package Properties area displays package information related to End User Management.

To view End User Management package properties information:

1 Select **Admin** > **Platform** > **Data Collection** > **Package Information** to open the Package Information area.

2 In the Package Information page, click **Edit** to display the Package Properties page. Click the **End User Management** tab:



3 View the following information:

- **Number of private POPs.** The number of private POPs allowed for this package. The number to the right of the box indicates the number of private POPs already in use.
- **Number of locations.** The number of locations allowed by the package. The number to the right of the box indicates the number of locations already in use.
- **Number of transactions.** The number of transactions allowed by the package. The number to the right of the box indicates the number of transactions already in use.

- **Number of URLs.** The number of single URLs monitors allowed by the package. The number to the right of the box indicates the number of URLs already in use.
- **Schedule - max. frequency (min.).** The maximum frequency in minutes that your profiles can be scheduled to run.
- **Number of WebTrace addresses.** The number of WebTrace addresses allowed for this package. The number to the right of the box indicates the number of WebTrace addresses already being monitored.

4 Click **Save** to save your changes.

Viewing System Availability Management Package Properties Information

The **System Availability Management** tab in the Package Properties area displays package information related to SiteScopes.

To view System Availability Management package properties information:

1 Select **Admin** > **Platform** > **Data Collection** > **Package Information** to open the Package Information area.

2 In the Package Information page, click **Edit** to display the Package Properties page. Click the **System Availability Management** tab.

3 You can view the following information:

- **Number of System Availability Management profiles.** The number of System Availability Management profiles allowed for this package. The number to the right of the box indicates the number of System Availability Management profiles already in use.

4 Click **Save** to save your changes.

Part IV

Scheduled Reports

16

Scheduled Reports

You can configure HP Business Availability Center to send reports at predefined times to specific users.

About Scheduled Reports

You configure scheduled reports to enable specific recipients to automatically receive performance reports, via e-mail, at regularly defined intervals. You configure scheduled reports in the Platform Administration area of the Administration Console.

You can schedule the following reports to be sent:

- **User report.** A report based on one of the user reports (custom or trend report) defined in the End User Management, Service Level Management, or System Availability Management applications. For details on configuring user reports, see "Creating User Reports" on page 19 in *Custom Reporting and Alerting*.

➤ **Performance Update report.** A summary report of key performance data for a specified Business Process profile. For details on the Performance Update report, see "The Performance Update Report" on page 295.

Note: By default, the value that appears in the **From** field in the e-mail containing the scheduled report is **HPBAC_Alert_Manager@<HP Business Availability Center server name>**. You can modify the value by selecting **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** and the **Scheduled Reports** context. Modify the value **E-mail sender** or **Scheduled Reports e-mail sender address** (to include an e-mail address in the From field). For details on modifying values, see "Editing Infrastructure Settings" on page 81.

Scheduling User Reports or the Performance Update Report

You configure scheduled reports by defining which type of report to send, the frequency with which the report is sent, to whom the report is sent, and in what format the generated report is delivered.

For details on managing scheduled reports, see "Managing Scheduled Reports" on page 293.

Note: To correctly view scheduled reports received in Microsoft Outlook 2003, in **Tools** > **Options** > **Security** > **Zone Settings**, select **Internet**; click Custom Level and specify the following settings in the Security Settings dialog box: **Download signed ActiveX control** = **Prompt, Run ActiveX controls and plug-ins** = **Enable, Script ActiveX controls marked safe for scripting** = **Enable**; in the **Reset to** list, select **Medium**.

To schedule a user-defined report or Performance Update report:

1 Select **Admin** > **Platform** > **Scheduled Reports**.

2 If you are scheduling a Performance Update report, select the profile upon which you want to base the scheduled report.

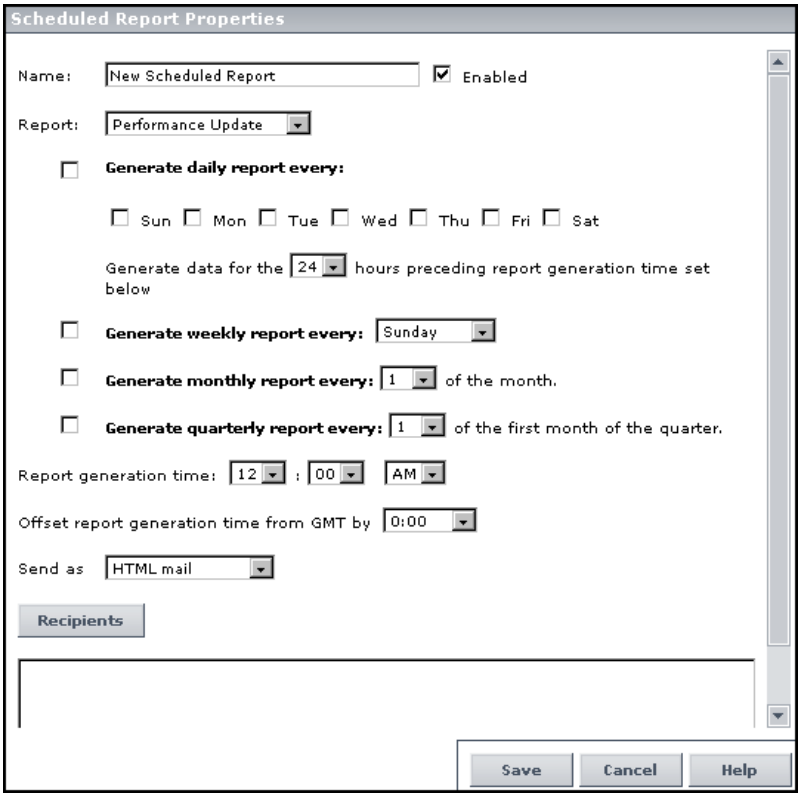
If you are scheduling a user-defined report (custom or trend report), select a profile to which the scheduled report is assigned for internal management purposes. You can choose any profile, but keep in mind that if you later delete that profile, the scheduled report is then not sent.

You can only schedule a user-defined report (custom or trend report) if you have defined one in the End User Management, Service Level Management, or System Availability Management applications. For details on configuring user reports, see "Creating User Reports" on page 19 in *Custom Reporting and Alerting*.

Important: The heading on the Scheduled Reports page reads **Scheduled Reports - User-Defined Reports**, whether or not you have actually configured a user-defined report.

---

3 Click **New Scheduled Report** to open the Scheduled Report Properties dialog box.



4 In the **Name** box, specify a name for the report, for example, “Kim’s daily update of MyProfile.”

5 De-select the **Enabled** box if you want to disable the report. By default, the **Enabled** box is selected.

6 In the Report list, select either Performance Update or one of the listed user-defined reports. If no user-defined reports exist, only the Performance Update is listed.

Note: If you choose a user-defined report that is later deleted, after report deletion, the scheduled report is not sent.

---

7 Select a schedule for the report. You can choose from any of the following options (you must choose at least one):

- To send a report on a daily basis, select **Generate daily report every** and the days of the week on which the report should be sent.

  You can also select how many hours of data are to appear in the report. The number of hours of data you indicate are the hours directly preceding the **Report generation time** set. The default is 24 hours of data.

- To send a report on a weekly basis, select **Generate weekly report every** and the day of the week on which the report should be sent.

- To send a report on a monthly basis, select **Generate monthly report every** and the day of the month on which the report should be sent. Note that, when necessary, months with less than 31 days are rounded down.

- To send a report on a quarterly basis, select **Generate quarterly report every** and the day of the first month of the quarter on which the report should be sent. Note that, when necessary, months with less than 31 days are rounded down.

8 From the **Report generation time** lists, select the time of day at which the report should be sent.

9 In the **Offset report generation time from GMT by** box, specify the time zone, relative to GMT, by which you want to offset the time at which the report is sent. For example, to specify Eastern Standard Time, type -5 since EST is equivalent to GMT -5:00.

For a reference list of GMT time zones for locations throughout the world, see "GMT Time Zones" on page 323 in *Reference Information*.

10 Specify whether to send the report as:

- **HTML mail.** The report is displayed in the e-mail client (the e-mail client must support, and be configured to display, HTML). All report resources (for example, graphics) are located on HP Business Availability Center servers. A network connection to HP Business Availability Center is required to view the report.
- **HTML attachment.** The report is displayed in a browser. All report resources (for example, graphics) are located on HP Business Availability Center servers. A network connection to HP Business Availability Center is required to view the report.
- **MHTML mail.** The report is displayed in the e-mail client (the e-mail client must support, and be configured to display, HTML). All report resources (for example, graphics) are included in the mail.
- **MHT attachment.** The report is displayed in a browser (the browser must support the MHT format—Microsoft Internet Explorer supports MHT format, for example). All report resources (for example, graphics) are included in the mail. Select **Zipped attachment** to send the report as a zipped attachment.
- **CSV mail.** The report is displayed in the e-mail client (the e-mail client must support, and be configured to display, HTML). All report resources (for example, graphics) are included in the mail.
- **CSV attachment.** The report is displayed in a program capable of displaying CSV format files (for example, Microsoft Excel). The report includes only tabular data and no graphics resources.
- **PDF attachment.** The report is displayed in PDF format in a new browser window. Select **Zipped attachment** to send the report as a zipped attachment.

Note: If you choose to use the HTML/MHTML mail option (which displays the report content in the e-mail client), make sure that the e-mail client does not employ security restrictions which prevent the running of scripts contained in HTML mail. E-mail clients that do employ such restrictions may be unable to properly display all report content.

---

11 Specify the report recipients by clicking the **Recipients** button and selecting the required recipients in the Select Recipients window. Click **OK** to save the settings and return to Scheduled Report Properties dialog box.

For details on configuring recipients, see "Recipients User Interface" on page 349.

12 Click **Save** to save settings and close the Scheduled Report Properties window. The scheduled report is added to the list.

Managing Scheduled Reports

You can edit scheduled reports, duplicate them, enable or disable them, delete them, and e-mail them on demand.

To edit a scheduled report:

1 Click the **Modify Scheduled Report** button to open the Scheduled Report Properties window.

2 Modify settings as required, and click **Save**.

To duplicate a scheduled report:

1 Click the **Duplicate Scheduled Report** button to open the Scheduled Report Properties window.

2 Specify a new name for the report, and modify report properties as required.

3 Click **Save**. The report is added to the report list.

Note: If the scheduled report is configured for a custom report that no longer exists, the report is not sent.

To enable a scheduled report:

1 Select one or more reports to enable them to be sent to recipients.

2 Click the **Enable Scheduled report** button at the bottom or side of the report list. Confirm that you want to enable the scheduled report(s).

3 Click **OK** in the dialog box.

To disable a scheduled report:

1 Select one or more reports to disable them so that they are not sent to recipients.

2 Click the **Disable Scheduled report** button at the bottom or side of the report list. Confirm that you want to disable the scheduled report(s).

3 Click **OK** in the dialog box.

To delete a scheduled report:

1 Select one or more scheduled reports to delete.

2 Click the **Delete Scheduled Report(s)** button at the bottom or side of the report list. Confirm that you want to delete the scheduled report(s).

To e-mail a scheduled report:

1 Select one or more scheduled reports to e-mail.

2 Click the **E-mail Scheduled Report(s)** button at the bottom or side of the report list to open the Send Scheduled Report Now window.

3 For each selected report, modify the recipients and report time frame, or accept the default values.

4 Click **Send** to send the report.

17

The Performance Update Report

The Performance Update report is a summary report of key performance data for the transactions in a specific profile. The Performance Update report is a scheduled report sent via e-mail.

About the Performance Update Report

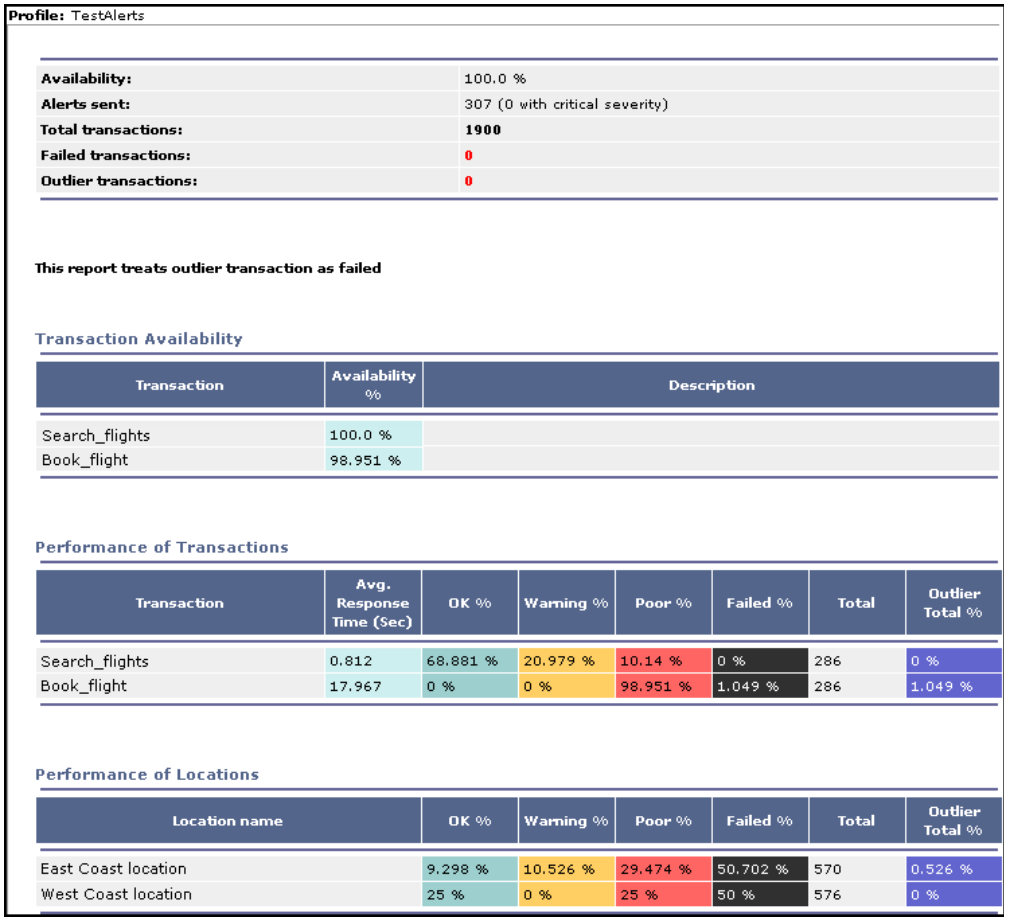
The Performance Update report is a scheduled report that is configured to be sent to specified recipients, via e-mail, on a periodic basis. The report includes key metrics on the performance of the transactions and locations defined in a specific profile.

For details on scheduling the Performance Update report, see "Scheduling User Reports or the Performance Update Report" on page 288.

You can also add components of the Performance Update report to custom reports. For details, see "Creating User Reports" in *Custom Reporting and Alerting*.

Viewing the Performance Update Report

You view the Performance Update report either in your e-mail client or in a Web browser.



Profile: TestAlerts

Availability:	100.0 %
Alerts sent:	307 (0 with critical severity)
Total transactions:	**1900**
Failed transactions:	**0**
Outlier transactions:	**0**

This report treats outlier transaction as failed

Transaction Availability

Transaction	Availability %	Description
Search_flights	100.0 %	
Book_flight	98.951 %	

Performance of Transactions

Transaction	Avg. Response Time (Sec)	OK %	Warning %	Poor %	Failed %	Total	Outlier Total %
Search_flights	0.812	68.881 %	20.979 %	10.14 %	0 %	286	0 %
Book_flight	17.967	0 %	0 %	98.951 %	1.049 %	286	1.049 %

Performance of Locations

Location name	OK %	Warning %	Poor %	Failed %	Total	Outlier Total %
East Coast location	9.298 %	10.526 %	29.474 %	50.702 %	570	0.526 %
West Coast location	25 %	0 %	25 %	50 %	576	0 %

You view the following information in the Performance Update report:

- **Report title and frequency.** Displays the title of the report, and in parentheses the report frequency.

  Time zone and time frame for report. Displays the configured time zone relative to GMT, as well as the time frame of the report (for a reference list of GMT time zones for locations throughout the world, see "GMT Time Zones" on page 323 in *Reference Information*).

- **Profile name.** Displays the Business Process profile upon which the report is based.
- **Availability.** Displays the percentage of transactions that succeeded (did not fail) during the measured period.
- **Alerts sent.** Displays the total number of alerts sent, including the number of critical severity alerts, for the measured period.
- **Total transactions.** Displays the total number of transactions run during the measured period.
- **Failed transactions.** Displays the total number of failed transactions for the measured period.
- **Outlier transactions.** Displays the total number of outlier transactions for the measured period.
- **Outlier transaction reporting status.** Describes whether HP Business Availability Center ignores outlier transactions in reports, or treats them as failed transactions (this setting is defined during profile definition in End User Management Administration).
- **Transaction Availability.** Displays the availability rate for each transaction in the profile, for the measured period. If a description of the transaction is set, the description is displayed (this setting is defined during transaction monitor configuration in End User Management Administration).

- **Performance of Transactions.** Displays, for the measured period and for each transaction, average transaction response time, the percentage of transaction instances that fell into each defined transaction threshold range, (OK, Warning, and Poor), the percentage of failed transaction instances, the total number of transaction instances, and the percentage of outlier transaction instances.
- **Performance of Locations.** Displays, for the measured period and for each location, the percentage of transactions that fell into each defined transaction threshold range, (OK, Warning, and Poor), the percentage of failed transaction instances, the total number of transactions, and the percentage of outlier transactions.

  You define transaction thresholds—to specify the OK, Warning, and Poor range for each transaction—when you create a profile. You can also modify the transaction threshold ranges, as well as the default outlier value of 45 seconds, from End User Management Administration. For details, see "Editing Business Process Transaction Monitors" on page 94 in *Using End User Management*.

Part V

User Management

18

User Management Overview

You use the User Management interface to configure groups and users, along with their respective permissions. You can set user and group hierarchy by adding users to groups and nesting groups within other groups. Additionally, you can customize the settings of all users in the system.

Getting Started

Before you configure the User Management portal, you should map out the required users and user groups and their relevant permission levels before defining them in HP Business Availability Center. For example, in a spreadsheet enter the following information:

- a list of all staff who will be required to administer the system, as well as the end users who will be accessing Dashboard and reports. Gather appropriate user details such as user names, login names, initial passwords, and user time zones. Although not needed to define users, at this stage it might be useful to also collect user contact information such as telephone number, pager, or e-mail address (contact information is required for HP Managed Software Solutions customers).

- if categorization of users into modes (operations and business) is required, specify into which user mode to categorize each user. For details, see "KPIs for User Modes" in Dashboard Administration.
- if groups of users will require similar system permissions, a list of user groups and the users that should belong to each group.
- the permissions each user or user group will require. To aid in this process, review the Permissions Management page to learn about the different contexts and resources for which permissions can be granted. For details, see "Understanding Permissions Resources" on page 317.

Accessing User Management

You access User Management in HP Business Availability Center by clicking **Admin > Platform > Users and Permissions > User Management.**

The User Management interface is available only to users with appropriate permissions. A user's permissions are either inherited from their assigned role (i.e. - Administrator, System Viewer) or granted individually when their parameters are configured. For details on permissions, see "Understanding Roles and Operations" on page 320.

User Management Workflow

The recommended workflow for working with User Management is:

Step 1: Create Groups

You create groups to make managing user permissions more efficient. Instead of assigning access permissions to each user one at a time, you can group users who are assigned the same permissions levels on the same resources. For details on creating groups, see "Group Management" on page 305.

Step 2: Assign Permissions to Groups

HP Business Availability Center enables you to apply permissions to groups and users for specific resources and instances of those resources that are defined in the system. For details, see "Permissions Management" on page 311.

Step 3: Create Users

You create users and then place them into the appropriate groups, depending on how you want to organize the users. For details, see "Creating Users" on page 365.

Step 4: Configure User and Group Hierarchy

In the Hierarchy tab, you set user and group hierarchy by adding users to groups and nesting groups within other groups. For details, see "Configuring User and Group Hierarchy" on page 375.

Step 5: Customize User Settings

In the Customization tab, you customize the menu items that are displayed in different contexts for users. For details, see "Customizing User Menus" on page 381.

This workflow is recommended because it lets you automatically adopt permissions from your respective groups, without having to configure permissions for individual users and then again for the groups. You can configure your User Management settings in any other logical order you choose.

General Tab

The General tab displays the settings of the group or user selected in the Browse tab of the Left pane. In the General tab, you can view the settings configured after creating a group or user, and you can update an existing group or user's settings.

- ➤ For details on creating groups, see "Defining New Groups" on page 307.
- ➤ For details on managing groups, see "Managing Groups" on page 308.
- ➤ For details on creating users, see "Defining New Users" on page 366.
- ➤ For details on managing users, see "Managing Users" on page 368.

19

Group Management

HP Business Availability Center enables you to create groups of users and groups of groups (nested groups) for increased flexibility in managing accessibility to the platform.

Introducing Group Management

You group users to make managing user permissions more efficient. Instead of assigning access permissions to each user one at a time, you can group users who are assigned the same permissions levels on the same resources.

Grouping Criteria

You may want to create different groups based on how users access the different resources in HP Business Availability Center. Examples of criteria for grouping users that are relevant to your organization may be:

Tasks Within the Organization	Locations and Territories
Customer service representatives	Users working in different sales territories
System administrators	Users based on geographical location
High-level management	Users accessing network servers in different locations

Nesting Groups

You can nest groups to make managing user and group permissions easier. Instead of assigning access permissions to each group one at a time, you can nest a group to inherit the permissions of its direct parent.

For details, see “Nested Groups Management” on page 375.

Defining New Groups

You define and manage groups in the Groups/Users section of the User Management interface, on the left side of the page. The access permissions are inherited by the users of the group.

The group name is the unique identifier for the user group.

To define a new group:

1 Click the **Create User/Create Group** button in the Groups/Users window.

2 Select **Create Group**.

3 Type a group name in the Group name box.

Note: For the group name, all special characters are allowed except the following: " \ / [ ] : | < > + = ; , ? *

---

4 Type a description for the group in the Group description box.

5 Click **OK** to save the group.

The group appears in the Groups/Users list on the left side of the screen.

You now can grant permissions for your groups. For details, see "Permissions Management" on page 311.

To copy settings of an existing group to a new group:

1 Select the group whose settings you wish to copy.

2 Click the **Clone** button in the Groups/Users window. The Create Group box appears, with the description of the source group appearing in the Group description box.

3 Type a group name in the Group name box.

4 Click **OK** to save the group. The group appears in the Groups/Users list on the left side of the screen.

Managing Groups

You can change the name or description of a group, and you can delete existing groups. You can also expand and collapse groups in the Browse tab of the Groups/Users window to view or hide users contained within the group.

Use the Search tab in the Groups/Users window to search for a specific group or user.

To change the name and/or description of an existing user group:

1 Select the group you want to edit in the Browse tab of the Groups/Users window and click the **General** tab on the right side of the screen.

2 Edit the group name and/or group description in the appropriate box.

3 Click **OK** to save the changes.

To delete existing user groups:

1 Select the group you want to delete in the Browse tab of the Groups/Users window and click the **General** tab on the right side of the screen.

2 Click the **Delete** button and click **OK** to confirm the deletion. HP Business Availability Center deletes the user group.

To expand or collapse groups and view/hide users contained in the group:

1 Select the group you wish to expand or collapse in the Browse tab of the Groups/Users pane.

2 Click the **Expand Groups** or **Collapse Groups** button.

3 If you clicked the **Expand Groups** button, the users contained within the group are visible. If you clicked the **Collapse Groups** button, the users within the group are hidden.

To search for a specific group or user:

1. Click the **Search** tab in the Groups/Users window.
2. Select **Search for users** or **Search for groups** to view a list of users or groups.

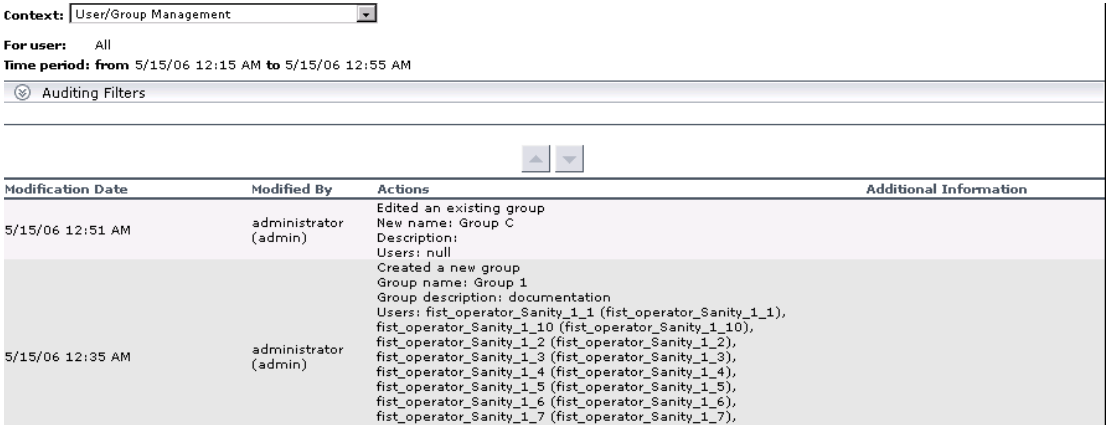
3. Enter the group or user information in the appropriate cell to search either by Login name, User name, or Last Login, and press ENTER.
4. Click on the user or group whose details you want to view. The details appear in the General tab in the right pane.

Notes and Limitations

- You can sort the columns by clicking on the column headers above the boxes.
- When selecting more than one user or group and modifying parameters, the changes only take effect for the first selected user. The exception is the Delete option, which deletes multiple users at once.
- You can include wildcards (*) in your search.
-  You can delete a group or user by clicking the Delete button after performing step 4.

To check user and group activity in the audit log:

You access the Audit Log by selecting **Admin** > **Platform** > **Setup and Maintenance** > **Audit Log.** The Audit Log contains information about all user and group activity. For details, see “Understanding the Audit Log” on page 209.



20

Permissions Management

HP Business Availability Center enables you to apply permissions to groups and users for specific resources and instances of those resources that are defined in the system.

Introducing Permissions

You can enable sophisticated and detailed permissions scenarios for the groups defined in your HP Business Availability Center platform. Permissions are based on both the user who is granted the permission and the resource on which the permission is granted.

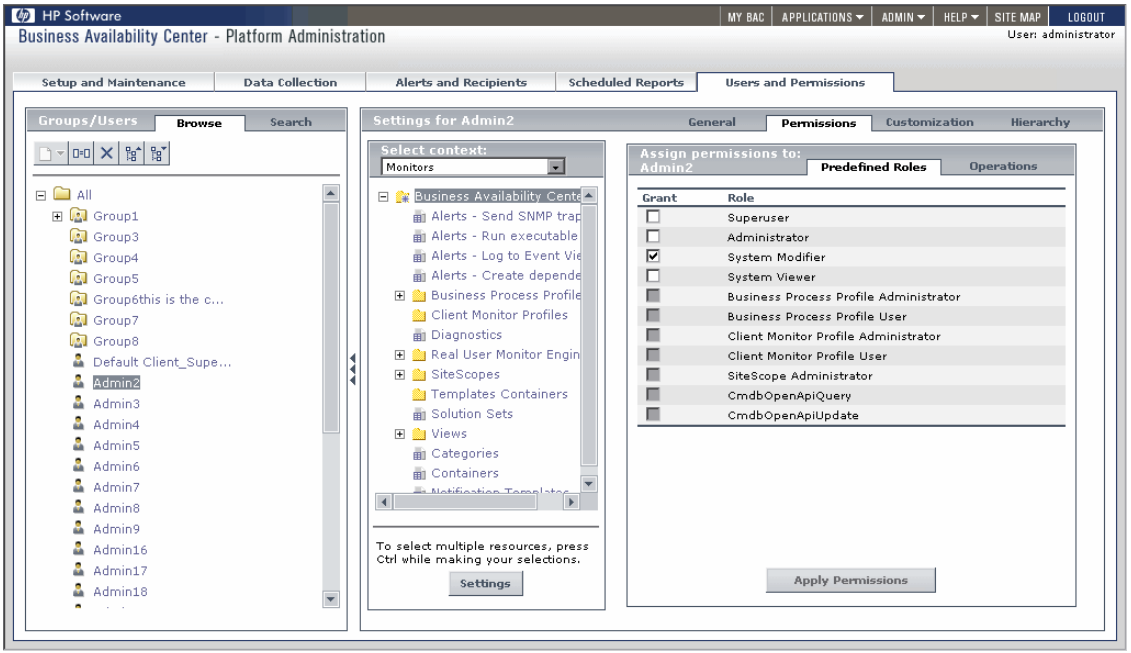
Granting permissions has three components:

- The user
- The resource
- The operation or role being granted

The Permissions tab is divided into two main areas:

- resource tree area in the center of the page
- roles and operations area on the right side of the page

Additionally, the Groups/Users pane is continually visible on the left side of the page.



To grant or remove permissions, you must select a user or group, select a context, select a resource, and check the operations or roles to apply. For details, see “Granting and Removing Permissions” on page 313.

Note: If you have upgraded from a previous version of HP Business Availability Center and had specific users and security levels defined, those users and security levels are mapped to the new roles functionality in Permissions Management. For details, see “Roles” on page 321.

Granting and Removing Permissions

Before granting and/or removing permissions on the resources in HP Business Availability Center, you should:

- determine for which users or groups you will be applying permissions (for details, see "Understanding Permissions Resources" on page 317)
- understand the various contexts and resources available in HP Business Availability Center (for details, see "Understanding Permissions Resources" on page 317)
- select whether you will be applying operations or roles to the users and/or groups (for details, see "Understanding Roles and Operations" on page 320)

Note: For the applied permissions to take effect, the user for whom permissions have been granted or removed must log out and log in again to HP Business Availability Center.

When granting permissions to users or groups on the resources in the Permissions tab, keep the following in mind:

- You can grant permissions to only one user or group at a time.
- Assigning **Add** permissions on the Operations tab **does not** automatically grant **View** permissions on the given resource.
- If you have many users for whom you have to grant permissions, it is recommended that you organize your users into logical groups using the Hierarchy tab (for details, see "Managing Group Members" on page 377).

To apply permissions:

1 In User Management, select the **Permissions** tab.

2 Select a user or group in the Groups/Users pane on the left side of the page.

Note: You can grant permissions to only one group or user at a time.

---

3 Select a context from the context list box above the resource tree in the center of the page. The resource tree displays the resources included in the selected context.

Note: The Business Availability Center resource appears as the top level of every context and can have only roles applied to it.

---

4 Optionally, click **Settings** at the bottom of the resource tree. The Apply Permissions Settings dialog box opens and you can configure the settings for this session of applying permissions. For details, see "Apply Permissions Settings" on page 316.

5 Highlight the resources to which you want to apply permissions. You can press Ctrl to make multiple selections in the resource tree.

Note: You can only select multiple resources when selecting instances. For information on instances, see "Resources and Resource Instances" on page 318.

---

6 Select the **Predefined Roles** tab or the **Operations** tab on the right-hand side of the page.

7 If you are applying predefined roles, select the applicable role for the highlighted resource.

If you are applying operations, select from the available operations for the highlighted resources. Depending on the resources highlighted, you can select the **Inherit** check box for the operation to be inherited to all the child resources within the selected resource.

Note: The **Granted from Group/Role/Parent** column displays those permissions that have been granted from either a group, a predefined role, or a parent resource. You cannot remove any of these permissions individually, but you can grant additional permissions. If you want to remove permissions that are granted from a group, role, or parent resource, you must make the change at the group, role, or parent resource level.

---

8 If, in step 4 on page 314, you chose to apply permissions automatically when selecting another resource, either select another resource or click **Apply Permissions**. If you did not choose this option, you must click **Apply Permissions** for the permissions to take effect. Repeat as necessary for other resources and users.

Apply Permissions Settings

You can apply specific permissions settings for configurations in your User Management session.

To configure settings for this session of applying permissions:

1 In the **Permissions** tab, click **Settings** at the bottom of the resource tree. The Apply Permissions Settings dialog box opens.

2 Select from the following options to change the settings by which Permissions Management functions:

- **Apply permissions automatically when selecting another resource.** Selecting this option removes the necessity for clicking the **Apply Permissions** button after each operation. If this option is not selected, you must click **Apply Permissions** before going on to the next operation.
- **Do not display warning message when revoking VIEW from resource.** When the view operation is removed from a resource for a user, that user has no access to the resource or to any of its child resources or instances. Therefore, by default, a warning message appears when removing view permissions. Selecting this option will disable that warning message.

3 Click **Close** to save your settings and continue applying permissions.

Note: When you select the settings for applying permissions, the options selected apply only to the current HP Business Availability Center session.

Understanding Permissions Resources

HP Business Availability Center enables you to finely tune your permissions management by applying permissions at the resource level. All of the resources on which permissions can be applied have been identified and categorized in a hierarchical tree, representing the HP Business Availability Center platform.

The resources and instances of those resources are organized according to logical groupings called **contexts**. Contexts make it easier to identify and select the area of the platform on which you want to apply permissions.

Resource Contexts

The resources are divided according to the context in which they function within the platform and not necessarily where they are found in the user interface.

While applying permissions, you select resources from the following contexts:

- **CMDB.** Includes the view resources for the CMDB in IT Universe
- **CMDB Open API.** Includes the extraction of data from the CMDB for use with third-party or custom tools or to write data to the database
- **Central Scripts Repository.** Includes the storage location of all BPM scripts
- **Monitors.** Includes all the resources relating to data collection and monitoring
- **My BAC.** Includes resources needed to administer modules and portlet definitions
- **Platform.** Includes all the resources for administering the platform
- **Production Analysis.** Includes all the resources relating to Application Performance Lifecycle (APL)

- **Service Level Management.** Includes the SLA resource
- **User Defined Reports.** Includes the custom report, trend report, custom link, and Excel report resources

For a detailed table, divided by context, describing how each operation is applied to each resource within each context, see "Operations" on page 337.

Resources and Resource Instances

There are three types of resources in Permissions Management. Each is represented by a different icon in the resource tree:


- resource collection (a resource that can have instances)


- instance of a resource


- resource that cannot have instances in the permissions resource tree

An instance of a resource is displayed only if it has been defined in the platform. The instance of a resource appears as a child object of the resource in the tree with the name as it has been defined in the application. Once instances of a resource are defined in the system, the resource collection acts as the parent resource for those instances.

There are some resources, such as the different data collector profiles, that contain other resources within them in the resource tree hierarchy. Some of these sub-resource types appear only if there are instances of the resource defined in your platform, such as Monitor and Transaction resources within a profile resource.

Examples of Resources and Instances

An example of how resources and instances are displayed in the permissions hierarchy is the Business Process Profile resource within the Monitors context. The Business Process Profile resource includes instances only if there have been Business Process profiles defined in the system. If there are profiles defined in the system, each of those appears as an instance of the Business Process Profile resource with the name defined for the profile in End User Management Administration.

Because monitors, transactions, and alerts are defined in your platform per profile, the Monitors, Transactions, and Alerts resources appear under each of the instances of the profile resource. Monitors and Transactions are resource collections and can have their own instances, but Alerts is a resource that cannot have instances.

You can apply permissions to the Business Process Profile resource level. This enables the user access to all Business Process profiles created in the system. If you want to restrict a user's access to specific Business Process profiles that relate to the user's tasks, you can apply permissions to a specific Business Process profile, to the Monitors resource or to any instance of monitors that have been defined under the profile.

Guidelines for Working with Resources

- The Business Availability Center resource refers to all contexts in HP Business Availability Center.
- Only roles can be applied to the Business Availability Center resource. For details, see "Roles" on page 321.
- To manage the permissions on a subresource, you must provide the user with at least **View** permissions on the selected resource's parent.
- You cannot grant **Add** permission on an instance of a resource, only on the resource itself.
- When a user defines or creates an instance of a resource, such as a Business Process profile, that user has **Full Control** permission on that resource instance and all of its child resources.
- Resources that cannot have instances in the permissions tree are divided into the following two types:

- Resources that are functions or options within the system that do not have any other instances or types.

  For example, the outlier value resource determines whether the user can edit the outlier threshold value. It has no instances.

- Resources that do have instances but permissions can be applied only on the resource type and affect all instances of the resource.

  For example, the category resource includes all categories defined in End User Management Administration. **Change** permissions granted on the categories resource enables a user to modify all the categories defined in the system. You cannot grant or remove permissions for specific categories, only for every category defined in End User Management Administration.

Understanding Roles and Operations

You can grant permissions to groups and users by selecting one of the two tabs in the roles and operations area of the Permissions Management page:

- **Predefined Roles.** Use to apply a collection of operations that have been predefined for various resources. For a detailed description of each role, including which operations are applied to what resources, see "Roles" on page 321.
- **Operations.** Use to apply specific operations on a resource for a user or group. For a detailed table of what each operation enables as it is applied to each resource, see "Operations" on page 337. When assigning operations, you can see the descriptions listed below as tooltips under the operations area. They appear when a resource is highlighted and you move your cursor over an operation.

Roles

HP Business Availability Center enables you to apply permissions using predefined roles for specific users or groups in your organization. These roles include a preconfigured collection of resources and a set of operations that apply to those resources.

Each role defined appears below with a table, listing by context which resources and which operations have been preconfigured and included in the role.

Roles can be applied only to specific resources:

- Roles that include resources from several contexts can be applied only to the Business Availability Center resource. Business Availability Center appears as the first resource collection in every context.
- Roles whose resources are all within one context can be applied to specific resources within that context.

Details of the resources on which roles can be applied appear within the description of each role below. Some of the resources are applicable to HP Managed Software Solutions customers only and are listed as such.

Note to users of previous versions of HP Business Availability Center: If you had users and permission levels defined in your previous version, those users and some of the applicable permissions levels have been upgraded to the current version and mapped to the roles in HP Business Availability Center. Under each role listed below is a note indicating the corresponding permission level from Topaz 4.5 Feature Pack 2 or earlier.

Superuser

The superuser role can be applied only to the Business Availability Center resource.

This role includes all available operations on all the resources in all the contexts. Only a superuser can apply the superuser role to another user.

Administrator

The administrator role can be applied only to the Business Availability Center resource.

An administrator has a collection of permissions that enable adding profiles to the system, and managing the resources related to those profiles. Once a profile is added, the administrator has full control privileges on all resources within that profile instance.

Context	Resource	Operation
CMDB	Views	Full Control
Central Repository Service	Root Folder and Sub Level Folders	Full Control
Monitors	Categories	Add
	Containers	Full Control
	Filters	Add
	Template Containers	Add
	Template	Add
	Diagnostics	Full Control
	Business Process Profile	Add
	Real User Monitor	Add
	SiteScope	Add
	SiteScope Group	Add
	SiteScope Preferences	Add
	Solution Sets	Full Control

Context	Resource	Operation
Platform	Audit Log	Full Control
	Database	Full Control
	Data Collectors	Change
		View
	Recipients	Full Control
	Scheduled Reports	Full Control
	Users	Full Control
	User Groups	Full Control
Service Level Management	SLAs	Full Control
User Defined Reports	Custom Links	Full Control
	Custom Reports	Full Control
	Default Header/footer	Full Control
	Excel Reports	Full Control
	Trend Reports	Full Control
My BAC	Manage Modules page	Full Control
	Manage Portlet Definitions page	Full Control

System Modifier

The system modifier role can be applied only to the Business Availability Center resource.

A system modifier can view and change any and all of the resources within HP Business Availability Center. There are some resources on which the view or the change operation is not applicable. A system modifier has permissions for only those operations that are available in HP Business Availability Center.

A system modifier does not have full control privileges on any resource and therefore, cannot grant or remove permissions for other users.

Context	Resource	Operation
CMDB	Views	View
		Change
Central Repository Service	Root Folder and Sub Level Folders	View
		Full Control
Monitors	Alerts (Business Process)	View
		Change
	Alerts - Create Dependency	Change
	Alerts - Log Event	Change
	Alerts - Run Executable File	Change
	Alerts - SNMP	Change
	Monitors (Business Process)	View
		Change
	Categories	View
		Change
	Containers	Change

Context	Resource	Operation
Monitors	Filters	View
		Change
	Template Containers	View
		Change
	Template	View
		Change
	Diagnostics	View
		Change
	Business Process Profile	View
		Change
	Real User Monitor Engines	View
		Change
	Alerts (Real User Monitor)	View
		Change
	End User (Real User Monitor)	View
		Change
	Engine Settings (Real User Monitor)	View
		Change
	Pages (Real User Monitor)	View
		Change
	Transactions (Real User Monitor)	View
		Change
	SiteScope	View
		Change
	SiteScope Group	View
		Change

Context	Resource	Operation
Monitors	SiteScope Preferences	View
		Change
	Solution Sets	Change
	Notification Templates	View
		Change
	Outlier Value (Business Process)	Change
	Transactions (Business Process)	View
		Change
Platform	Audit Log	View
	Databases	Change
		View
	Data Collectors	View
		Change
	Recipients	View
		Change
	Sample Type	Change
		View
	Scheduled Reports	Change
		View
	Users	Change
		View
	User Group	Change
		View
Service Level Management	SLAs	Change
		View

Context	Resource	Operation
User Defined Reports	Custom Links	View
		Change
	Custom Reports	View
		Change
	Default Header/footer	Change
	Excel Reports	View
		Change
	Trend Reports	View
		Change

System Viewer

The system viewer role can be applied only to the Business Availability Center resource.

A system viewer can only view resources within HP Business Availability Center and has no permissions to change, add, or delete any resources or resource instances. There are some resources on which the view operation is not applicable. A system viewer has no access to those resources.

Context	Resource	Operation
CMDB	Views	View

Context	Resource	Operation
Monitors	Alerts (Business Process)	View
	Monitors (Business Process)	View
	Categories	View
	Filters	View
	Template Containers	View
	Templates	View
	Diagnostics	View
	Business Process Profile	View
	Real User Monitor Engines	View
	Alerts (Real User Monitor)	View
	End User (Real User Monitor)	View
	Engine Settings (Real User Monitor)	View
	Pages (Real User Monitor)	View
	Transactions (Real User Monitor)	View
	SiteScope	View
	SiteScope Group	View
	SiteScope Preferences	View
	Notification Templates	View
	Transactions (Business Process)	View

Context	Resource	Operation
Platform	Audit Log	View
	Database	View
	Data Collectors	View
	Recipients	View
	Sample Types	View
	Scheduled Reports	View
	Users	View
	User Group	View
Service Level Management	SLAs	View
User Defined Reports	Custom Links	View
	Custom Reports	View
	Excel Reports	View
	Trend Reports	View

Business Process Profile Administrator

The Business Process profile administrator role can be applied to only the Business Process Profile resource or specific instances of the profile resource.

When granted this role at the resource collection level, the Business Process profile administrator can manage all of the platform's Business Process profiles, including permissions on all the profiles. When granted this role at the instance level, the administrator can manage only those resources associated with the specific Business Process profile instance.

Any administrator who was added as a user on a specific Business Process profile in the previous version is upgraded to the Business Process profile administrator role for that profile. This is in addition to being assigned the administrator role as described above (for details, see "Administrator" on page 322).

Context	Resource	Allowed Operations
Monitors	Business Process Profile	Full Control
	Monitor	Full Control
	Transaction	Full Control
	Alert	Full Control

Business Process Profile User

The Business Process profile user role can be applied to only the Business Process Profile resource or specific instances of the profile resource.

These users have view permissions, but can modify transaction threshold settings and transaction descriptions.

Any regular user who was added as a user on a specific Business Process profile in the previous version is upgraded to the Business Process profile user role for that profile.

Context	Resource	Allowed Operations
Monitors	Business Process Profile	View
	Monitor	View
	Transaction	View
		Change
	Alert	View

SiteScope Administrator

The SiteScope administrator role can be applied to only the SiteScope resource or specific instances of the resource.

When granted this role at the resource collection level, the SiteScope administrator can manage all of the platform's SiteScopes, including permissions on the SiteScopes. When granted this role at the instance level, the administrator can manage only those resources associated with the specific SiteScope instance.

Any administrator who was added as a user on a specific SiteScope in the previous version is upgraded to the SiteScope administrator role for that SiteScope.

Context	Resource	Allowed Operation
Monitors	SiteScopes	Full Control
	Groups (SiteScope)	Full Control
	SiteScope Preferences	Full Control

CmdbOpenAPIQuery

The CmdbOpenAPIQuery role can be applied to only the cmdb.open_api resource.

This role enables users to query the CMDB (Configuration Management Database) for communication with third-party applications.

Context	Resource	Allowed Operation
CMDB Open API	cmdb.open_api	View
		Change

CmdbOpenApiUpdate

The CmdbOpenApiUpdate role can be applied to only the cmdb.open_api resource.

This role enables users to update the CMDB (Configuration Management Database) for communication with third-party applications.

Context	Resource	Allowed Operation
CMDB Open API	cmdb.open_api	View
		Change

Customer Superuser

Note: This role can be applied to HP Managed Software Solutions customers only.

The customer superuser role can be applied to only a specific instance of the customer resource. The customer resource is available only to HP Managed Software Solutions customers and represents the customer level in the permissions resource tree. It is available in all contexts and applies to all contexts (like the Business Availability Center resource). The customer superuser is granted full control on all the resources and instances that belong to that customer. These include all resources, instances of those resources, and child resources under the customer resource.

Context	Resource	Allowed Operation
CMDB	Views	Full Control

Context	Resource	Allowed Operation
Monitors	Alerts	Full Control
	Alert - Create Dependency	Full Control
	Notification Templates	Full Control
	Diagnostics	Full Control
	Monitors (Business Process)	Full Control
	Categories	Full Control
	Containers	Full Control
	Filters	Full Control
	Template Containers	Full Control
	Template	Full Control
	Business Process Profile	Full Control
	Real User Monitor Engines	Full Control
	Alerts (Real User Monitor)	Full Control
	End User (Real User Monitor)	Full Control
	Engine Settings (Real User Monitor)	Full Control
	Pages (Real User Monitor)	Full Control
	Transactions (Real User Monitor)	Full Control
	SiteScope	Full Control
	Groups (SiteScope)	Full Control
	SiteScope Preferences	Full Control
	Solution Sets	Full Control
	Outlier Value (Business Process)	Full Control
	Transactions (Business Process)	Full Control

Context	Resource	Allowed Operation
Platform	Audit Log	Full Control
	Hosts	Full Control
	Package Information	Full Control
	Recipients	Full Control
	Scheduled Reports	Full Control
	Script Repository	Full Control
	System Tickets	Full Control
	Users	Full Control
	User Groups	Full Control
Service Level Management	SLAs	Full Control
User Defined Reports	Custom Links	Full Control
	Custom Reports	Full Control
	Default Header/Footer	Full Control
	Excel Reports	Full Control
	Trend Reports	Full Control
My BAC	Manage Modules page	Full Control
	Manage Portlet Definitions page	Full Control

Customer Administrator

Note: This role can be applied to HP Managed Software Solutions customers only.

The customer administrator role can be applied to only a specific instance of the customer resource. The customer resource is available only to HP Managed Software Solutions customers and represents the customer level in the permissions resource tree. It is available in all contexts and applies to all contexts (like the Business Availability Center resource).

The customer administrator is granted full control on a selection of resources, as well as either view, execute, or both on other resources. This user can add profiles of any type, and has full control on the created profile. However, the user is not granted permissions for profiles that were created by other users, even if these profiles are for the same customer. In the case of the My BAC resources, any user with this role can make changes to resources defined by other users.

Context	Resource	Allowed Operation
CMDB	Views	Full Control

Context	Resource	Allowed Operation
Monitors	Alerts	View
	Diagnostics	View
		Execute
	Categories	Add
	Containers	Full Control
	Filters	Add
	Template Containers	Add
	Templates	Add
	Business Process Profile	Add
	RUM	Add
	SiteScope	Add
	Groups (SiteScope)	Add
	SiteScope Preferences	Add
	Solution Sets	Full Control
Platform	Audit Log	Full Control
	Package Information	Full Control
	Recipients	Full Control
	Scheduled Reports	Full Control
	Script Repository	Full Control
	System Tickets	Full Control
Service Level Management	SLAs	Full Control

Context	Resource	Allowed Operation
User Defined Reports	Custom Links	Full Control
	Custom Reports	Full Control
	Default Header/Footer	Full Control
	Excel Reports	Full Control
	Trend Reports	Full Control
My BAC	Manage Modules page	Full Control
	Manage Portlet Definitions page	Full Control

Operations

When working with operations, keep the following in mind:

- All of the operations that can be applied to a resource collection can also be applied to any instance of that resource. The one exception is the **Add** operation which cannot be applied to an instance of a resource.
- The **Full Control** operation automatically includes all the other operations available on the resource. When applied, the other operations are automatically selected.
- When the **Full Control** operation is applied to any resource, the user also has permissions to grant and remove permissions on that resource, or resource instance, for other users or groups.
- When the **View** operation is one of the resource's available operations and you select one of the other available operations, the **View** operation is also automatically selected.

Within each context listed below is a table listing:

- every resource
- which operations can be applied to that resource
- a description of what the operation enables

CMDB

The **CMDB** context enables you to define the operations permitted for the views defined in IT Universe Administration and viewed in the View Explorer, Dashboard, and Service Level Management.

Tip: If a user has permissions on a view in CMDB, all the profiles that are in that view are visible to the user, even if the user does not have permissions on the profile. To prevent a user from viewing profiles for which the user does not have permissions while enabling the user to access a view, create a view for the user including only those configuration items for which you want the user to have permissions and grant the user permission on that view.

Resources	Operation	Description
Views	Add	Enables adding views in the View Manager, and creating Enrichments, Correlations, Queries, and Reports in UCMDB.
	Change	Enables adding a configuration item or relationship to a view, editing the view in the View Manager, and if user is the creator of the view, removing configuration items or relationships from the view. Enables modifying of Enrichments, Correlations, Queries, and Reports in UCMDB.
	View	Enables viewing the configured views in read-only mode, and viewing of Enrichments, Correlations, Queries, and Reports in UCMDB.
	Delete	Enables deleting views from the View Manager and deleting of Enrichments, Correlations, Queries, and Reports in UCMDB.
	Full Control	Enables performing all available operations on the views in the view Manager and IT Universe Admin, viewing all views in the applications, and granting and removing permissions for those operations. Also enables performing of all available options for Enrichments, Correlations, Queries, and Reports in UCMDB, and the granting of permissions to other UCMDB users.

Resources	Operation	Description
CMDB	Full Control	Enables performing all available operations on the CMDB, and granting and removing permissions to access the CMDB.

Central Repository Service

The **Central Repository Service** context enables you to define the operations permitted for the folders under the Root folder. Operations assigned to a folder affect all folders contained beneath it.

Monitors

Resources	Operation	Description
Central Repository Service	View	Enables downloading scripts and reports into the Central Repository Service.
	Full Control	Enables performing all available operations on the folders in the Central Scripts Repository: view, edit, and delete any script or subfolder in the folder.

The **Monitors** context includes all those resources that relate to data collection and monitoring. These resources can be found in Platform Administration and End User Management Administration.

The profile resources (Business Process and SiteScope) determine the permissions level of the user in all areas of the platform where you must select a profile to access the page or perform the action. These include most areas of End User Management Administration, Alert Management, Downtime/Event Scheduling, Transaction Ordering, Transaction Coloring, and various Reports.

Some of the resources listed appear only when instances of the parent resource have been defined in the platform. For example, the Monitors and Transactions resources appear only as child objects of an instance of a Business Process Profile.

Resources	Operation	Description
Alerts - Send SNMP Trap	Change	Enables selecting the option to send SNMP traps on alert, editing SNMP trap addresses, and clearing the option to send SNMP traps on alert
	Full Control	Enables performing all available operations on sending SNMP traps on alerts, and granting and removing permissions for those operations
Alerts - Run Executable File	Change	Enables selecting the option to run an executable file on alert, selecting and editing executable files to run on alert, and clearing the option to run an executable file on alert
	Full Control	Enables performing all available operations on running an executable file on alert, and granting and removing permissions for those operations
Alerts - Log to Event Viewer	Change	Enables selecting whether alerts should be logged in the Windows Event Viewer, which is accessed from Windows Administrative Tools
	Full Control	Enables selecting whether alerts should be logged in the Windows Event Viewer, and granting and removing permissions on that operation

Resources	Operation	Description
Alerts - Create Dependencies	Change	Enables creating and removing dependencies between alerts
	Full Control	Enables creating and removing alert dependencies, and granting and removing permissions for those operations
Business Process Profiles	Add	Enables creating Business Process profiles
	Change	Enables renaming Business Process profiles and modifying profile properties
	View	Enables viewing the Business Process profile details in End User Management Administration, and the Business Process profile in any application that lists the profiles, such as Alert Management, Service Level Management, Downtime/Event Scheduling, Analytics, and reports
	Delete	Enables deleting Business Process profiles
	Execute	Enables running and stopping Business Process profiles
	Full Control	Enables performing all available operations on Business Process profiles, and granting and removing permissions for those operations

Resources	Operation	Description
Monitors (under Business Process Profile instance)	Add	Enables adding transaction monitors, WebTrace monitors, and single URL monitors (Managed Services only) to Business Process profiles
	Change	Enables editing transaction monitor, WebTrace monitor, and single URL monitor (Managed Services only) properties
	View	Enables viewing transaction monitor, WebTrace monitor, and single URL monitor (Managed Services only) properties
	Delete	Enables deleting transaction monitors, WebTrace monitors, and single URL monitors (Managed Services only) from the profile
	Full Control	Enables performing all available operations on transaction monitors, WebTrace monitors, and single URL monitors (Managed Services only), and granting and removing permissions for those operations
Transactions (under Business Process Profile)	Change	Enables editing transaction descriptions and threshold settings
	View	Enables viewing transaction details
	Full Control	Enables performing all available operations on transactions, and granting and removing permissions for those operations

Resources	Operation	Description
Outlier Value (under Business Process Profile > Transaction instance)	Change	Enables setting a transaction's outlier value
	Full Control	Enables setting the transaction's outlier value, and granting and removing permissions for that operation
Alerts (under Business Process Profile instance)	Add	Enables adding alerts to the Business Process profile
	Change	Enables editing details of alerts associated with the Business Process profile
	View	Enables viewing alerts in the Business Process profile and viewing alert details in Alerts Management
	Delete	Enables deleting alerts associated with the Business Process profile
	Full Control	Enables performing all available operations on the alerts in the Business Process profile, and granting and removing permissions for those operations

Resources	Operation	Description
Diagnostics	Change	Enables viewing Diagnostics administration and configuring the Diagnostics settings
	View	Enables viewing the Diagnostics application when accessing Diagnostics from the Business Application Center
	Execute	Enables changing the settings in the HP Diagnostics UI, such as setting thresholds
	Full Control	Enables performing all operations on Diagnostics, and granting and removing permissions for those operations
Real User Monitor Engines	Add	Enables adding Real User Monitor engines to End User Management Administration
	Change	Enables editing Real User Monitor engine details
	View	Enables viewing Real User Monitor engine details
	Delete	Enables removing Real User Monitor engines from End User Management Administration
	Full Control	Enables performing all available operations on Real User Monitor engines, and granting and removing permissions for those operations

Resources	Operation	Description
Engine Settings (under Real User Monitor Engine instance)	Change	Enables editing the Real User Monitor preferences details
	View	Enables viewing the preferences of a Real User Monitor engine
	Full Control	Enables performing all available operations on Real User Monitor engines, and granting and removing permissions for those operations
Domains (under Real User Monitor Engine instance)	Add	Enables adding the Real User Monitor to general settings
	Change	Enables editing the Real User Monitor general settings
	View	Enables viewing the general settings of a Real User Monitor engine
	Delete	Enables deleting a domain from a Real User Monitor Engine
	Full Control	Enables performing all available operations on Real User Monitor general settings, and granting and removing permissions for those operations

Resources	Operation	Description
RUM Applications (under Real User Monitor Engine instance)	Add	Enables adding applications to a Real User Monitor engine, and pages and transactions to an application
	Change	Enables editing the Real User Monitor application, page, and transaction details
	View	Enables viewing the Real User Monitor application, page, and transaction
	Delete	Enables deleting a page or transaction from a Real User Monitor application or a Real User Monitor application from a container or RUM engine instance
	Full Control	Enables performing all available operations on a Real User Monitor application, page, and transaction, and granting and removing permissions for those operations
Alerts (under Real User Monitor Engine instance)	Add	Enables adding alerts to a Real User Monitor engine
	Change	Enables editing Real User Monitor alert properties
	View	Enables viewing the properties of a Real User Monitor alert
	Delete	Enables deleting an alert from a Real User Monitor engine
	Full Control	Enables performing all available operations on Real User Monitor alerts, and granting and removing permissions for those operations

Resources	Operation	Description
SiteScope	Add	Enables adding SiteScopes and SiteScope profiles to Monitor Administration
	Change	Enables modifying SiteScope and SiteScope profile properties and attaching a SiteScope to, or detaching it from, Monitor Administration
	View	Enables viewing SiteScope or SiteScope profile properties
	Delete	Enables deleting a SiteScope profile from Monitor Administration
	Full Control	Enables performing all available operations on SiteScopes and SiteScope profiles, and granting and removing permissions for those operations
Template Containers	Add	Enables adding a container for templates to the End User Management Administration enterprise
	Change	Enables modifying template container properties
	View	Enables viewing template container properties in End User Management Administration
	Delete	Enables deleting a template container from the End User Management Administration enterprise
	Full Control	Enables all available operations on template containers, and granting and removing permissions for those operations

Resources	Operation	Description
Solution Sets	Change	Enables editing the Solution Set container, and adding, editing, and deleting Solution Set template objects
	Full Control	Enables all operations on Solution Sets, and granting and removing permissions for those operations
Views	Add	Enables creating view filters in End User Management Administration
	Change	Enables editing view filter definitions in End User Management Administration
	View	Enables viewing view filter definitions in End User Management Administration
	Delete	Enables deleting view filters from End User Management Administration
	Full Control	Enables performing all available operations on view filters, and granting and removing permissions for those operations
Categories	Add	Enables creating a category in End User Management Administration
	Change	Enables editing End User Management Administration category definitions
	Delete	Enables deleting categories from End User Management Administration
	Full Control	Enables performing all available operations on End User Management Administration categories, and granting and removing permissions for those operations

Resources	Operation	Description
Containers	Add	Enables adding a container to the End User Management Administration enterprise
	Change	Enables renaming and modifying the properties of a container
	Delete	Enables deleting a container from End User Management Administration
	Full Control	Enables performing all available operations on an End User Management Administration container, and granting and removing permissions for those operations
Solution Sets	Change	Enables editing the Solution Set container, and adding, editing, and deleting Solution Set template objects
	Full Control	Enables all operations on Solution Sets, and granting and removing permissions for those operations

Resources	Operation	Description
Notification Templates (HP Managed Software Solutions only)	Add	Enables creating and cloning a customer-specific notification template
	Change	Enables editing the properties of a customer-specific notification template
	View	Enables viewing the properties of a customer-specific notification template
	Delete	Enables deleting a customer-specific notification template
	Full Control	Enables performing all available operations on a customer-specific notification template, and granting and removing permissions for those operations
Notification Templates	Add	Enables creating and cloning notification templates
	Change	Enables editing notification template properties
	View	Enables viewing notification template properties
	Delete	Enables deleting a notification template
	Full Control	Enables performing all available operations on notification templates, and granting and removing permissions for those operations

My BAC

The My BAC context enables you to assign permissions to work with the module and portlet definition pages in My BAC Administration.

Resources	Operation	Description
Modules	Full Control	Enables creating, editing, deleting, and performing all operations on the Manage Modules page
Portlet definitions	Full Control	Enables creating, editing, deleting, and performing all operations on the Manage Portlet Definitions page

Platform

The Platform context includes all the resources related to administering the platform. Some of the resources listed are available for HP Managed Software Solutions customers only, and are marked accordingly.

Resources	Operation	Description
Audit Log	View	Enables viewing the audit log
	Full Control	Enables viewing the audit log, and granting and removing permission to view the audit log
Users	Add	Enables adding users to the system
	Change	Enables modifying user details
	View	Enables viewing user details
	Delete	Enables deleting users from the system
	Full Control	Enables performing all available operations on users, and granting and removing permissions for those operations

Resources	Operation	Description
User Groups	Add	Enables adding user groups to the system
	Change	Enables modifying user group details
	View	Enables viewing user group details
	Delete	Enables deleting user groups
	Full Control	Enables performing all available operations on user groups, and granting and removing permissions for those operations
Data Collectors	Change	Enables performing remote upgrades, remote uninstalls, and settings updates on data collectors in Data Collector Maintenance
	View	Enables viewing the data collectors in Data Collector Maintenance
	Delete	Enables removing data collector instances
	Full Control	Enables performing all available operations in Data Collector Maintenance, and granting and removing permissions for those operations
System Tickets	View	Enables viewing system tickets details
	Execute	Enables executing system tickets in the system
	Full Control	Enables performing all available operations on System Tickets, and granting and removing permissions for those operations

Resources	Operation	Description
Scheduled Reports	Add	Enables creating new scheduled reports
	Change	Enables modifying scheduled reports
	View	Enables viewing scheduled reports
	Delete	Enables deleting scheduled reports
	Full Control	Enables performing all available operations on scheduled reports, and granting and removing permissions for those operations
Recipients	Add	Enables adding recipients to the platform
	Change	Enables editing recipient details
	View	Enables viewing recipients and recipient details
	Delete	Enables deleting recipients from the platform
	Full Control	Enables performing all available operations on recipients, and granting and removing permissions for those operations

Resources	Operation	Description
Custom Data Types	Add	Enables adding custom data types to the system
	Change	Enables modifying custom data types in the system
	View	Enables viewing custom data types in the system
	Delete	Enables deleting custom data types in the system
	Full Control	Enables full access permissions to Custom Data TypesMeasurement Filters page, and granting and removing permissions for those operations
Databases	Add	Enables adding profile databases to the system
	Change	Enables modifying profile database details in database management
	View	Enables viewing profile database management details
	Delete	Enables deleting profile databases from the system
	Full Control	Enables performing all available operations on profile databases in database management, working with the purging manager, and granting and removing permissions for those operations

Resources	Operation	Description
Script Repository (HP Managed Software Solutions only)	Add	Enables uploading new scripts to the script repository
	Change	Enables modifying scripts in the script repository
	View	Enables viewing scripts in the script repository
	Remove	Enables deleting a script from the script repository.
	Execute	Enables subscribing to script verification and verifying scripts for private POP only
	Full Control	Enables performing all available operations on scripts in the scripts repository, and granting and removing permissions for those operations
Package Information (HP Managed Software Solutions only)	Change	Enables modifying package locations, renaming packages, and selecting recipients for package notifications
	View	Enables viewing package information
	Full Control	Enables performing all available operations on package information, and granting and removing permissions for those operations
System Tickets (HP Managed Software Solutions only)	View	Enables viewing system ticket details
	Execute	Enables registering system notifications
	Full Control	Enables performing all available operations on system tickets, and granting and removing permissions for those operations

Production Analysis

Use the Production Analysis context to assign permissions to access the Production Analysis reports generating from the Application Performance Lifecycle application. These reports enable users to extract real-user transaction data to be used in Performance Center load tests and to create Virtual User Generator (VuGen) script templates, based on real-user activity.

Resources	Operation	Description
Production Analysis	Full Control	Enables accessing and downloading Production Analysis reports generated by Application Performance Lifecycle

System Availability Management Administration (SAM Admin)

Use the SAM Admin context to assign permissions to the various SiteScopes configured within the system.

Note: The permission levels granted via the System Availability Management Administration (SAM Admin) context override any permission levels granted in the SiteScope stand-alone interface.

Resources	Operation	Description
SiteScopes	Add	Enables adding SiteScope profiles to System Availability Management
	Change	Enables modifying a SiteScope profile in System Availability Management and enables adding the contents to the SiteScope root node (group, alert, report) and modifying contents to the SiteScope root node (alert, report), if the user has permissions for these resources
	View	Enables viewing SiteScope profiles in System Availability Management
	Delete	Enables deleting a SiteScope profile from System Availability Management and enables deleting the contents of the SiteScope root node (alert, report), if the user has permissions for these resources
	Execute	Enables executing contents of the SiteScope root node (alert, report), if the user has permissions for these resources
	Full Control	Enables performing all available operations on SiteScope profile and SiteScope root node

Resources	Operation	Description
SiteScope Groups	Change	Enables modifying and adding a SiteScope group and enables modifying and adding the contents of the group (monitor, alert, report), if the user has permissions for these resources
	View	Enables viewing the SiteScope group and all the objects contained within that group
	Delete	Enables deleting a SiteScope group and enables deleting the contents of the group (monitor, alert, report), if the user has permissions for these resources
	Execute	Enables executing SiteScope monitors, generating reports, and testing alerts contained within the group, if the user has permissions for these resources
	Full Control	Enables performing all available operations on the SiteScope group and all the objects contained within the group (monitor, alert, report), if the user has permissions for these resources
SiteScope Monitors	Change	Enables modifying, adding, deleting, disabling or enabling SiteScope monitors
	Execute	Enables executing SiteScope monitors, acknowledging SiteScope monitors from the Dashboard, and using monitor tools
	Full Control	Enables performing all available operations on SiteScope monitors

Resources	Operation	Description
SiteScope Alerts	Change	Enables modifying, adding, deleting and disabling SiteScope alerts
	Execute	Enables creating Adhoc alert reports and test SiteScope alerts
	Full Control	Enables performing all available operations on SiteScope alerts
SiteScope Preferences	Change	Enables modifying, adding, deleting, and viewing any of the Preference objects
	Execute	Enables executing tests of SiteScope preferences
	Full Control	Enables performing all available operations on SiteScope preferences
SiteScope Reports	Change	Enables modifying, adding, deleting, disabling, and enabling SiteScope reports
	Execute	Enables generating SiteScope reports
	Full Control	Enables performing all available operations on SiteScope reports
SiteScope Views	Change	Enables modifying, adding, and deleting SiteScope views
	View	Enables viewing predefined and user-defined SiteScope views
	Full Control	Enables performing all available operations on SiteScope views
SiteScope Categories	Change	Enables modifying, adding, and deleting SiteScope categories
	View	Enables viewing SiteScope categories
	Full Control	Enables performing all available operations on SiteScope categories

Resources	Operation	Description
SiteScope Templates	Change	Enables modifying, adding, and deleting SiteScope templates
	View	Enables viewing SiteScope templates and copying templates for deployment
	Full Control	Enables performing all available operations on SiteScope templates
SiteScope Other Options	View	Enables viewing SiteScope Progress and Logs
	Execute	Enables using SiteScope Tools, Browse and Summary
SiteScope Users	Change	Enables modifying, adding, and deleting user preferences for all other SiteScope users, except the SiteScope administrator user
SiteScope Dashboard	Change	Enables modifying Dashboard favorites

Service Level Management

Use the Service Level Management context to assign permissions to all SLAs or specific instances.

Resources	Operation	Description
SLAs	Add	Enables adding SLAs
	Change	Enables renaming SLAs, adding descriptions to SLAs, viewing SLA configuration in administration pages, and changing SLA configurations
	View	Enables generating and viewing reports and custom reports on SLAs
	Delete	Enables deleting SLAs
	Full Control	Enables performing all available operations on SLAs, and granting and removing permissions for those operations

UCMDB WS API

The **UCMDB WS API** context includes the resource cmdb.open_api.

You can give a user permissions so that they can query or update the CMDB using the CMDB API. This enables the user to write API methods to add, remove, and update CIs.

Resources	Operation	Description
cmdb.open_api	Change	Enables adding a configuration item or relationship to a view; editing the view in the View Manager; and if the user is the creator of the view, removing configuration items or relationships from the view
	View	Enables viewing the configured views in read-only mode

User Defined Reports

Use the User Defined Reports context to assign permissions to the various types of user-defined reports and related settings.

Resources	Operation	Description
Custom Reports	Change	Enables creating, editing, and deleting custom reports
	View	Enables viewing custom reports
	Full Control	Enables performing all available operations on custom reports, and granting and removing permissions for those operations
Trend Reports	Change	Enables creating, editing, and deleting trend reports
	View	Enables viewing trend reports
	Full Control	Enables performing all available operations on trend reports, and granting and removing permissions for those operations
Custom Links	Change	Enables creating and deleting custom links
	View	Enables viewing custom links
	Full Control	Enables performing all available operations on custom links, and granting and removing permissions for those operations
Excel Reports	Change	Enables adding, deleting, and updating Excel open API reports
	View	Enables viewing Excel open API reports
	Full Control	Enables performing all available operations on Excel open API reports, and granting and removing permissions for those operations

Resources	Operation	Description
Default Header/Footer	Change	Enables modifying the default header and footer for custom and trend reports
	Full Control	Enables modifying, and granting and removing permissions to modify, the default header and footer for custom and trend reports

21

Creating Users

You create users to provide individuals with access to HP Business Availability Center. A user has access to a variety of areas within the system, depending on the level of permissions they are granted.

You define and manage HP Business Availability Center users in the User Management page under the Users and Permissions tab of Platform Administration.

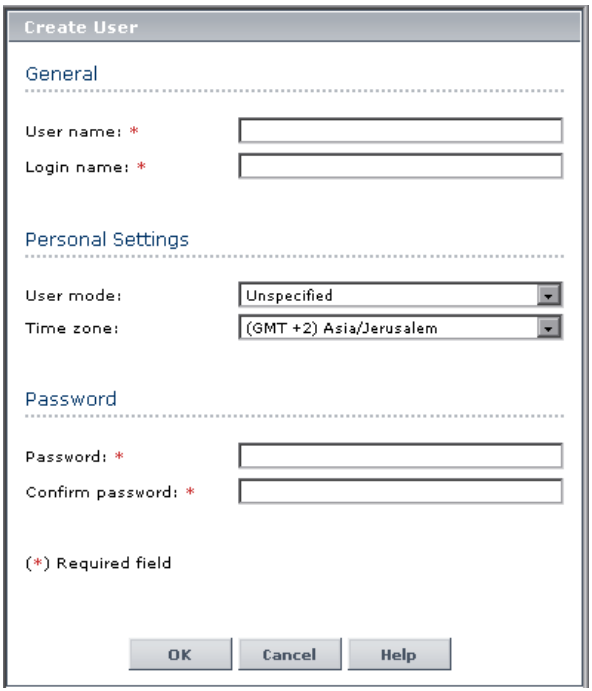
Defining New Users

You define new users by assigning them a user name, a login name, and a password. The login name is the unique identifier for the user.

To define a new user:

1 Select **Admin** > **Platform** > **Users and Permissions** > **User Management**. The User Management page opens.

2 Click the **Create User/Create Group** button in the Groups/Users pane on the left side of the page, and select **Create User.** The Create User dialog box opens.



3 Type a user name in the **User name** box.

4 Type a login name for the user in the **Login name** box. The user must use the assigned login name when accessing HP Business Availability Center.

Note: For both the user name and login name, the maximum number of characters you can enter is 50. All special characters are allowed except the following: " \ / [ ] : | < > + = ; , ? *

---

5 Select the **User Mode** for the user. Users see the KPI version appropriate for their user mode. For details, see "KPIs for User Modes" in *Using Dashboard*.

Select from the following options:

- **Unspecified.** Leaves the user without a particular mode. Select this option if:
  - HP Business Availability Center is working with user modes and you want this user to see KPIs for both modes in Dashboard views.
  - Your system is not working with user modes.
- **Operations User.** Enables the user to view the operations version of KPIs.
- **Business User.** Enables the user to view the business version of KPIs.

6 Select the appropriate time zone for the user from the **Time Zone** list.

7 Enter a valid e-mail address in the **E-mail** box.

Note: The E-mail field is available only for HP Managed Software Solutions customers.

---

8 Type a password in the **New Password** box, and retype it in the **Confirm Password** box to verify it.

9 Click **OK**. HP Business Availability Center adds the user name and properties to the existing users list.

To create additional users, repeat steps 2 through 9 above. Create as many new users as you need.

To copy settings of an existing user to a new user:

1 Select the user whose settings you wish to copy.

2 Click the **Clone** button in the Groups/Users window. The Create User box appears, with the description of the source group appearing in the User description box.

3 Type a user name in the User name box.

4 Click **OK** to save the user. The user appears in the Groups/Users list on the left side of the screen.

Managing Users

Once you have created users, you can use the User Management page to perform the following tasks:

- Rename a user – for details, see page 369
- Modify the user time zone – for details, see page 369
- Change a user's password – for details, see page 370
- Delete a user – for details, see page 371
- Modify the e-mail address (for MMS users only) - for details, see page 371
- Check user and group activity in the audit log - for details, see page 373

Note: One superuser is defined for every installation of HP Business Availability Center. This superuser's default login name and password are admin, admin. This original superuser is not listed among the users in User Management and, therefore, this user's password can be changed only in the Change Password page under Personal Settings (**Admin** > **Personal Settings**). For details, see "Configuring General Settings" on page 386.

The superuser permissions role can be applied to other users in the system. These users with superuser permissions are listed, and can be modified, in User Management. For details on applying permissions, see "Granting and Removing Permissions" on page 313.

To modify the user name, time zone, or user mode of an existing user:

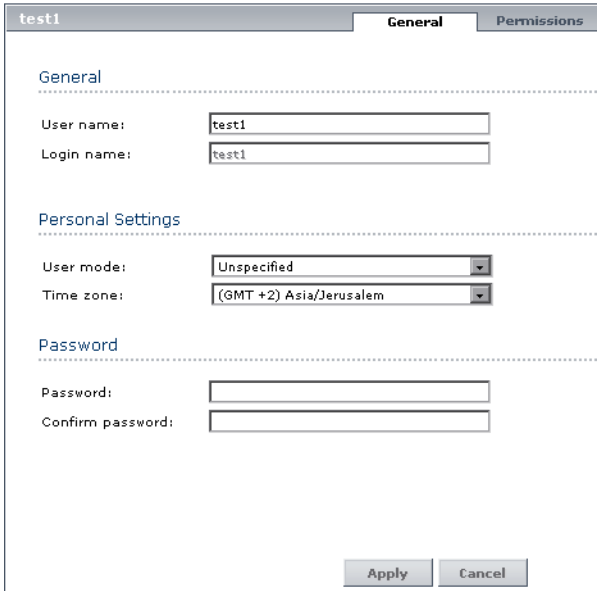
Note: This option is not available to HP Managed Software Solutions customers. Customers can change the user name and time zone settings from the Personal Settings area.

---

1 In Platform Administration, select **Users and Permissions** > **User Management**. The User Management page opens, displaying the list of existing users.

2 Select the user for whom you want to modify their name, time zone, or both.

3 Click the **General** tab to view the user details form and display the user's current user name, login name and time zone.



4 Modify the user name in the **User name** box and/or time zone in the **Time zone** box as required. Note that the login name is not editable.

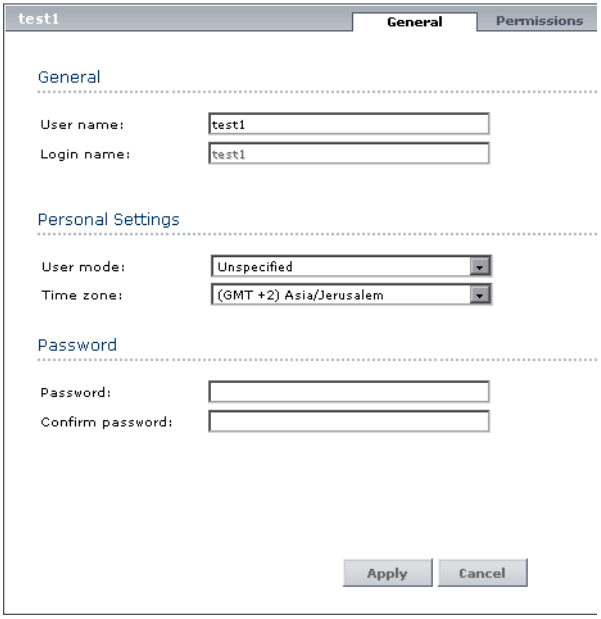
5 Click **OK** to save the changes.

To change an existing user's password:

Note: This option is not available to HP Managed Software Solutions customers. Customers can change passwords from the Personal Settings area.

---

1. In Platform Administration, select **Users and Permissions** > **User Management**. The User Management page opens, displaying the list of existing users.
2. Select the user whose password you want to modify.
3. Click the **General** tab to view the user details form and display the user's current password.



4. Enter the new password in the **Password** box and retype it into the **Confirm Password** box.
5. Click **Apply** to save the changes.

To delete an existing user:

1 In Platform Administration, select **Users and Permissions** > **User Management**. The User Management page opens, displaying the list of existing users.

2 Select the user you want to delete.

3 Click the **Delete** button and click **OK** to confirm that you want to delete the user. HP Business Availability Center deletes the user.

To modify an e-mail address:

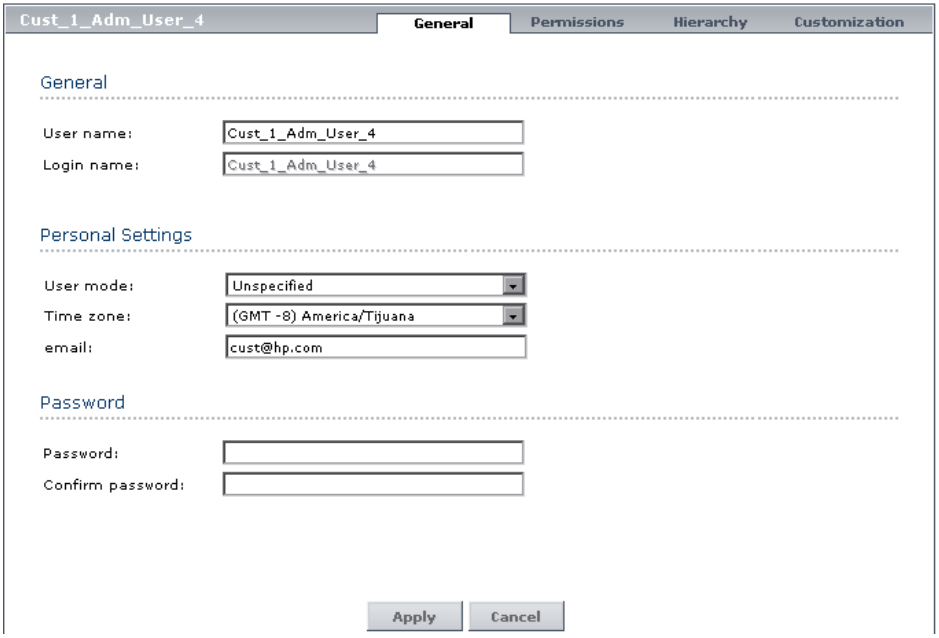
Note: The e-mail field is available only for HP Managed Software Solutions customers.

---

1 In Platform Administration, select **Users and Permissions** > **User Management**. The User Management page opens, displaying the list of existing users.

2 Select the user who's e-mail address you want to modify.

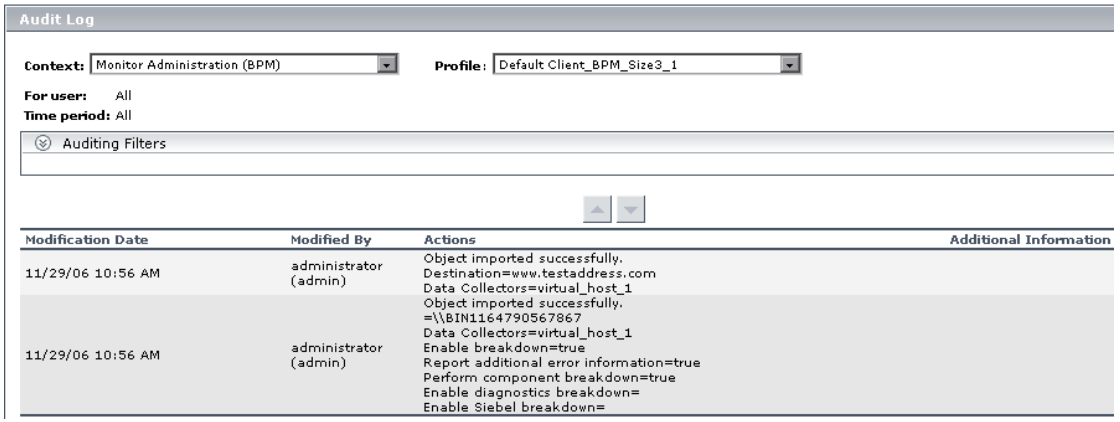
3 Click the **General** tab to view the user details form and display the user's current e-mail address.



4 Enter the new e-mail address in the **E-mail** box click **Apply** to save the change.

To check user and group activity in the audit log:

You access the Audit Log by selecting **Admin** > **Platform** > **Setup and Maintenance** > **Audit Log.** The Audit Log contains information about all user and group activity. For details, see "Understanding the Audit Log" on page 209.



22

Configuring User and Group Hierarchy

HP Business Availability Center enables you to add users to groups and to nest groups within other groups in the Hierarchy tab of the User Management interface.

Nested Groups Management

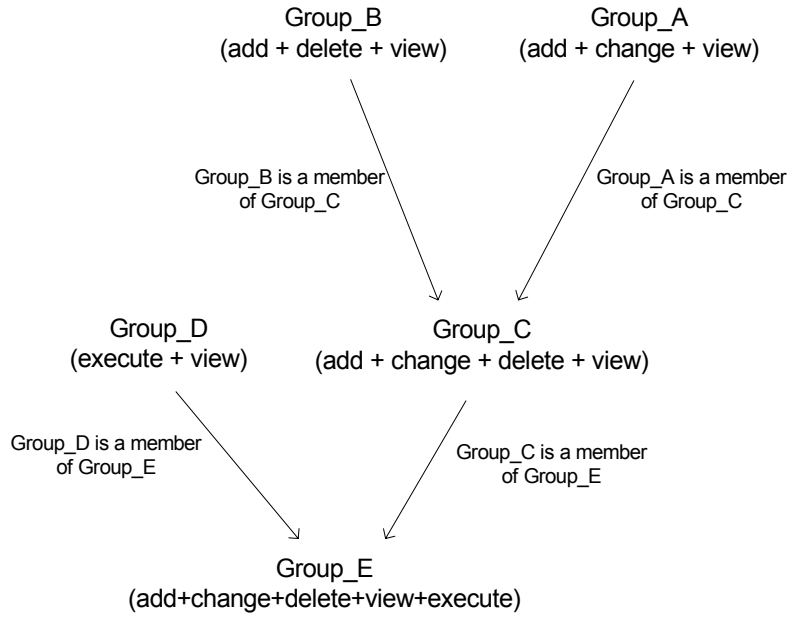
You can nest groups to make managing user and group permissions easier. Instead of assigning access permissions to each group one at a time, you can nest a group to inherit the permissions of its direct parent.

This section includes:

For information on setting up nested groups, see "Managing Group Members" on page 377.

An Example of Nested Groups

In the example below, Group_A and Group_B are nested members of Group_C. Group_C inherits the combined permissions of both groups. Group_C and Group_D are nested members of Group_E. Group_E directly inherits the permissions of Group_C and Group_D, and indirectly inherits the permissions of Group_A and Group_B.



When permissions are added to, or removed from, a nested group, the changes are automatically implemented in the nested group's immediate parent and continue to propagate onward. For example, if delete permission in Group_B is removed, Group_C's permissions become add + change + view. Group_E's permissions become add + change + view + execute.

Notes and Limitations

- All permissions in the above example refer to the same resource.
- A group can be a member of several groups.
- A circle of nested groups is not permitted. For example, Group_A is a member of Group_B, and Group_B is a member of Group_C. Group_C can not be a member of Group_A.
- Permissions are assigned to nested groups in the same way as for regular, non-nested, groups. Changes in nested group permissions take effect at the user's next login.
- There is no maximum number of levels of nested groups.

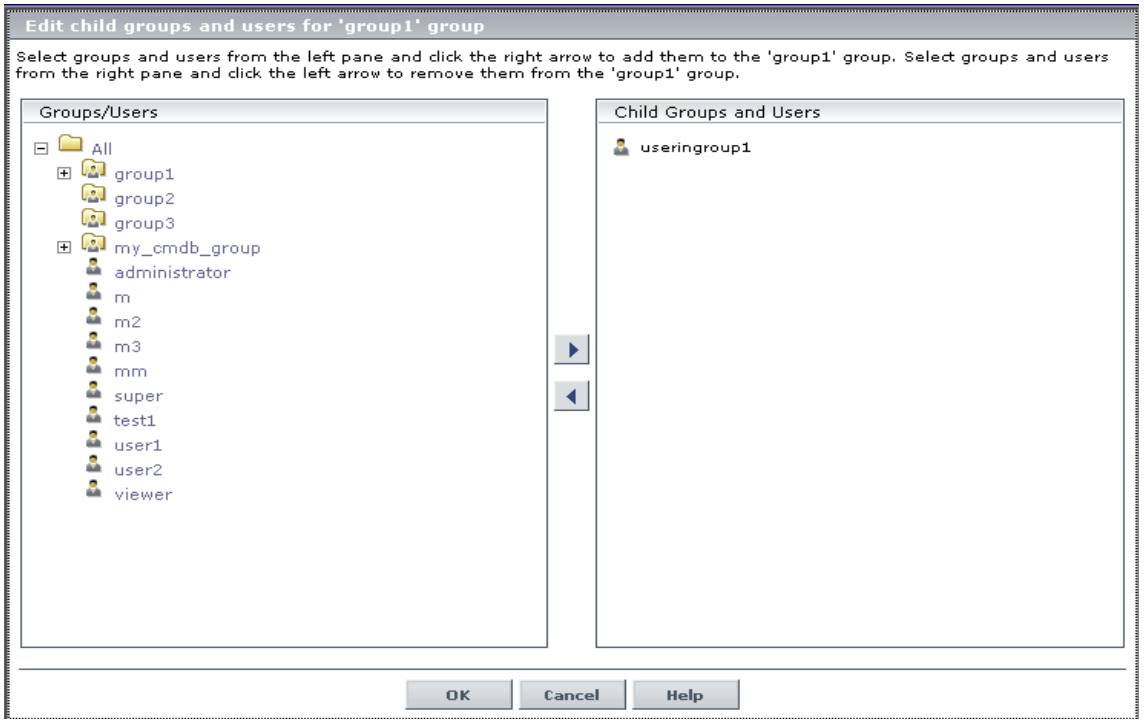
Managing Group Members

You can assign users to a group, or unassign users from a group via the **Hierarchy** tab in User Management. You can also nest one group within another.

To modify group/user assignment:

1. Select **Admin** > **Platform** > **Users and Permissions** > **User Management**. The User Management page opens, displaying the list of existing groups and users.
2. Click a group or user in the **Browse** tab of the Groups/Users pane on the left side of the screen.
3. Click the **Hierarchy** tab on the right side of the screen.

4 Select the group in the Groups/Users tab that you want to administer, and click the **Edit Child Groups and Users** button. The Edit Child Groups and Users window opens.



5 Assign users and nest groups by selecting the user or group in the Groups/Users pane, and clicking on the left-to-right arrow to move the group or user to the **Child Groups and Users** pane.

Unassign users and remove nested groups by selecting the group or user in the **Child Groups and Users** pane, and clicking on the right-to-left arrow.

To choose more than one group or user for nesting, press CTRL while making your selections.

6 Click **OK** to save the settings.

Notes and Limitations

- Selecting a user permits you only to view the user's parent groups - to nest a user, you must select the group in which you want to nest it, as described in steps 4 - 6 above.
- When removing a nested group from its parent, the group itself is not deleted.

23

Customizing User Menus

The Customization tab is divided into two sub-panes. In the left pane, you select the page users see when entering HP Business Availability Center. In the right pane, you choose the menu items available on that page.

Important: You must select a user in the Browse tab of the Groups/Users pane for the Customization tab to be visible.

The Customization Tab

On the Customization tab, you can:

- Specify the default context that is displayed for specific users when logging into HP Business Availability Center.
- Specify the first page that is displayed for specific users in each of the different parts of HP Business Availability Center.
- Specify the tabs and options that are available on pages throughout HP Business Availability Center.

  Customizing your entry page, menu items, and tabs enables your interface to display only the areas of HP Business Availability Center that are relevant to you.

You can use the menu customization page to perform the following tasks:

To set the default entry context displayed when logging into HP Business Availability Center:

1 Select **Admin** > **Personal Settings** > **Menu Customization** to open the Menu Customization page.

2 Choose the context from the left pane.

3 Click the **Set as Default Entry Context** button. The **Default Entry Context** icon appears next to your selection.

4 Click **OK** to save your settings.

To set the default page within the context displayed when logging into HP Business Availability Center:

1 Select **Admin** > **Personal Settings** > **Menu Customization** to open the Menu Customization page.

2 Choose one of the pages in the right pane and click the **Set as Default Entry Page** button. The **Default Entry Page** icon appears next to your selection.

You can set the default entry page for each context listed in the left pane.

You can select pages and tabs to be visible for each context in the left pane.

3 Click **OK** to save your settings.

Part VI

Personal Settings

24

Configuring Personal Settings

Personal settings enable customization of the way HP Business Availability Center presents information to individual users.

About Configuring Personal Settings

Individual users can configure personal settings to customize specific user-related behavior of HP Business Availability Center.

Users can configure the following personal settings:

- User name – for details, see page 386
- User mode – for details, see page 386
- Time zone used when displaying reports – for details, see page 387
- Password – for details, see page 387
- Refresh rate of reports – for details, see page 388
- Customized menu items– for details, see page 388

Configuring General Settings

On the General Settings page, you configure the user name, user mode, time zone, password, and refresh rate settings.

HP Business Availability Center saves these settings per defined user. Any changes you make remain in effect for all future Web sessions for only that user.

To configure the User name setting:

1 Select **Admin** > **Personal Settings** > **General Settings** to open the General Settings page.

2 Enter the user name you want in the **User name** field.

3 Click **Apply** to save your settings.

Note: You cannot change the entry in the **Login name** field.

To configure the User mode setting:

1 Select **Admin** > **Personal Settings** > **General Settings** to open the General Settings page.

2 Select the user mode in the Personal Settings section. HP Business Availability Center enables you to work with either the Operations User mode or the Business User mode. Different versions of Dashboard KPIs can be defined for each mode. You can see the KPI version appropriate for your user mode. For details, see "KPIs for User Modes" in *Using Dashboard*.

Select from the following options:

- **Unspecified.** This leaves you without a particular mode. Select this option if:
  - HP Business Availability Center is working with user modes and you want to see KPIs for both modes in Dashboard views.
  - Your system is not working with user modes.

- **Operations User**. This enables you to view the operations version of KPIs.
- **Business User.** This enables you to view the business version of KPIs.

3 Click **Apply** to save your settings.

To configure the Time zone setting:

1 Select **Admin** > **Personal Settings** > **General Settings** to open the General Settings page.

2 Select the time zone in which you want reports to be displayed, in the Personal Settings section. For a reference list of GMT time zones for locations throughout the world, see "GMT Time Zones" in *Reference Information*.

Note that the time zone automatically takes Daylight Saving Time into account. Therefore, you should select your GMT time zone in Standard Time and not in Daylight Saving Time.

3 Click **Apply** to save your settings.

To configure the E-mail setting:

Note: This setting is visible only to HP Managed Software Solutions customers.

---

1 Select **Admin** > **Personal Settings** > **General Settings** to open the General Settings page.

2 Enter a valid e-mail address in Personal Settings section, in the **E-mail** field.

3 Click **Apply** to save your settings.

To configure or edit the password:

1 Select **Admin** > **Personal Settings** > **General Settings** to open the General Settings page.

2 Enter the current password in the **Old password** field.

3 Enter the new password in the **Password** field.

4 Enter the new password again in the **Confirm password** field.

5 Click **Apply** to save your settings.

To configure the refresh rate setting:

1 Select **Admin** > **Personal Settings** > **General Settings** to open the General Settings page.

2 Select the rate at which you want HP Business Availability Center to automatically refresh the browser and load the most up-to-date data from the database, in the Refresh Settings section. Auto-refresh is only active when in the **Past day** or **Past hour** time resolution.

Note that, when viewing reports in the **Past day** or **Past hour** time resolution, or in the **day** or **hour** time resolution, for a period within the past 24 hours, the auto-refresh feature also automatically moves the time range of the report forward by the selected refresh period.

3 Click **Apply** to save your settings.

Customizing the Menus

On the Menu Customization tab, you can:

- Specify the default context that is displayed when logging into HP Business Availability Center.
- Specify the first page that is displayed in each of the different parts of HP Business Availability Center.
- Specify the tabs and options that are available on pages throughout HP Business Availability Center.

Customizing your entry page, menu items, and tabs enables your interface to display only the areas of HP Business Availability Center that are relevant to you.

You can use the menu customization page to perform the following tasks:

To set the default entry context displayed when logging into HP Business Availability Center:

1 Select **Admin** > **Personal Settings** > **Menu Customization** to open the Menu Customization page.

2 Choose the context from the left pane.

3 Click the **Set as Default Entry Context** button. The **Default Entry Context** icon appears next to your selection.

4 Click **OK** to save your settings.

To set the default page within the displayed context and which pages are to be visible:

1 Select **Admin** > **Personal Settings** > **Menu Customization** to open the Menu Customization page.

2 Choose a context from the left pane. If you want to configure it as the context to be visible when you log into HP Business Availability Center, click the **Set as Default Entry Context** button.

3 Choose one of the pages in the right pane and click the **Set as Default Entry Page** button. The **Default Entry Page** icon appears next to your selection.

You can set the default entry page for each context listed in the left pane.

4 Select pages and tabs to be visible for each context in the left pane by selecting the checkbox in the right pane next to the page or tab you want visible.

5 Click **OK** to save your settings.

Part VII

Report Administration

25

Customizing Reports

HP Business Availability Center enables you to generate reports automatically or manually and to specify a header and a footer for a report.

About Customizing Reports

HP Business Availability Center enables you to customize reports by:

- **specifying the default browser.** For details, see "Specifying the Default Browser" on page 394.
- **specifying a header and a footer for reports.** For details, see "Configuring a Report Header and Footer" on page 395.
- **generating reports automatically.** For details, see "Configuring Report Generation Settings" on page 398.

- **customizing the display of global reports.** For details, see "Global Reports Display Customization" on page 399.
- **configuring the maximum number of data units exportable to .pdf.** For details, see "Maximum Number of Data Units Exportable to PDF" on page 399.
- **customizing the display of specific reports.** For details, see "Specific Reports Display Customization" on page 400.

Note: HP Business Availability Center also enables you to customize the look and layout of specific reports (customizable reports). Contact Customer Support to assist you in performing this type of report customization.

Specifying the Default Browser

You can specify the default browser to view reports in.

To configure report generation settings for reports:

1. Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** > **Foundations**.
2. Select **Reporting** to open the Reporting-Display area.
3. Click the **Edit** button next to the **Default Browser** setting to open the Default Browser dialog box.
4. Set the **Value** field as required:
   - select **true** to enable Internet Explorer
   - select **false** to enable another browser
5. Click **Save** to save your settings.

   To restore default settings, click the **Restore Default** button.

Configuring a Report Header and Footer

You can add a header and a footer to a report. You can also modify an existing header and footer or return to the default header and footer (blank).

The technique used to customize reports is different for different reports. The reports can be split into two different groups:

- **Customizable Reports**
  - **All Service Level Management reports.** For details, see *Using Service Level Management*.
  - **All Dashboard reports.** For details, see "Working in Reports" in *Reference Information*.
  - **Selected Real User Monitor reports.** The following reports are included: Session Analyzer, Session Details, Page Details, Event Count over Time, Event Summary, and Event Log. For details, see "Real User Monitor Reports User Interface" in *Using End User Management*.
  - **All Application Lifecycle reports.** For details, see "Application Performance Lifecycle Workflow" in *Using Application Performance Lifecycle*.
  - **SOA reports.** For details, see "SOA Views and Reports" in *Solutions and Integrations*.
- **Legacy Reports**
  - **End User Management reports.** For details, see *Using End User Management*.
  - **System Availability Management reports.** For details, see *Using System Availability Management*.
  - **selected Real User Monitor reports.** The following reports are included: Global Statistics, Page Summary, Transaction Summary, End User Summary, and Server Summary. For details about these reports, see "Real User Monitor Reports User Interface" in *Using End User Management*.

This section includes the following topics:

Adding a Header and a Footer to a Legacy Report

To add a header and a footer to a legacy report, create a custom report using the Custom Report Manager, specify a header and a footer for the custom report, and include the legacy report in the custom report. For details, see "Defining a Header and Footer for a Custom Report" in *Custom Reporting and Alerting*.

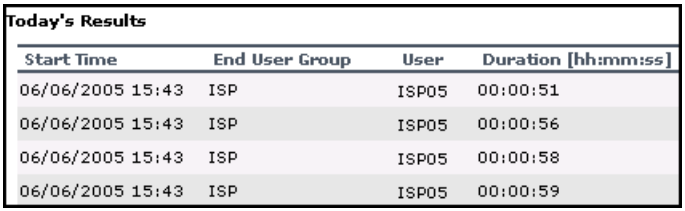
Adding a Header and a Footer to a Customizable Report

To add a header and a footer to a customizable report, specify the header and/or footer in the Report Header/Footer setting as explained below.

A customizable report header/footer has the following characteristics:

- The text of the header/footer has to be valid HTML.
- The changes take effect immediately.
- The change is applied to all the customizable reports.
- The header/footer is static. It remains displayed on the page while you scroll the report lines.
- If you added a report header/footer to a customizable report using the Report Header/Footer setting, and you include the customizable report in a custom report built using the Custom Report Manager, then the custom report header/footer overrides the customizable report header/footer.

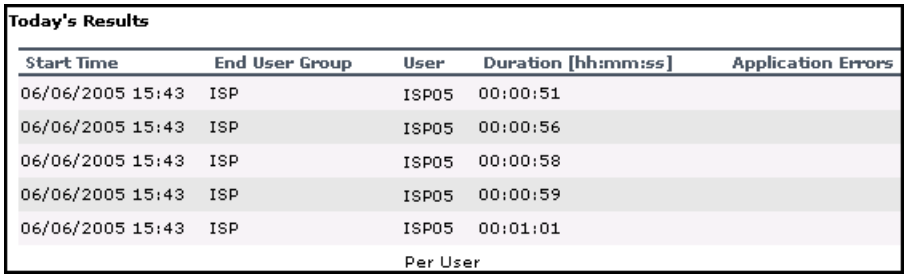
  For example, if you specify the header Today's Results, the header appears with a bold font.



Today's Results

Start Time	End User Group	User	Duration [hh:mm:ss]
06/06/2005 15:43	ISP	ISP05	00:00:51
06/06/2005 15:43	ISP	ISP05	00:00:56
06/06/2005 15:43	ISP	ISP05	00:00:58
06/06/2005 15:43	ISP	ISP05	00:00:59

As another example, if you specify the footer Per User the report shows the footer aligned to the center of the report.



Today's Results

Start Time	End User Group	User	Duration [hh:mm:ss]	Application Errors
06/06/2005 15:43	ISP	ISP05	00:00:51	
06/06/2005 15:43	ISP	ISP05	00:00:56	
06/06/2005 15:43	ISP	ISP05	00:00:58	
06/06/2005 15:43	ISP	ISP05	00:00:59	
06/06/2005 15:43	ISP	ISP05	00:01:01	

Per User

To add a header and a footer to a new report:

1 Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** > **Foundations**.

2 Select **Reporting** to open the Reporting - Display area.

3 To specify a header:

a Click the **Edit** button next to the **Display static report header** setting to open the Display static report header dialog box.

b In the **Value** box, enter the text of the header.

c Click **Save** to save the changes.

To restore default settings, click the **Restore Default** button.

4 To specify a footer:

a Click the **Edit** button next to the **Display static report footer** setting to open the Display static report footer dialog box.

b In the **Value** box, enter the text of the footer.

c Click **Save** to save the changes.

To restore default settings, click the **Restore Default** button.

Configuring Report Generation Settings

You can configure HP Business Availability Center to generate reports automatically after selecting the report from the menu or to generate reports only on demand from within the report.

To configure these settings, users with appropriate administrative privileges should perform the changes described in the procedure below.

Note: You must log in again for the changes to take effect.

To configure report generation settings for reports:

1. Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** > **Foundations**.
2. Select **Reporting** to open the Reporting-Display area.
3.  Click the **Edit** button next to the **Generate Reports Automatically** setting to open the Generate Reports Automatically dialog box.
4. Set the property value as required:
   - ➤ select **true** to enable automatic report generation
   - ➤ select **false** to disable automatic report generation
5. Click **Save**.

To remove automatic report generation, set the property back to **false**.

To restore default settings, click the **Restore Default** button.

For more information on the Infrastructure Settings Manager, see “Infrastructure Settings” on page 79.

Global Reports Display Customization

You can customize the appearance of your reports by configuring display elements to be applied to all reports.

To customize the global display for reports:

1. Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** > **Foundations**.
2. Select **Reporting** to open the Reporting - Display area.
3. Click the **Edit** button next to the **Global reports display customization** setting to open the Global reports display customization dialog box.
4. Enter the XML script in the **Value** field for the report components you want to customize. A sample configuration file is located at:

   <HP Business Availability Center root directory>\HPBAC\AppServer\webapps\site.war\WEB-INF\rfw\conf\internal\rfw-presentation.xml
5. Click **Save** to save your settings.

   To restore default settings, click the **Restore Default** button.

Maximum Number of Data Units Exportable to PDF

You can configure the maximum number of data units that can be presented when exporting hierarchic reports in .pdf format.

To configure the maximum amount of data units exportable to .pdf:

1. Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** > **Foundations**.
2. Select **Reporting** to open the Reporting - Display area.
3. Click the **Edit** button next to the **Maximum number of data units exportable to .pdf** setting to open the Maximum number of data units exportable to .pdf dialog box.

4 Enter the number of data units you want to set as the maximum number exportable to a hierarchic .pdf report in the **Value** field.

5 Click **Save** to save your settings.

To restore default settings, click the **Restore Default** button.

Maximum Number of Rows Per Table

You can configure the maximum number of rows that are presented when generating a table in a report.

To configure the maximum number of rows per table:

1 Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** > **Foundations**.

2 Select **Reporting** to open the Reporting - Display area.

3 Click the **Edit** button next to the **Maximum number of rows per table** setting to open the Maximum number of rows per table dialog box.

4 Enter the maximum number of rows in the **Value** field you want displayed in the table.

5 Click **Save** to save your settings.

To restore default settings, click the **Restore Default** button.

Specific Reports Display Customization

You can customize the appearance of your reports by configuring display elements to be applied to specific reports.

To customize the display for specific reports:

1 Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** > **Foundations**.

2 Select **Reporting** to open the Reporting - Display area.

3 Click the **Edit** button next to the **Specific reports display customization** setting to open the Specific reports display customization dialog box.

4 Enter the XML script in the **Value** field for the report components you want to customize. A sample configuration file is located at:

<HP Business Availability Center root directory>\HPBAC\AppServer\webapps\site.war\WEB-INF\rfw\conf\applications*-presentation.xml

5 Click **Save** to save your settings.

To restore default settings, click the **Restore Default** button.

26

Reports Log

HP Business Availability Center logs all activities related to reports as well as errors that occur when generating reports. Such activities include: creating a new report, generating a report, modifying report filters, drilling down in reports, and so forth.

Overview of Reports Log

HP Business Availability Center records all activities related to specific reports in a reports log. The activities that are logged are:

- **any error related to a report.** For details, see "Logging Errors" on page 406.
- **any other activity performed on the report.** For details, see "Logging Activities" on page 406.

Each error and activity is recorded using a specific format – for details about the reports log format, see "Reports Log Structure" on page 407.

This section includes the following topics:

Customizable Reports

The reports log records activities for:

- **all Service Level Management reports.** For details, see *Using Service Level Management*.
- **all Dashboard reports.** For details, see "Working in Reports" in *Reference Information*.
- **selected Real User Monitor reports.** The following reports are included: Session Analyzer, Session Details, Page Details, Event Count over Time, Event Summary, and Event Log. For details, see "Real User Monitor Reports User Interface" in *Using End User Management*.
- **all Application Lifecycle reports.** For details, see "Application Performance Lifecycle Workflow" in *Using Application Performance Lifecycle*.
- **SOA reports.** For details, see "SOA Views and Reports" in *Solutions and Integrations*.

Reports Log Location

The reports log is located at **HPBAC\log\EJBContainer\reports.log.**

Setting the Reports Log Level

Depending on the log level you specify, the following information can be recorded in the reports log:

- debugging information
- activities performed on reports
- warning messages

- error messages
- fatal errors

The log levels have the following hierarchy: **DEBUG**, **INFO**, **WARN**, **ERROR**, and **FATAL**, where **DEBUG** represents the lowest level and **FATAL** the highest level. The default level is **ERROR**.

The log level hierarchy means that if you select one of the levels, the report includes all the information related to that level and the levels above it, as follows:

Level	Reports log
DEBUG	Includes debugging information, activities performed on reports, warning messages, error messages, and fatal errors.
INFO	Includes activities performed on reports, warning messages, error messages, and fatal errors.
WARN	Includes warning messages, error messages, and fatal errors.
ERROR	Includes error messages, and fatal errors.
FATAL	Includes fatal errors.

To set the Reports Log level:

1. Open the **HPBAC\conf\core\Tools\log4j\EJB\topaz.properties** file with a text editor.
2. Search for the following line:
log4j.category.com.mercury.am.bac.core.reports= ${<loglevel>}, reports.appender
3. Change <**loglevel**> to **DEBUG, INFO, WARN, ERROR**, or **FATAL**.
4. Save the file.

Logging Errors

Logging occurs for any error during:

- report initialization
- report customization – for more information, see "Customizing Reports" on page 393
- rendering (creating the report display)

For details about the reports log structure, see "Reports Log Structure" on page 407.

Logging Activities

Logging occurs for any action related to reports. The actions that are logged are:

- creating a new report
- generating a report
- updating the filter of a report that is included in a custom report
- drilling down in a report and between reports
- updating the filter of a report
- printing a generated report, exporting it using e-mail, or opening it in Microsoft Excel file format or in PDF format. For more information about these activities, see "Sharing and Storing Reports" in *Custom Reporting and Alerting*

Reports Log Structure

The reports log includes entries for each activity or error. Each entry has the following structure:

```
2005-08-24 11:25:07,590 [TP-Processor1] (NewReportAction.java:66) <loglevel> -
MERQ-120238: USER ACTION started
----------------------------------------=----------------------------------------
Action=             <action>
User=               <user> (id:<id>)
Report ID=          <report_id>;  State ID: <state_id>
----------------------------------------=----------------------------------------
2005-08-24 11:25:15,980 [TP-Processor1] (DisplayAction.java:77) <loglevel> - MERQ-
120242: USER ACTION ended
----------------------------------------=----------------------------------------
User=               <user> (id:<id>)
Report ID=          <report_id>;  State ID: <state_id>
Duration=           <duration> ms  (init:6141;  render:3859)
Time filter=        View: <view>; From:<from_day_time>; To: <to_day_time>; Every:
<periodicity>
----------------------------------------=----------------------------------------
```

where:

- <**log_level**> represents the level that you selected – for details about the log level, see "Setting the Reports Log Level" on page 404.
- <**action**> is the type of activity that has been logged:
  - **New report.** The user created a new report from a menu.
  - **Generate.** The user clicked the **Generate** button.
  - **CustomSaveFilter.** The user clicked **OK** in the filter of new reports when creating a custom report.
  - **Update filter.** The user modified the filter in one of the reports.
  - **Navigate.** The user drilled down in a report or between reports.
  - **Export.** The user exported a report to Excel, .PDF, .CSV, or e-mail formats.
- <**user**> is the login name.
- <**id**> is for internal use.
- <**report_id**> is the report requested by the user action.

- **<state_id>** is for internal use.
- **<duration>** is the number of milliseconds the server took to perform the user action.
- The time filter that was used in the activity includes the following information:
  - **<view>** indicates the filter that was selected. This information is for internal use.
  - **<from_day_time>** indicates when the activity started. This information is for internal use.
  - **<to_day_time>** indicates when the activity ended.
  - **<periodicity>** indicates the sampling periodicity. This information is for internal use.

For example, the following entry specifies that a new report CMDBOverTime has been created by the admin user:

```
2005-08-24 11:25:07,590 [TP-Processor1] (NewReportAction.java:66) INFO  - MERQ-120238: USER ACTION started
-----------------------------------------=----------------------------------------
Action=                 New report
User=                   admin (id:1)
Report ID=              CmdbOverTime;  State ID: 0
-----------------------------------------=----------------------------------------
2005-08-24 11:25:15,980 [TP-Processor1] (DisplayAction.java:77) INFO  - MERQ-120242: USER ACTION ended
-----------------------------------------=----------------------------------------
User=                   admin (id:1)
Report ID=              CmdbOverTime;  State ID: 0
Duration=               10078 ms  (init:6141;  render:3859)
Time filter=            View: pastDay; From: 23/08/05 11:25; To: 24/08/05 11:25; Every: 1 hours
-----------------------------------------=----------------------------------------
```

Part VIII

Authentication

27

Authentication Strategies

This chapter explains how to set up authentication strategies, such as LDAP, for HP Business Availability Center.

Note to HP Managed Software Solutions customers: This chapter is not relevant to HP Managed Software Solutions customers.

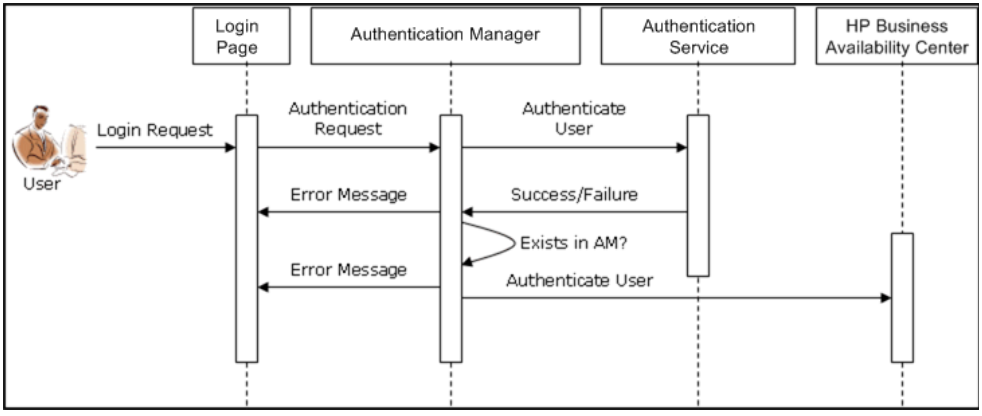
Authentication for HP Business Availability Center

HP Business Availability Center authentication is based on a concept of authentication strategies. Each strategy handles authentication against an authentication service such as the internal HP Business Availability Center service, Lightweight Directory Access Protocol (LDAP), Single Sign-on (SSO), or any other option enabled on the specific HP Business Availability Center installation.

When a login request is initiated, a strategy is invoked by a request for authentication using a specific context appropriate for that strategy.

HP Business Availability Center Login Workflow

This section describes a typical authentication flow in HP Business Availability Center:



- A user accesses the HP Business Availability Center login page. The login page is returned to the Web browser and includes a hidden key that specifies which authentication strategy to follow.
- The user enters a principal (in this case, user name) and credentials (in this case, password) and submits the login request (in this case, clicks **Log In**).

- The request is transferred to the HP Business Availability Center Authentication Manager together with the strategy name, principal, and credentials.
- The Authentication Manager reads the strategy name and dispatches the request to the relevant authentication strategy to validate the user.
- The relevant authentication strategy accepts the request and tries to authenticate the user against the authentication service in question.
- If authentication is approved, HP Business Availability Center verifies whether the user is defined in HP Business Availability Center.

Note: When creating users in HP Business Availability Center, make sure that user names match the user names in the relevant strategy database. A user can not login to HP Business Availability Center if the name does not match.

- If the user passes the previous steps, they are considered an authenticated user. The HP Business Availability Center Site Map page is displayed in the Web browser (or whichever page has been defined as the default page).

  If any of the steps fail, the user is notified (a page and error message are sent back to the Web browser). The page and error message depend on which strategy you are implementing.

Setting Up an Authentication Strategy

The default authentication strategy is the internal HP Business Availability Center service. If you use the default, you do not have to make any changes to the system.

You can use an external LDAP server to store the authentication information instead of using the internal HP Business Availability Center service. The LDAP server must be in the same subnet as the rest of the HP Business Availability Center servers.

If you want to use LDAP or SSO authentication strategy, you must configure the appropriate authentication strategy:

- To define an LDAP authentication strategy, see the next section.
- To define an SSO authentication strategy, see "Defining a Single Sign-on Authentication Strategy".

Note: For the procedure for defining other authentication strategies, contact Customer Support.

Defining an LDAP Authentication Strategy

You can define an LDAP authentication strategy for a HP Business Availability Center system.

This section contains the following topics:

- "Setting the LDAP Authentication Strategy"
- "Setting a Secure Connection with the SSL (Secure Sockets Layer) Protocol" on page 416
- "Resolving a Distinguished Name (DN) from a User ID" on page 417
- "Enabling an LDAP Authentication Strategy" on page 418

Setting the LDAP Authentication Strategy

This section explains how to set an LDAP authentication strategy in HP Business Availability Center.

To set the LDAP authentication strategy:

1. Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**. Select the **Foundations** context and choose **LDAP Authentication** from the list.
2. In the **LDAP Authentication - LDAP Server Settings** table, access the LDAP Server URL dialog box by clicking the **Edit** button.
3. Enter the LDAP URL value, using the format ldap://<ldapHost>[:<port>]/[<baseDN>][??scope]

   For example, ldap://my.ldap.server:389/ou=People,o=myOrg.com??sub)
4. Click **Save** to save the new value, **Default** to replace the entry with the default value (a blank URL), or **Cancel** to close the dialog box without changing the value.
5. The default protocol used to communicate with the LDAP server is TCP, but you can change the protocol to SSL. For details, see the next section.
6. By default, HP Business Availability Center does not resolve user IDs. You can, however, change this setting. For details, see "Resolving a Distinguished Name (DN) from a User ID" on page 417.

The next stage in setting the LDAP authentication strategy is to enable the strategy in HP Business Availability Center. For details, see "Enabling an LDAP Authentication Strategy" on page 418.

Setting a Secure Connection with the SSL (Secure Sockets Layer) Protocol

Since the login process involves the passing of confidential information between HP Business Availability Center and the LDAP server, you can apply a certain level of security to the content. You do this by enabling SSL communication on the LDAP server and configuring HP Business Availability Center to work using SSL.

HP Business Availability Center supports SSL that uses a certificate issued by a trusted Certification Authority (CA). This CA is included with the Java runtime environment.

Most LDAP servers, including Active Directory, can expose a secure port for an SSL based connection. If you are using Active Directory with a private CA, you may need to add your CA to the trusted CAs in Java.

For details on configuring the HP Business Availability Center platform to support communication using SSL, see "Using SSL in HP Business Availability Center" in the *HP Business Availability Center Hardening Guide* PDF.

To add a CA to trusted CAs to expose a secure port for an SSL based connection:

1. Export a certificate from your CA and import it into the JVM that is used by HP Business Availability Center.
2. Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**. Select the **Foundations** context and choose **LDAP Authentication** from the list.
3. In the **LDAP Authentication - LDAP Server Settings** table, access the Security Protocol dialog box by clicking the **Edit** button.
4. Change the value to **ssl**.
5. Click **Save** to save the new value, **Default** to replace the entry with the default value (internal HP Business Availability Center service), or **Cancel** to close the dialog box without changing the value.

Resolving a Distinguished Name (DN) from a User ID

In most Directory Services, a user must log in with a complete distinguished name to be authenticated. This DN is usually a very long string such as: cn=John Smith, cn=Users, ou=Sales, dc=USA, dc=MyCompany, dc=COM. Typing this long string is both annoying and error prone. It is very common, therefore, for applications that integrate with a Directory Service to translate the user's unique ID (for example, the login name) into a complete DN before trying to bind it to the authentication strategy. HP Business Availability Center supports this feature.

You can enable HP Business Availability Center to search the LDAP server with a named or anonymous user.

The user ID is resolved as follows:

- HP Business Availability Center takes the user's unique ID (the user name).
- HP Business Availability Center performs a search in the Directory for the user by looking for either uid or sAMAccountName (the LDAP and Active Directory attribute names that hold the user's unique ID, respectively).
- If the search retrieves one (and only one) result, the user's DN is taken from the result and used instead of the login name in the bind operation. If the search retrieves zero or more than one result, the login fails.

To enable HP Business Availability Center to resolve user IDs:

1. Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**. Select the **Foundations** context and choose **LDAP Authentication** from the list.
2. In the **LDAP Authentication - LDAP UID Search** table, access the Distinguished Name (DN) Resolution dialog box by clicking the **Edit** button next to the Distinguished Name (DN) Resolution entry.
3. Change the value to **true**.
4. Click **Save** to save the new value, **Default** to replace the entry with the default value (the default is **false**), or **Cancel** to close the dialog box without changing the value.

5 Enter the DN of a user entitled to perform searches in the LDAP database: Access the Distinguished Name of Search-Entitled User dialog box by clicking the **Edit** button next to the Distinguished Name of Search-Entitled User entry. Enter the DN in the Value field.

To enable anonymous login to the LDAP server, leave this field blank. Note, however, that the anonymous user must have permissions to search the LDAP database.

6 Click **Save** to save the new value, **Default** to replace the entry with the default value (the default is **false**), or **Cancel** to close the dialog box without changing the value.

7 Enter the password of a user entitled to perform searches in the LDAP database. Access the Password of Search-Entitled User dialog box by clicking the **Edit** button next to the Password of Search-Entitled User entry. Enter the password in the Value field.

If you defined an anonymous user (in step 5 on page 418), leave this field blank.

8 Click **Save** to save the new value, **Default** to replace the entry with the default value (the default is **false**), or **Cancel** to close the dialog box without changing the value.

Enabling an LDAP Authentication Strategy

This section explains how to enable an LDAP authentication strategy in HP Business Availability Center.

To enable an LDAP authentication strategy:

1 Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**. Select the **Foundations** context and choose **Business Availability Center Interface** from the list.

2 In the **Business Availability Center Interface – Authentication** table, access the Login Authentication Method dialog box by clicking the **Edit** button.

3 Enter the appropriate strategy name in the Value field. Note that this field is case sensitive. Enter **LDAP**.

4 Click **Save** to save the new value, **Default** to replace the entry with the default value (the default is **false**), or **Cancel** to close the dialog box without changing the value.

Defining a Single Sign-on Authentication Strategy

This section contains the following topics:

About Single Sign-On Authentication Support

HTTP Single Sign-On Authentication provides support for single sign-on over HTTP. Single sign-on (SSO) requires a central login server for a group of applications.

The SSO authentication server authenticates users, and applications inside the group trust the authentication. You do not need further authentication when moving from one application to another.

All requests to client applications are channeled through the SSO authentication server. The internal applications only need to know the name of the authenticated user. That name is passed by the SSO authentication server as the value of an HTTP request header.

The following section explains the procedure for installing SSO authentication support in HP Business Availability Center.

Implementing Single Sign-On Authentication Support

If you are implementing SSO using a reverse proxy, see "Special SSL Configuration Considerations" in Using SSL in HP Business Availability Center

To implement SSO authentication support, perform the following steps:

1. Stop the HP Business Availability Center Gateway Server.
2. Add a new key **HttpSSOAuthenticationLoginHandler.headerName** to the **SYSTEM** table in the management database. The value of the key must be the HTTP header name that the SSO server sends to HP Business Availability Center.

   ```
   SQL> INSERT INTO System VALUES
   ('HttpSSOAuthenticationLoginHandler.headerName','HTTP_header_name');
   ```

3 In <**HP Business Availability Center root directory**>**conf****security.xml**, the following code should be present right after the <authentication> tag:

```
<strategy domain="UserNameOnly"
class="com.hp.security.authentication.UserNameOnly.UserNameOnlyAuthentic
ationStrategy" ></strategy>
```

Add the above code if it is not present.

4 Change the default HP Business Availability Center URL to **http://<HP Business Availability Center server>/topaz/HttpSSOlogin.jsp**. This can be done in one of two ways:

- Redirect requests from the SSO login page to **http://<HP Business Availability Center server>/topaz/HttpSSOlogin.jsp**.
- In <**HP Business Availability Center root directory**>**AppServer****webapps****site.war****index.html**, change **src** to **/topaz/HttpSSOlogin.jsp**.

5 By default, logging out of HP Business Availability Center returns you to the main login page. You can change the logout page to a different URL by adding a new key **LOGOUT_URL** to the **SYSTEM** table:

```
SQL> INSERT INTO System VALUES ('LOGOUT_URL', 'your_logout_url');
```

Note: This step is optional.

---

6 Restart the HP Business Availability Center Gateway Server.

Index

D

F

G

H

I

L

M

N

O

P

R

S

T

U

V