HP Business Availability Center

for the Windows and Solaris operating systems

Software Version: 7.50

Platform Administration

Document Number: BACPLAT7.50/01
Document Release Date: February 2009
Software Release Date: May 2008

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://h20230.www2.hp.com/selfsolve/manuals

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

Welcome to This Guide

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

This chapter includes:

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

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 monitor report schedules.

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

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.

This chapter includes:

Concepts

Tasks

Reference

Logging In and Out - Overview

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 to a user depends on the user's permissions. For details on granting user permissions, see "Assign Permissions" on page 435.

HP Business Availability Center is by default configured with Lightweight Single Sign-On (LW-SSO). LW-SSO enables you to login to HP Business Availability Center and automatically have access to other configured applications, without needing to login to those applications. For details on how LW-SSO affects logging into HP Business Availability Center, see "Logging Into HP Business Availability Center with Lightweight Single Sign-On (LW-SSO)" on page 16.

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

Note to HP Software-as-a-Service customers: You access HP Business Availability Center via the HP Software-as-a-Service support Web site (mms.mercury.com).

Logging Into HP Business Availability Center with Lightweight Single Sign-On (LW-SSO)

By default, Lightweight Single Sign-On Authentication Support (LW-SSO) is enabled for HP Business Availability Center. Single Sign-On enables you to login to HP Business Availability Center and automatically have access to other configured applications, without needing to login to those applications. You must ensure that the other applications in the Single Sign-On environment have LW-SSO enabled and are working with the same initString for LW-SSO Authentication to work.

With LW-SSO enabled, you must keep the following factors in mind:

- If you do not require Single Sign-On for HP Business Availability Center, it is recommended that you disable LW-SSO. To do so, you must access the LW-SSO configuration setting in the JMX console on the application server that is embedded in HP Business Availability Center, as follows:
  - Enter the URL of the JMX console (**http://<server name>:8080/jmx-console/**) in a web browser.
  - Enter your JMX console authentication credentials. If you do not know your authentication credentials, contact your system administrator.

    For details on accessing the JMX console, see "Accessing the JMX Console" on page 18.
  - Modify the appropriate settings, as follows:
    - Domain name: **Topaz**
    - Service: **LW-SSO Configuration**
    - Method: **Enabled = False**

  When accessing the JMX console, you must enter the JMX authentication credentials, which by default are:

  Username: **admin**

  Password: **admin**

  You can change the password by accessing the following file:

  Once LW-SSO is disabled, the default HP Business Availability Center authentication service is automatically enabled. You do not need to enter the syntax **.<domain_name>** in your HP Business Availability Center login URL when LW-SSO is disabled.

- If you enable one of the other authentication strategies supported by HP Business Availability Center, Identity Management Single Sign-On (IDM-SSO) or Lightweight Directory Access Protocol (LDAP), you also do not need to enter the syntax **.<domain_name>** in your HP Business Availability Center login URL. For details on implementing an IDM-SSO authentication strategy, see "Implement an Identity Management Single Sign-On Authentication Support (IDM-SSO) - Workflow" on page 115. For details on implementing an LDAP authentication strategy, see "Define an LDAP Authentication Strategy – Workflow" on page 106.

- If you disable LW-SSO, you do not need to enter the syntax **.<domain_name>** in the HP Business Availability Center login page URL. For details on the requirements for logging into HP Business Availability Center, see "Log In and Out" on page 23.

Advanced Login Options

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

Advanced login options include:

- **Automatic login.** You can configure HP Business Availability Center so that after the initial login, you do not have to enter a login name and password, and instead, the default page that is set to open for the user opens automatically. For details, see "Use the Automatic Login URL Mechanism" on page 26.
- **Direct login capabilities.** You can guide another user to a specific target page in HP Business Availability Center. For details, see "Use the Link to This Page Option to Open a Specific Page" on page 26.
- **Limiting login access.** Limit the number of machines accessing HP Business Availability Center using the same login name. For details, see "Limit Access by Different Machines Using the Same Login Name" on page 27.
- **Linking to specific pages.** You can guide another user to a specific target page in HP Business Availability Center by creating a URL with a user name, password, and information about the target page. For details on the user interface for linking to specific pages, see "Link to This Page Window" on page 29.

Accessing the JMX Console

To access the JMX console, you must first enter the relevant URL (**http://<server name>:8080/jmx-console/**, where <server name> is the name of the machine on which HP Business Availability Center is running), and enter the JMX console authentication credentials, which by default are:

Login name = **admin**

Password = **admin**

You can change the default password by accessing the relevant properties files, located at:

\HPBAC\EJBContainer\server\mercury\conf\props\jmx-console-users.properties

The syntax in this file appears as **username=password**. You change the username or password and save the file to register your change.

Note: This file is not encrypted, which could lead to unauthorized access to the properties file. To prevent unauthorized access, you may want to configure the HPBAC directory to allow access only to selected users.

You must also implement changes into the following files:

\HPBAC\conf\jmxsecurity.txt

The syntax in this file appears as **username password**. You change the username or password and save the file to register your change.

\HPBAC\AppServer\webapps\myStatus.war\myStatus.html

Locate the syntax, "GET", url, false,"admin","admin", where "**admin**","**admin**" = "**username**", "**password**". Change the username or password and save the file to register your change.

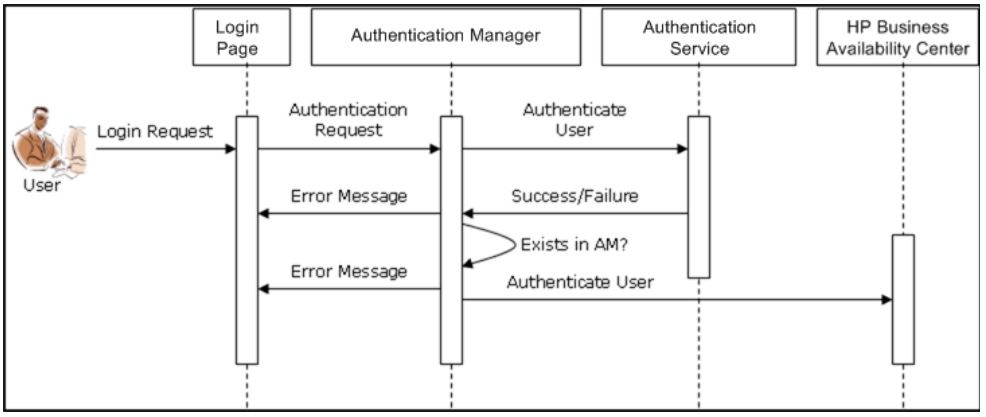
Authentication for HP Business Availability Center - Overview

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, which also serves as a user repository), Single Sign-on (SSO, which enables you to login to HP Business Availability Center and automatically have access to other configured applications), or any other option enabled on the specific HP Business Availability Center installation.

The default authentication strategy for logging into HP Business Availability Center is the internal HP Business Availability Center service. You enter your HP Business Availability Center username and password from the login page, and your credentials are stored and verified by the HP Business Availability Center database. For a description of the workflow for authentication in HP Business Availability Center, see “HP Business Availability Center Login Flow” on page 21.

HP Business Availability Center Login Flow

This section describes the general authentication flow in HP Business Availability Center:



- A user accesses the login page and enters a principal (login name) and credentials (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 the user according to the selected strategy.

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 a Single Sign-On Authentication Strategy

The Single Sign-On (SSO) authentication strategy enables you log in to a single application and then permits you to access other applications configured in the original application's group. The applications inside the group trust the authentication, and you do not need further authentication when moving from one application to another.

The default single sign-on authentication strategy for HP Business Availability Center is Lightweight Single Sign-On Authentication (LW-SSO). LW-SSO is embedded in HP Business Availability Center and does not require an external machine for authentication. For details on LW-SSO, see "Lightweight Single Sign-On (LW-SSO) Authentication - Overview" on page 73.

Important: Any application using LW-SSO must be configured according to the time zone in which it is located.

If the applications configured outside of HP Business Availability Center do not support LW-SSO, or if you want a more secure Single Sign-On connection, you can configure Identity Management Single Sign-On (IDM-SSO). IDM-SSO requires a central login server for a group of applications.

For details on defining an IDM-SSO authentication strategy, see "Implement an Identity Management Single Sign-On Authentication Support (IDM-SSO) - Workflow" on page 79.

All requests to client applications are channeled through the SSO authentication strategy. The internal applications need to know only the name of the authenticated user. That name is passed as follows:

- in LW-SSO as a cookie containing the name of the authenticated user.
- in IDM-SSO as an HTTP request header, whose key is defined in the IDM documentation.

If you have defined an IDM-SSO authentication strategy and then want to re-enable LW-SSO, see "Implement a Lightweight Single Sign-On Authentication Support (LW-SSO) - Workflow" on page 74.

If you do not upgrade to IDM-SSO, or if no other applications are configured to work with HP Business Availability Center, HP Business Availability Center uses its own internal authentication service. HP Business Availability Center requires that each resource uses the same authentication service.

Log In and Out

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

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

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

1 In a Web browser, enter the URL **http://<server_name>.<domain_name>/HPBAC** (**hpbac** can also be used), where **server_name** is the name or IP address of the HP Business Availability Center server, and **domain_name** is the name of the user's domain according to his network configuration. 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.

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 of the page, 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 "General Tab" on page 455.

For details on the user interface for creating users in the HP Business Availability Center system, see "Create User Dialog Box" on page 449.

For details on login authentication strategies that can be used in HP Business Availability Center, see "Authentication Strategies" on page 97.

For login troubleshooting information, see "Troubleshooting and Limitations" on page 32.

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

To log out of HP Business Availability Center:

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

Use Advanced Login Options

You can choose to enable advanced login options for HP Business Availability Center. For details, see "Advanced Login Options" on page 18.

This section includes the following topics:

- "Use the Link to This Page Option to Open a Specific Page" on page 26
- "Limit Access by Different Machines Using the Same Login Name" on page 27
- "Open an Application Page Using a URL" on page 27

1 Enable Automatic Login in the Login Page

When automatic login is enabled from the login page and 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
- the default page that is set to open for the user opens automatically

To enable automatic login:

a In the HP Business Availability Center login page, select the option to **Remember my login name and password for 14 days**.

b When completing your session, do not click **Logout** at the top of the page, but simply close the browser window.

Logging out disables the automatic login option and requires the login name and password to be entered when again accessing HP Business Availability Center.

For details on Automatic Login Limitations, see "Automatic Login Limitations" on page 37.

2 Use 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 a Web browser, enter the URL **http://<server_name>.<domain_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, **domain_name** represents the name of the user's domain according to his network configuration, and **loginname** and **userpassword** 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.

3 Use the Link to This Page Option to Open a Specific Page

Use the Link to This Page option to guide another user to a specific target page in HP Business Availability Center. Link to This Page creates a URL with a user name, password, and information about the target page.

Depending on how you configure the parameters in the Link to This Page dialog box, the receiver accesses the target 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. You can send this URL by email or SMS to another user. 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. For details, see "Link to This Page Window" on page 29.

4 Limit 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 Maximum machines per login name value in Infrastructure Settings, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, select **Security**, and locate the **Maximum machines per login name** entry. Modify the 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.

For a limitation of this feature, see "Limiting Access by Different Machines Using the Same Login Name Limitation" on page 38.

5 Open an Application Page Using a URL

You can open a specific HP Business Availability Center page directly in your browser by using a URL. For details, see "Display a Specific View Using a URL" on page 43.

Logging Into HP Business Availability Center User Interface

This section describes:

HP Business Availability Center Login Page

Description	Enables you to log in to HP Business Availability Center. **To access:** In a Web browser, enter the URL **http://<server_name>.<domain_name>/HPBAC (hpbac can also be used)**, where **server_name** is the name or IP address of the HP Business Availability Center server, and **domain_name** is the name of the user's domain according to his network configuration.
Important Information	If Lightweight Single Sign-On (LW-SSO) is disabled, you do not need to add the **.<domain_name>** syntax in the login URL.
Included in Tasks	"Log In and Out" on page 23
Useful Links	"Logging Into HP Business Availability Center with Lightweight Single Sign-On (LW-SSO)" on page 16

The following elements are included:

GUI Element (A-Z)	Description
Login Name	Enter the relevant login name to access HP Business Availability Center.
Password	Enter the relevant password to access HP Business Availability Center.
Remember my login name and password for 14 days	Select to enable HP Business Availability Center remember your login name and password for 14 days. Login credentials are automatically entered in future login sessions when this option is selected.

Link to This Page Window

Description	Enables you to guide another user to a specific target page in HP Business Availability Center. **To Access:** Select **Admin** > **Link to this page**
Important Information	➤ Depending on how you configure Link to This Page, the receiver accesses the page using one of the following: ➤ His own user name and password ➤ A URL encrypted with your user name and password ➤ A URL encrypted with another user's user name and password If using an encrypted URL, the receiver bypasses the HP Business Availability Center login page because the URL supplies the user name and password information. ➤ 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, but you configure Link to This Page with **Use Credentials** of a regular user. When the receiver uses this URL, he is sent to the Setup and Maintenance page and is unable to access Infrastructure Settings. ➤ The Link to This Page option 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 logged in, the receiver does not proceed to the target page. There is no informational message about the reason for the login failure.

Included in Tasks	"Use Advanced Login Options" on page 24
Useful Links	"Advanced Login Options" on page 18 "Opening an Application Page Using a URL" in *Reference Information*.

The Link to This Page Window includes the following elements (listed alphabetically):

GUI Element	Description
Cancel	Click to cancel the Link to this page operation.
Create Link	Click to create a URL for the user to enter into their browser and view the specified HP Business Availability Center page.
Confirm password	Re-enter the password entered in the **Password** field.
Copy to Clipboard	Click to copy the **Link** field to the clipboard.
Generate HTML	Click to generate an HTML page for the specified HP Business Availability Center page.
Link	The URL that the receiver uses to access the specified HP Business Availability Center page.
Login name	The login name to be encrypted in the URL the receiver uses to access the specified page. This must be the login name of an actual user.
My credentials	Select if the link is to be encrypted with your login name and password.
No credentials	Select if the receiver uses his own login name and password to access the page specified in the link.
Password	The password to be encrypted in the URL the receiver uses to access the specified page. This must be the password of an actual user.
Use credentials	Select if the link is to be encrypted with the login name and password of another user.

Security Notes and Precautions

This section describes security notes and precautions to be aware of when using Direct Login to log into HP Business Availability Center:

- 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 and Limitations

Use the information below to troubleshoot possible causes of failure to log in to HP Business Availability Center.

Login Troubleshooting

Reference the possible login failure causes using the error number shown in the error alert dialog box. For additional troubleshooting information, refer to the HP Software Self-solve knowledge base.

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 Microsoft 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/jmx-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 an authentication strategy has been configured correctly. For details on single sign-on authentication strategies, see "Setting Up a Single Sign-On Authentication Strategy" on page 22.
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.

Automatic Login Limitations

This section describes limitations of the Automatic Login option:

- Using the **Logout** option at the top of the HP Business Availability Center page cancels the Automatic Login 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, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, and select **Security.** In this context, you can:
  - Customize the number of days to enable the option by editing the **Days to remember login** value to the desired number of days (the default value is 14).
  - Completely remove this option from appearing in the login page by setting the **Enable automatic login** value to false (the default value is true).
  - Configure the number of machines that can access HP Business Availability Center using the same login name by configuring the **Maximum machines per login name** value (the default value is 0).

    For details on using the Infrastructure Settings page, see "Infrastructure Settings Manager Page" on page 211.

Limiting Access by Different Machines Using the Same Login Name 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.

Link to This Page Limitations

When selecting **Create Link** or **Generate HTML** after choosing to send the page with **No Credentials**, you must log out of HP Business Availability Center before invoking the login URL or HTML, if it is being invoked on the same machine you created it on.

Resetting LDAP/SSO Settings via the JMX Console

If your LDAP or SSO settings have not been configured properly, it is possible to be prevented from accessing HP Business Availability Center. If this happens, you must reset your LDAP or SSO settings remotely via the JMX console in the application server that comes with HP Business Availability Center:

To reset LDAP/SSO settings via the JMX console:

1. Enter the URL of the JMX console (**http://<server name>:8080/jmx-console/**) in a web browser.
2. Enter your JMX console authentication credentials. If you do not know your authentication credentials, contact your system administrator.
3. Modify the appropriate settings, depending on the authentication method you are resetting:
   - To reset LDAP settings, modify the JMX settings as follows:
     - Domain name: **Foundations**
     - Service: **users-remote-repository**

- Method: **setRemoteUserRepositoryMode = Disabled**

- To reset SSO settings, modify the JMX settings as follows:
  - Domain name: **Topaz**
  - Service: **SSO**
  - Method: **setIdmSsoConfigurationEnable = False**

2

Opening an Application Page Using a URL

This chapter provides information on how to build a URL that opens a specific HP Business Availability Centerpage directly in your browser.

This chapter includes:

Concepts

Tasks

Direct Links to an Application Page

You can open a specific HP Business Availability Center page directly in your browser by using a URL. This enables third-party applications, such as HP ServiceCenter, to retrieve information from HP Business Availability Center without being located in the HP Business Availability Center context.

Note: It is recommended to add the server's URL to trusted sites in Microsoft Internet Explorer.

The URL you use takes you first to the HP Business Availability Center login page. After you enter your login name and password, the target page opens in your browser.

By default, Lightweight Single Sign-On Authentication Support (LW-SSO) is enabled for HP Business Availability Center. For details, see "Logging Into HP Business Availability Center with Lightweight Single Sign-On (LW-SSO)" on page 16.

Note: If LW-SSO is enabled, then the URLs must be encoded.

If LW-SSO is disabled, then you need to include the user name and password in the URL. To get the user name and password encrypted, use the Link to This Page feature from any context in HP Business Availability Center. In the Link to This page dialog box, select **My credentials** and then click **Create link** to see the encryption created. For details, see "Link to This Page Window" on page 29.

Optionally, you can also choose not to encrypt the user name and password in the URL. In such a case, set the **directLoginEncrypted** parameter to false.

Note: If you select the **Remember my login name and password** check box in the login page, HP Business Availability Center takes you directly to the target page without having to enter your credentials the next time you use a URL to access your target page. If LW-SSO is enabled, and both HP Business Availability Center and the third-party application use the same credentials, the target page automatically opens in your browser.

Display a Specific View Using a URL

You can display a specific view directly in your browser, without being located in the HP Business Availability Center context.

For details about views, see "View Manager" in *Model Management*.

This section explains the URL syntax for displaying a specific view directly in your browser.

Note: When you copy the URL, delete any soft breaks so it is copied as one line.

Build the URL using the following syntax:

LW-SSO enabled:

```
http://<serverName>.<domainName>/topaz/cms/topologyApplet.do?cmd=setView&
-treeViewName=<treeViewName>&-graphViewName=<graphViewName>
&customer=<customerId>
```

Not LW-SSO enabled:

```
http://<serverName>/topaz/TopazSiteServlet?createSession=true&
requestType=login&directLogin=true&directLoginEncrypted=true&
userlogin=<userlogin>&userpassword=<userpassword>&
customerId=<customerId>portlet_url=/cms/topologyApplet.do?
&customer=<customerId>&cmd=setView&-treeViewName=<treeViewName>&-
graphViewName=<graphViewName>
```

Note: The **portlet_url** parameter must be URL encoded.

The parameters whose values must be provided are described below:

- <**userlogin**>. The login name to be encrypted in the URL.
- <**userpassword**>. The password to be encrypted in the URL.
- <**serverName**>. The name of the HP Business Availability Center server.
- <**graphViewName**>. The name of the view, which is also known as the <map view name>.
- <**treeViewName**>. In most cases, it is the same as the <graphView Name>. For views created in HP Business Availability Center versions earlier than 7.0, you may need to use the <CmdbObject> of the view.

For example (LW-SSO enabled):

```
http://<serverName>.<domainName>/topaz/cms/topologyApplet.do?cmd=setView
&-treeViewName=NetworkTopology&-graphViewName=NetworkTopology
&customer=1
```

For example (not LW-SSO enabled):

```
http://<serverName>/topaz/TopazSiteServlet?createSession=true&
requestType=login&directLogin=true&directLoginEncrypted=true&
userlogin=5F8138FB2D131A1C&userpassword=5F8138FB2D131A1C&
customerId=customer1&portlet_url=/cms/topologyApplet.do?&
customer=1&cmd=setView&-treeViewName=NetworkTopology&-
graphViewName=NetworkTopology
```

Generate a Change Report Using a URL

A Change report displays information about the changes made to CIs in the CMDB or all the CIs in a certain view. For more details about what the report displays, see "Change Report" in *Model Management*.

You can generate a Change report by building a URL that opens a Change report directly in your browser, without being located in the HP Business Availability Center context.

This section explains the URL syntax for generating a Change report directly in your browser.

Note: When you copy the URL, delete any soft breaks so it is copied as one line.

Build the URL using the following syntax:

LW-SSO enabled:

```
http://<serverName>.<domainName>/topaz/rfw/newReport.do?reportID=change
&autoGenerate=true&populateAnyway=true&filter.viewId=9<filter.viewId>(optional)
&filter.dateFrom=<filter.dateFrom>&filter.dateTo=<filter.dateTo>&filter.objectIds=
<filter.objectIds>&customer=<customerId>
```

Not LW-SSO enabled:

```
http://<serverName>/topaz/TopazSiteServlet?createSession=true&requestType=login&
directLogin=true&directLoginEncrypted=true&userlogin=<userlogin>&userpassword=<
userpassword>&customerId=<customerId>&portlet_url=/rfw/newReport.do?reportID=
change&autoGenerate=true&populateAnyway=true&filter.viewId=<filter.viewId&filter.d
ateFrom=filter.dateFrom&filter.dateTo=filter.dateTo&filter.objectIds=filter.objectIds
```

Note: The **portlet_url** parameter must be URL encoded.

The parameters whose values must be provided are described below:

- <**userlogin**>. The login name to be encrypted in the URL.
- <**userpassword**>. The password to be encrypted in the URL.
- <**serverName**>. The name of the HP Business Availability Center server.
- <**filter.dateFrom**>. The start date and time for the report using the following format: <the number of milliseconds since January 1, 1970, 00:00:00 GMT represented by this date>.
- <**filter.dateTo**>. The end date and time for the report using the following format: <the number of milliseconds since January 1, 1970, 00:00:00 GMT represented by this date>.
- **<filter.viewId>.** (This parameter is optional.) The ID of a view. The Change report displays information about the changes made to the CIs in a specific view, such as, the number of added CIs or deleted CIs.
- <**filter.objectIds**>. The ID of a specific CI. The Change report displays information about the changes made to a specific CI and all its children.
  - If a value is provided for the <**filter.viewId**> parameter, the value for <**filter.objectIds**> is: -9999999.
  - If a value is not provided for the **filter.objectIds** parameter, then information is given about the changes made to the CIs in a specific view.

For example (LW-SSO enabled):

```
http://<serverName>.<domainName>/topaz/rfw/newReport.do?reportID=change
&autoGenerate=true&populateAnyway=true&filter.viewId=9e5a5a2d4835acf5d3d58
20199d66a0d&filter.dateFrom=1177162740000&filter.dateTo=117975474000
&filter.objectIds=-9999999&customerId=customerId=1
```

For example (not LW-SSO enabled):

```
http://<serverName>/topaz/TopazSiteServlet?createSession=true&requestType=login&
directLogin=true&directLoginEncrypted=true&userlogin=5F8138FB2D131A1C&userpa
ssword=5F8138FB2D131A1C&customerId=<customerId>&portlet_url=/rfw/newReport.
do?reportID=change&autoGenerate=true&populateAnyway=true&filter.viewId=9e5a5a
2d4835acf5d3d5820199d66a0d&filter.dateFrom=1177162740000&filter.dateTo=117
9754740000&filter.objectIds=-9999999
```

Generate a Get Related CIs Report Using a URL

A Get Related CIs report lists the CIs that are related to a specified CI. For more details about what the report displays, see "Get Related CIs Report" in *Model Management*.

You can generate a Get Related CIs report in IT Universe Manager, or by building a URL that opens a Get Related report directly in your browser, without being located in the HP Business Availability Center context.

This section explains the URL syntax for generating a Get Related CIs report directly in your browser.

Note: When you copy the URL, delete any soft breaks so it is copied as one line.

Build the URL using the following syntax:

LW-SSO enabled:

```
http://<serverName>.<domainName>/topaz/rfw/newReport.do?reportID=neighbor
&autoGenerate=true&populateAnyway=true&filter.className=<CITtype>
&filter.objectId=<objectId>&customer=<customerId>
```

Not LW-SSO enabled:

```
http://<serverName>/topaz/TopazSiteServlet?createSession=true&requestType=login&
directLogin=true&directLoginEncrypted=true&userlogin=<userlogin>&userpassword=<
userpassword>&customerId=<customerId>&portlet_url=/rfw/newReport.do?&custome
rId=1&reportID=neighbor&autoGenerate=true&populateAnyway=true&filter.className
=<CITtype>&filter.objectId=<objectId>
```

Note: The **portlet_url** parameter must be URL encoded.

The parameters whose values must be provided are described below:

- <**userlogin**>. The login name to be encrypted in the URL.
- <**userpassword**>. The password to be encrypted in the URL.
- <**serverName**>. The name of the HP Business Availability Center server.
- <**className**>. The CI type of the CI whose related CIs you want to see.
- <**objectId**>. The object ID of the CI whose related CIs you want to see.

Note: To retrieve the object ID of a CI, right-click the required CI in IT Universe Manager and select Properties.

- <**filter.viewId**>. (This parameter is optional.) The ID of a view. The Get Related CIs report displays the CIs that are related to a specified CI in a specific view.

  For example (LW-SSO enabled):

  ```
  http://<serverName>.<domainName>/topaz/rfw/newReport.do?reportID=neighbor&
  autoGenerate=true&populateAnyway=true&filter.className=host&filter.objectId
  =9e5a5a2d4835acf5d3d5820199d66a0d&customer=1
  ```

  For example (not LW-SSO enabled):

  ```
  http://<serverName>/topaz/TopazSiteServlet?createSession=true&requestType=login&
  directLogin=true&directLoginEncrypted=true&userlogin=5F8138FB2D131A1C&userpa
  ssword=5F8138FB2D131A1C&customerId=<customerId>&portlet_url=/rfw/newReport.
  do?&customerId=1&reportID=neighbor&autoGenerate=true&populateAnyway=true&filt
  er.className=host&filter.objectId=b84a33c50d81034363a99898013da76a
  ```

Generate an Impact Analysis Report Using a URL

HP Business Availability Center enables you to simulate how infrastructure changes can impact your system. For details, see "Correlation Manager" in *Model Management*.

You can generate an Impact Analysis report that displays a list of the trigger CIs and the CIs that were impacted as a result of the change. For more details about what the report displays, see the Generate Report field in "Run Correlation Dialog Box" in *Model Management*.

You can generate an Impact Analysis report in Topology View, or by building a URL that opens an Impact Analysis report directly in your browser, without being located in the HP Business Availability Center context.

This section explains the URL syntax for generating an Impact Analysis report directly in your browser.

Note: When you copy the URL, delete any soft breaks so it is copied as one line.

Build the URL using the following syntax:

LW-SSO enabled:

```
http://<serverName>.<domainName>/topaz/rfw/newReport.do?reportID=impact
&populateAnyway=true&autoGenerate=true&filter.objectIds=[xxx,yyy,zzz]&filter.impact
Category=<impactCategory>&filter.impactSeverity=<impactSeverity>&customer=
<customerId>
```

Not LW-SSO enabled:

```
http://<serverName>/topaz/TopazSiteServlet?createSession=true&requestType=login
&directLogin=true&directLoginEncrypted=true&userlogin=<userName>&userpassword
=<userPassword>&customerId=<customerId>&portlet_url=/rfw/newReport.do?reportID
=impact&populateAnyway=true&autoGenerate=true&filter.objectIds=[xxx,yyy,zzz]&
filter.impactCategory=<impactCategory>&filter.impactSeverity=<impactSeverity>
```

Note: The **portlet_url** parameter must be URL encoded.

The parameters whose values must be provided are described below:

- <**userlogin**>. The login name to be encrypted in the URL.
- <**userpassword**>. The password to be encrypted in the URL.
- <**serverName**>. The name of the HP Business Availability Center server.
- <**impactCategory**>. The name of the category to be analyzed.
- <**impactSeverity**>. The severity level of the category.
- <**[xxx,yyy,zzz]**>. The object ID of the trigger CIs in the CMDB. The object IDs are separated by a comma (,).

Note:

- To retrieve the object ID of a CI, right-click the required CI in IT Universe Manager and select Properties.
- Parameters are separated from the rest of the URL by a question mark (**?**).
- Configured URLs must use the ampersand character (**&**) as the parameter delimiter.

For example (LW-SSO enabled):

```
http://<serverName>.<domainName>/topaz/rfw/newReport.do?reportID=impact
&populateAnyway=true&autoGenerate=true&filter.objectIds=[111,222,333]
&filter.impactCategory=change&filter.impactSeverity=2&customer=1
```

For example (not LW-SSO enabled):

```
http://<serverName>/topaz/TopazSiteServlet?createSession=true&requestType=login
&directLogin=true&directLoginEncrypted=true&userlogin=5F8138FB2D131A1C&
userpassword=5F8138FB2D131A1C&customerId=<customerId>&portlet_url=/rfw/new
Report.do?reportID=impact&populateAnyway=true&autoGenerate=true
&filter.objectIds=[111,222,333]&filter.impactCategory=change&filter.impactSeverity=2
```

Generate an Impact Map Using a URL

HP Business Availability Center enables you to simulate how infrastructure changes can impact your system. For details, see "Correlation Manager Overview" on page 165.

An Impact map displays all the CIs that are impacted by the CI that was defined as the root cause of the changes. For more details about what the topology map displays, see Show Impact in "Topology View Window" in *Model Management*.

You can generate an Impact map in Topology View, or by building a URL that opens an Impact report directly in your browser, without being located in the HP Business Availability Center context.

This section explains the URL syntax for generating an Impact map directly in your browser.

Note: When you copy the URL, delete any soft breaks so it is copied as one line.

Build the URL using the following syntax:

LW-SSO enabled:

```
http://<serverName>.<domainName>/topaz/cms/topologyApplet.do?objectId=
<objectId>&category=<category>&cmd=impact&className=<className>
&severity=<severity>
```

Not LW-SSO enabled:

```
http://<serverName>/topaz/TopazSiteServlet?createSession=true&requestType=login
&directLogin=true&directLoginEncrypted=true&userlogin=<userName>&userpassword
=<userPassword>&customerId=<customerId>&portlet_url=/cms/topologyApplet.do?
&customer=<customerId>&objectId=<objectId>&category=<category>
&cmd=impact&className=<className>&severity=<severity>
```

Note: The **portlet_url** parameter must be URL encoded.

The parameters whose values must be provided are described below:

- <**userlogin**>. The login name to be encrypted in the URL.
- <**userpassword**>. The password to be encrypted in the URL.
- <**serverName**>. The name of the HP Business Availability Center server.
- <**displayLabel**>. The display label of the CI in the CMDB. This parameter must be url_encoded.

Note: The URL must contain one of two parameters: either <displayLabel> or <objectId>.

- <**objectId**>. The object ID of the trigger CI.

Note: To retrieve the object ID of a CI, right-click the required CI in IT Universe Manager and select Properties.

- <**category**>. The category used to create the impact.
- <**className**>. The CIT of the trigger CI.

Note: The <className> parameter is important for performance issues, especially when using the <displayLabel> parameter.

➤ **<severity>**. The severity of the impact. The severity must be within the category's Enumeration severity values. For details, see System Type Manager in *Model Management*.

For example (LW-SSO enabled):

```
http://<serverName>.<domainName>/topaz/cms/topologyApplet.do?objectId=
429a953e5ead3b3325e6fc485b1ebb8a&category=change&cmd=impact
&className=sap_system&severity=2&customer=1
```

For example (not LW-SSO enabled):

```
http://<serverName>/topaz/TopazSiteServlet?createSession=true&
requestType=login&directLogin=true&directLoginEncrypted=true&
userlogin=5F8138FB2D131A1C&userpassword=5F8138FB2D131A1C&
customerId=<customerId>portlet_url=/cms/topologyApplet.do?&customer=1&
objectId=429a953e5ead3b3325e6fc485b1ebb8a&category=change&
cmd=impact&className=sap_system&severity=2
```

Generate a Host OS Breakdown Report Using a URL

A Host OS Breakdown report displays a breakdown of operating systems. For more details about what the report displays, see "Host OS Breakdown Report" in *Model Management*.

You can generate a Host OS Breakdown report by selecting **Applications** > **Universal CMDB** > **Overview Reports** > **Host OS Breakdown**, or by building a URL that opens a Host OS Breakdown report directly in your browser without being located in the HP Business Availability Center context.

This section explains the URL syntax for generating a Host OS Breakdown report directly in your browser.

Note: When you copy the URL, delete any soft breaks so it is copied as one line.

Build the URL using the following syntax:

LW-SSO enabled:

```
http:/<serverName>.<domainName>/topaz/rfw/newReport.do?reportID=
hostbreakdown&autoGenerate=true&customer=customer1
```

Not LW-SSO enabled:

```
http://<serverName>/topaz/TopazSiteServlet?createSession=true&requestType=login
&directLogin=true&directLoginEncrypted=true&userlogin=<userName>&userpassword
=<userPassword>&customerId=<customerId>&portlet_url=/rfw/newReport.do?reportID
=hostbreakdown&autoGenerate=true
```

Note: The **portlet_url** parameter must be URL encoded.

The parameters whose values must be provided are described below:

- <**userlogin**>. The login name to be encrypted in the URL.
- <**userpassword**>. The password to be encrypted in the URL.
- <**serverName**>. The name of the HP Business Availability Center server.

View CI Properties Using a URL

You can display the properties of a specific CI directly in your browser, without being located in the HP Business Availability Center context.

For details about CI properties, see "Properties Dialog Box" in *Model Management*.

This section explains the URL syntax for viewing the properties of a specific CI directly in your browser.

Note: When you copy the URL, delete any soft breaks so it is copied as one line.

Build the URL using the following syntax:

LW-SSO enabled:

```
http://<serverName>.<domainName>/topaz/itu/propertiesinit.do?__ITUCmdbID
=<__ITUCmdbID>
```

Not LW-SSO enabled:

```
http://<serverName>/topaz/TopazSiteServlet?createSession=true&requestType=login
&directLogin=true&directLoginEncrypted=true&userlogin=<userName>
&userpassword=<userPassword>&customerId=<customerId>&portlet_url=
/itu/properties-init.do?__ITUCmdbID=<__ITUCmdbID>
```

Note: The **portlet_url** parameter must be URL encoded.

The parameters whose values must be provided are described below:

- <**userlogin**>. The login name to be encrypted in the URL.
- <**userpassword**>. The password to be encrypted in the URL.
- <**serverName**>. The name of the HP Business Availability Center server.
- <**__ITUCmdbID**>. The object ID of the CI whose properties you want to display.

Note: To retrieve the object ID of a CI, right-click the required CI in IT Universe Manager and select Properties.

For example (LW-SSO enabled):

```
http://<serverName>.<domainName>/topaz/itu/propertiesinit.do?
__ITUCmdbID=82b1e1dba3cf013af9f775a15d9b1f07&customer=1
```

For example (Not LW-SSO enabled):

```
http://<serverName>/topaz/TopazSiteServlet?createSession=true&
requestType=login&directLogin=true&directLoginEncrypted=true&
userlogin=5F8138FB2D131A1C&userpassword=5F8138FB2D131A1C&
customerId=<customerId>portlet_url=/itu/properties-
init.do?__ITUCmdbID=82b1e1dba3cf013af9f775a15d9b1f07
```

View Related CIs Using a URL

You can display the related CIs of a specific CI. You view related CIs in IT Universe Manager, or by building a URL that opens a topology map directly in your browser, without being located in the HP Business Availability Center context.

For more details about related CIs, see "IT Universe Manager Window" in *Model Management*.

This section explains the URL syntax for viewing a CI's related CIs directly in your browser.

Note: When you copy the URL, delete any soft breaks so it is copied as one line.

Build the URL using the following syntax:

LW-SSO enabled:

```
http://<serverName>.<domainName>/topaz/cms/topologyApplet.do?cmd=related
&objectId=<objectId>&numberOfHopsOfRelated=<numberOfHopsOfRelated>
&customer=<customerId>
```

Not LW-SSO enabled:

```
http://<serverName>/topaz/TopazSiteServlet?createSession=true&requestType=login
&directLogin=true&directLoginEncrypted=true&userlogin=<userName>
&userpassword=<userPassword>&customerId=<customerId>&portlet_url=
/cms/topologyApplet.do?cmd=related&objectId=<objectId>&numberOfHopsOfRelated
=<numberOfHopsOfRelated>
```

Note: The **portlet_url** parameter must be URL encoded.

The parameters whose values must be provided are described below:

- <**userlogin**>. The login name to be encrypted in the URL.
- <**userpassword**>. The password to be encrypted in the URL.
- <**serverName**>. The name of the HP Business Availability Center server.
- <**objectId**>. The object ID of the CI whose related CIs you want to view.

Note: To retrieve the object ID of a CI, right-click the required CI in IT Universe Manager and select **Properties**.

- <**numberOfHopsOfRelated**>. The distance in levels from the source CI to its related CIs. The default is 1. The maximum is 3.

  For example (LW-SSO enabled):

  ```
  http://<serverName>.<domainName>/topaz/cms/topologyApplet.do?cmd=related
  &objectId=429a953e5ead3b3325e6fc485b1ebb8a&numberOfHopsOfRelated=1
  &customer=1
  ```

  For example (not LW-SSO enabled):

  ```
  http://<serverName>/topaz/TopazSiteServlet?createSession=true&requestType=login
  &directLogin=true&directLoginEncrypted=true&userlogin=5F8138FB2D131A1C
  &userpassword=5F8138FB2D131A1C&customerId=<customerId>&portlet_url=/cms/
  topologyApplet.do?cmd=related&objectId=429a953e5ead3b3325e6fc485b1ebb8a
  &numberOfHopsOfRelated=1
  ```

3

Navigating HP Business Availability Center

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

This chapter includes:

Concepts

Reference

Navigating HP Business Availability Center

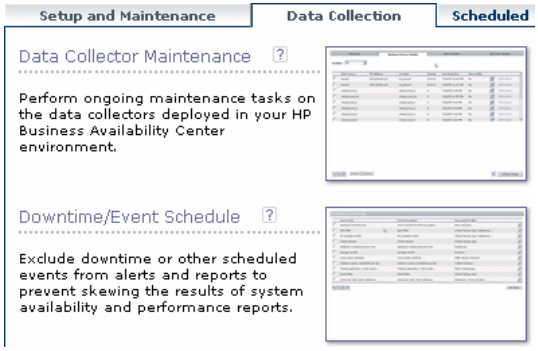
HP Business Availability Center runs in a Web browser. You move around HP Business Availability Center using the following navigation functions:

- **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.

- **Menu bar.** Enables navigation to the applications, Administration Console pages, help resources, and a link to the site map.

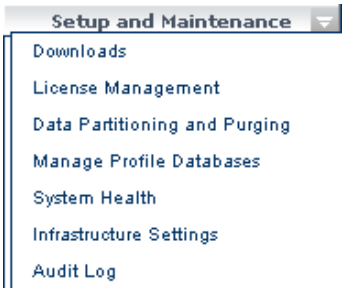
Additionally, there is a **Logout** button on the top right corner of the page.

- **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.

Working with the HP Business Availability Center Documentation Library

The HP Business Availability Center Documentation Library is an integrated help system comprising all the guides contained in the end-user documentation set delivered with Business Availability Center. The sections below describe how to navigate and use the Documentation Library.

Navigating the Documentation Library

The Documentation Library 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 by clicking the **Home** entry on the Contents tab of the Documentation Library Navigation Pane (described below) and by clicking the Home icon  located at the top of every content page.

  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 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. You can limit your search to a specific guide or set of guides by selecting a value from the scope list.
- **Favorites tab.** The Favorites tab enables bookmarking specific pages for quick reference. Note that the Favorites tab is available only 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 63. Note that this button is displayed only when the navigation pane is closed.

- **Show in Contents button.** Click to open the table of contents in the Contents tab and highlight the entry corresponding to the currently displayed page. This button is displayed only 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.

Organization of Information into Topics

The material in most of the Documentation Library guides is organized by topic types. Three main topic types are in use: **Concepts**, **Tasks**, and **Reference**. The topic types are differentiated visually using icons. Below is an explanation of each topic type along with its corresponding icon:

- **Concepts.** Concept topics provide background, descriptive, or conceptual information. Read concept topics to get general information about what a feature does and how it works.

- **Tasks**. Task topics provide step-by-step guidance on how to complete specific tasks that are typically required to administer or use the software. Task topics also include scenarios for certain tasks. Read task topics and follow the steps listed to get a task done.

- **Reference**. Reference topics provide detailed lists and explanations of parameters, common user interface elements, and other reference-oriented material. Read reference topics when you need to look up some specific piece of reference information relevant to a particular context.

- **User Interface**. User Interface topics are a specialized form of reference topics that are used mainly for context-sensitive help. Help links from the software generally open the user interface topics.

- **Troubleshooting and Limitations**. Troubleshooting and limitations topics are a specialized form of reference topics that provide troubleshooting and list limitations of the feature. Read troubleshooting and limitations topics if you encounter unexpected behavior of the software. It is recommended that you review a feature's limitations before using it.

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*.
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*.

Menu Option	Description
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. For details, see the HP Diagnostics documentation installed with the product.
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 *Alerts*.
Problem Isolation	Select to open the Problem Isolation application, used for triaging and isolating problematic CIs identified by HP Business Availability Center as well as for viewing and analyzing proactive analysis data. For details, see *Using Problem Isolation*.
User Reports	Select to access the Report Manager and create and save user reports—customized reports containing user-defined data and formatting that can help you focus on specific aspects of your organization's application and infrastructure resource performance. For details on the Report Manager, see *Reports*.
Universal CMDB	Select to open the HP Universal CMDB application, used to view a topology map of CIs, to compare CIs and views, to view reports about changes that occur in the CMDB, and to view overview reports. For details, see *Model Management*.

Menu Option	Description
Business Availability Center for Siebel	Select to open HP Business Availability Center for Siebel Applications diagnostics tools. For details, see *Solutions and Integrations*.
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*.
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 agreements (SLAs, OLAs, UCs) and build services that link to the data that Service Level Management collects. For details, see *Using Service Level Management*.

Menu Option	Description
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, see the HP Diagnostics documentation installed with the product.
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 *Alerts*.
Problem Isolation	Select to open the Problem Isolation Administration pages, where you configure on-demand monitors, problem suspects, and proactive analysis. For details, see *Using Problem Isolation*.
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 Discovery and Dependency Mapping 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 *Model Management*.
Business Availability Center for Siebel Administration	Select to open the Business Availability Center for Siebel Applications Administration page. For details, see *Solutions and Integrations*.

Menu Option	Description
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 (HP ServiceCenter, HP OVO, Netscout nGenius, and others) and customize the Integration Monitor configuration files to correctly map the data Integration Monitors collect to a format recognizable by HP Business Availability Center. For details, see *Solutions and Integrations*.
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 "Link to This Page Window" on page 29.
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 HP Software Support Web Site directly to the troubleshooting landing page (required HP Passport login). The URL for this Web site is http://h20230.www2.hp.com/troubleshooting.jsp

- **HP Software Support.** Opens the HP Software 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://www.hp.com/go/hpsoftwaresupport
- **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/go/software.
- **Task Assistant.** Opens the task assistant, which assists in accomplishing specific tasks by listing the task steps and providing links to the relevant Help topics for each step.
- **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.

4

Lightweight Single Sign-On Authentication

This chapter provides information on the Lightweight Single Sign-On Authentication Strategy.

This chapter includes:

Concepts

Tasks

Lightweight Single Sign-On (LW-SSO) Authentication - Overview

The default single sign-on authentication strategy for HP Business Availability Center is Lightweight Single Sign-On Authentication (LW-SSO). LW-SSO is embedded in HP Business Availability Center and does not require an external machine for authentication.

Important: Any application using LW-SSO must be configured according to the time zone that it is located in.

If the applications configured outside of HP Business Availability Center do not support LW-SSO, or if you want a more secure Single Sign-On connection, you can configure Identity Management Single Sign-On (IDM-SSO). IDM-SSO requires a central login server for a group of applications.

For details on defining an IDM-SSO authentication strategy, see "Implement an Identity Management Single Sign-On Authentication Support (IDM-SSO) - Workflow" on page 79.

For an overview of Single Sign-On Authentication, see "Setting Up a Single Sign-On Authentication Strategy" on page 22.

For details on limitations of working with LW-SSO, see "Lightweight Single Sign-On Authentication - General Reference" on page 95.

Implement a Lightweight Single Sign-On Authentication Support (LW-SSO) - Workflow

By default, Lightweight Single Sign-On Authentication Support (LW-SSO) is enabled for HP Business Availability Center. If you have configured Identity Management SSO authentication support (IDM-SSO) and want to re-enable LW-SSO, follow this procedure:

To re-enable LW-SSO after configuring IDM-SSO:

1. Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, and select **Single Sign On**.
2. Locate the **Unknown User Handling Mode** entry in the Single Sign On - Light Weight (LW-SSO) field, and select one of the options to indicate how HP Business Availability Center is to handle unknown users - users that were authenticated but do not exist in the HP Business Availability Center users repository:

- **Integration User.** A user with the login credentials **Integration User** is created in place of the user who attempted to login. This user has System Viewer permissions.
- **Allow.** The user is created as a new HP Business Availability Center user and allowed access to the system. This user has System Viewer permissions, and his default password is his login name.
- **Deny.** The user is denied access to HP Business Availability Center, and is returned to the login page.

The changes take effect immediately.

3 Navigate to **<HP Business Availability Center Gateway Server>/conf/settings/SingleSignOn/ActiveDirectoryDefaultSettings.properties**. Refer to your LW-SSO documentation for instructions on configuring your LW-SSO framework, based on information in the configuration file.

4 In the Single Sign On - Identity Management (IDM-SSO) field, select the **Enable IDM-SSO Authentication** setting and modify the value to **false**.

Update Lightweight Single Sign-On (LW-SSO) Parameters Via JMX Console

You can update selected Lightweight Single Sign-On (LW-SSO) parameters remotely via the JMX console on the application server that is embedded in HP Business Availability Center. If you want to disable LW-SSO, you can do so only from the JMX console.

To update Lightweight Single Sign-On (LW-SSO) parameters via the JMX console:

1 Enter the URL of the JMX console (**http://<server name>:8080/jmx-console/**) in a web browser.

2 Enter your JMX console authentication credentials. If you do not know your authentication credentials, contact your system administrator.

3 Locate the LightWeight Single Sign-On context, as follows:

a Domain name: **Topaz**

b Service: **LW-SSO Configuration**

4 Modify parameters accordingly.

The changes take effect immediately.

5

Identity Management Single Sign-On Authentication

This chapter provides information on the Identity Management Single Sign-On (IDM-SSO) Authentication Strategy.

This chapter includes:

Concepts

Tasks

Identity Management Single Sign-On (IDM-SSO) Authentication - Overview

You implement IDM-SSO as an authentication strategy if you want a more secure connection than that offered by LW-SSO, or if the applications configured outside of HP Business Availability Center do not support LW-SSO. The IDM server is monitored by a single center Policy Server, and consists of a User Repository and a Policy Store (both could reside over the same server as the policy server), and a Web Server Agent installed over each of the application's web servers communicating with the Policy Server. The

IDM server controls users' access to various organizational resources, protecting confidential personal and business information from unauthorized users. The IDM server identity manager handles the user's passwords and credentials by assigning different user rules in relation to the organization's different resources. For details, see your IDM vendor's documentation.

HP Business Availability Center requires the IDM vendor to store user information to render it available as a header on http requests. All HP Business Availability Center resources must use the same authentication service configured on the IDM-SSO server.

Configuring an IDM-SSO overrides any infrastructure settings configured for LW-SSO. For details on configuring IDM-SSO, see "Implement an Identity Management Single Sign-On Authentication Support (IDM-SSO) - Workflow" on page 79.

Note: If you have upgraded from a version prior to HP Business Availability Center 7.5 with IDM-SSO enabled, the HP Business Availability Center AuthenticationUpgrader takes the values of the **header** and **URL** attributes configured in the SYSTEM table and converts them to the appropriate values in the **Header name** and **Logout URL** fields in Infrastructure Settings, and sets the **Enable IDM-SSO Authentication** field value to **true**.

Implement an Identity Management Single Sign-On Authentication Support (IDM-SSO) - Workflow

This task describes how to implement Identity Management SSO authentication support (IDM-SSO):

This task includes the following steps:

- "Configure the IDM Server to Secure HP Business Availability Center Resources" on page 79
- "Login to the IDM Server" on page 80
- "Verify IDM-SSO Configuration" on page 80
- "Configure IDM-SSO Infrastructure Settings" on page 80

1 Configure the IDM Server to Secure HP Business Availability Center Resources

a You must configure the IDM server to secure HP Business Availability Center resources. For details, see your IDM vendor's documentation.

b Configure or disable the security setting of the appropriate HP Business Availability Center URLs on the IDM server. The URLs are contained in the following files:

- **\HPBAC\conf\settings\SingleSignOn\SSOsecuredURL.txt.** URLs which must be secured.
- **\HPBAC\conf\settings\SingleSignOn\SSOnonsecuredURL.txt.** URLs which must be non-secured.

If you are configuring an IDM server while using a reverse proxy, you must configure the appropriate URLs listed in the HP Business Availability Center Hardening Guide. For a list of these URLs, see "Support for Both HP Business Availability Center Data Collectors and Application Users" in the *HP Business Availability Center Hardening Guide* PDF.

Note:

- URLs that are indicated by either of these files as requiring Basic Authentication must be configured with Basic Authentication on the IDM-SSO server.
- If your IDM-SSO vendor enables you to configure your authentication setting per URL, you must configure any Business Process Monitor URLs to use Basic Authentication. If your IDM-SSO vendor requires you to configure your authentication setting per application, the presence of any Business Process Monitor URLs means that you must configure all of the application's URLs to use Basic Authentication.

---

2 Login to the IDM Server

You login to the IDM server from the IDM login page, which adds the username to the current session header. The header name is used to configure the **Header name** Infrastructure Settings entry in the "Configure IDM-SSO Infrastructure Settings" step below.

3 Verify IDM-SSO Configuration

You must verify that the IDM-SSO server is configured correctly, by following this process:

a Open the IDM login page by navigating to the following URL:

http://<gateway for Business Availability Center server name>.devlab.ad/topaz/verifyIDM.jsp

b Enter the IDM username and password to login to the IDM server.

c Enter an HTTP request header in the Header Name field. If the header name is valid, enter the header name in the relevant field in Infrastructure Settings, as described below.

4 Configure IDM-SSO Infrastructure Settings

You configure IDM-SSO Infrastructure Settings in the Infrastructure Settings Manager, as follows:

a Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, and select **Single Sign On**.

b Locate the **Header name** entry in the Single Sign On - Identity Management (IDM-SSO) field, click the **Edit Setting** button and enter the HTTP header name for the user identity attribute as defined by the IDM server.

c Optionally, you can configure an alternate logout URL to view a page other than the main login page when logging out of HP Business Availability Center.

- Specify the desired URL in the IDM server. The default logout URL is **/topaz/logout.jsp**. For details, refer to your IDM server's documentation.
- In the Logout URL field, click the **Edit Setting** button and enter the URL of the page you want to appear when logging out of HP Business Availability Center.

The change takes effect immediately.

d In the Single Sign On - Identity Management (IDM-SSO) field, locate the **Enable IDM-SSO Authentication** entry and configure the setting to **True**.

The changes remain in effect for all future web sessions.

To reset your system to configurations before IDM-SSO was connected, you must use the JMX console. For details, see "Resetting LDAP/SSO Settings via the JMX Console" on page 38.

6

Lightweight Directory Access Protocol (LDAP) Authentication and Mapping

This chapter provides information on the Lightweight Directory Access Protocol (LDAP) Authentication and Group Mapping strategies.

This chapter includes:

Concepts

Tasks

Lightweight Directory Access Protocol (LDAP) Authentication - Overview

You can use an external LDAP server to store authentication information (usernames and passwords) of HP Business Availability Center users instead of using the internal HP Business Availability Center service. You can also use the LDAP server for mapping HP Business Availability Center user groups to groups configured on the LDAP server. For optimal performance, it is recommended that the Business Availability Center servers and LDAP server be in the same subnet. For optimal security, it is recommended to either configure an SSL connection between the Business Availability Center Gateway server and LDAP server, or to have Business Availability Center servers and the LDAP server on the same secure internal network segment.

For details on defining an LDAP authentication strategy, see "Define an LDAP Authentication Strategy – Workflow" on page 86.

For details on mapping groups with the LDAP server, see "Mapping Groups with LDAP" on page 84.

Mapping Groups with LDAP

The LDAP server can be used as a user repository for mapping user groups on the LDAP server to user groups in HP Business Availability Center. If users are moved between LDAP groups, they are automatically moved between the corresponding mapped groups located on the HP Business Availability Center server once you login again to HP Business Availability Center. Individual HP Business Availability Center users must be nested in groups to be included in mapping from the LDAP groups.

Synchronizing groups is done via the Group Mapping function, which is accessible via the **Groups Mapping** button on the Users and Permissions interface. This button is enabled only if the following conditions are met:

- The LDAP setting in HP Business Availability Center Infrastructure settings is configured either to **Authentication** or **Mapping**.
- The user has administrator permissions.

Once LDAP groups are synchronized with HP Business Availability Center groups, all User Management configuration options on the Users and Permissions interface are disabled, the password field in Users and Permissions is invisible, and you cannot nest users in groups via the Hierarchy tab, as these actions are managed by the LDAP server.

If you want to change the attribute that a user logs in to the application with (such as from a username to an email address), you must change the **Unique User ID** setting in the Infrastructure Settings from **uid** to the appropriate attribute (such as **idnumber**) that you want to login with. If the user belongs to a group, they retain the permissions of that group. If they do not belong to a group, you must reconfigure the permissions for that user.

For details on synchronizing LDAP groups with HP Business Availability Center groups, see "Synchronize User Groups with LDAP" on page 90.

For details on synchronizing groups after upgrading from a previous version of HP Business Availability Center, see "Synchronizing Groups After Upgrading from a Previous Version of HP Business Availability Center" on page 85.

Synchronizing Groups After Upgrading from a Previous Version of HP Business Availability Center

When upgrading from a previous version of HP Business Availability Center, the **Enable User Synchronization** setting in Infrastructure Settings is by default set to **False**. This enables you to map the LDAP groups to groups in HP Business Availability Center via the Group Mappings button on the Users and Permissions interface. For details on the Group Mappings button, see "Group Mappings Dialog Box" on page 451. If you do not map the groups at this time, all HP Business Availability Center groups are nested under the Root directory.

Once the LDAP and HP Business Availability Center groups have been mapped, you must change the **Enable User Synchronization** setting in Infrastructure Settings to **True** for users to be synchronized upon login to HP Business Availability Center.

Define an LDAP Authentication Strategy – Workflow

This task describes how to define an LDAP Authentication Strategy in HP Business Availability Center.

This task includes the following steps:

- "Verify LDAP Integration with the Test LDAP Integration Tool" on page 86
- "Configure Infrastructure Settings to Set an LDAP Authentication Strategy" on page 87
- "Enable an LDAP Authentication Strategy" on page 89

1 Verify LDAP Integration with the Test LDAP Integration Tool

You must verify that the LDAP server has been configured correctly before assigning LDAP as your authentication strategy, or mapping your HP Business Availability Center groups to groups on the LDAP server.

a Navigate to the Test LDAP Integration Tool window, located at:

<HP Business Availability Center root directory>/tools/testLDAP

b Select the appropriate file to run:

- **For Windows Users.** Select the .bat file.
- **For UNIX Users.** Select the .sh file.

c Enter the relevant information in the available fields, as follows:

- **LDAP Server URL**
- **User unique ID attribute**
- **Full Distinguished Name of Search-Entitled User.** You must enter the full value of the Search-Entitled User.
- **Password of Search-Entitled User**
- **Find this user unique ID.** The username of a specific user on the LDAP server that you want to search for.

Click **Find** to verify that the LDAP integration has been configured successfully.

You then enter information in the following fields:

- **Found DN.** This field is filled automatically if the Find operation is successful.
- **Password.** The password of the user indicated in the user unique ID field.

Click **Bind** to verify that the selected user exists in the LDAP server, and that LDAP authentication can be performed according to the information entered in the verification tool.

Once these values are verified as correct by the Test LDAP Integration tool, you then enter the values in the appropriate fields on the Infrastructure Settings page. To access the Infrastructure Settings page, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose the **Foundations** context and select **LDAP Configuration** from the list.

2 Configure Infrastructure Settings to Set an LDAP Authentication Strategy

To set up an LDAP authentication strategy, you must first modify the settings in the Infrastructure Settings Manager. Any changes you make remain in effect for all future Web sessions.

To access the Infrastructure Settings Manager, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, and select the **LDAP Configuration** context. Perform the following steps in the relevant Infrastructure Settings:

a **Modify the LDAP URL Value.** Locate the **LDAP Server URL** entry in the LDAP Configuration - LDAP General table. Modify the value using the following format:

ldap://<ldapHost>[:<port>]/[<baseDN>][??scope]

For example: ldap://my.ldap.server:389/ou=People,ou=myOrg.com??sub

For SSL: ldaps://my.ldap.server:636/ou=People,ou=myOrg.com??sub

The default protocol used to communicate with the LDAP server is TCP, but you can change the protocol to SSL. For details, see “Using SSL in HP Business Availability Center” in the *HP Business Availability Center Hardening Guide* PDF.

b Enter the Password of Search-Entitled User. Locate the **Password of Search-Entitled User** entry in the LDAP Configuration-LDAP General Authentication pane. Enter the Password of the Search-Entitled User.

c Configure the Users Filter Value. Locate the **Users filter** entry in the LDAP Configuration - LDAP General table. Configure the value according to the type of LDAP server in use.

d Configure LDAP General Authentication Values

- In the LDAP Configuration - LDAP General Authentication table, locate the **Distinguished Name (DN) Resolution** entry. Ensure that the value is set to **True**. You then enter relevant values in the following fields:
- **Distinguished Name of Search-Entitled User**
- **Password of Search-Entitled User**
- **Search Retries Count** (optional)

e Configure Groups DN and Root Groups DN

- In the LDAP Configuration - LDAP General Authentication table, locate the **Groups base DN** and **Root groups base DN** entries. Enter the full DN for each setting.

f Configure LDAP Setting

- Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, select **LDAP Configuration**, and locate the **Remote Users Repository Mode** entry in the LDAP Configuration - LDAP General table. Modify the value to either **Mapping** or **Authentication**.

g Configure Microsoft Active Directory Default Settings

If you are using Microsoft Active Directory for LDAP, you must also configure the appropriate default Infrastructure Settings to validate your LDAP configuration before running the Test LDAP Integration tool:

- Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, and select **the LDAP Configuration** context. Navigate to the LDAP Configuration - LDAP General pane, and configure the **Users Filter** setting where the following value is true:

```
Users filter=(&(sAMAccountName=*)(objectclass=user))
```

➤ In the LDAP Configuration - LDAP Options for Classes and Attributes pane, configure the following settings with the indicated values:

Group class object=group

Groups member attribute=member

User unique ID attribute=sAMAccountName

Users object class=user

Note: If you have upgraded from a version prior to HP Business Availability Center 7.5, the AuthenticationUpgrader checks if LDAP had been configured using the old authentication type settings and if so, assigns the above settings in Infrastructure Settings, and also sets the Remote Users Repository mode setting to **authentication.**

---

3 Enable an LDAP Authentication Strategy

You must enable the LDAP Authentication Strategy for it to take effect.

a In the Infrastructure Settings Manager, choose **Foundations** and select the **LDAP Configuration** context.

b In the **LDAP Configuration - LDAP General** table, locate the **Remote Users Repository Mode** entry and select from the following values:

➤ **Mapping.** LDAP Active Directory is enabled only for group mapping and not for user authentication.

➤ **Authentication.** LDAP Active Directory is enabled for both group mapping and user authentication.

To disable LDAP from being used for either group mapping or user authentication, select **Disabled**.

The changes take effect immediately.

Synchronize User Groups with LDAP

This task describes how to synchronize LDAP user groups with HP Business Availability Center user groups:

This task includes the following steps:

- "Verify LDAP Integration with the Test LDAP Integration Tool" on page 86
- "Configure Infrastructure Settings to Set an LDAP Synchronization Strategy" on page 90
- "Create a Superuser in HP Business Availability Center that Matches an LDAP Superuser" on page 91
- "Enable User Synchronization" on page 91
- "Create HP Business Availability Center Groups" on page 91
- "Map LDAP Groups to HP Business Availability Center Groups" on page 91

1 Verify LDAP Synchronization

You verify that the LDAP server has been configured correctly before you can synchronize LDAP groups with HP Business Availability Center groups. For details, see "Verify LDAP Integration with the Test LDAP Integration Tool" on page 86.

2 Configure Infrastructure Settings to Set an LDAP Synchronization Strategy

To set up an LDAP authentication strategy, you must first modify the settings in the Infrastructure Settings Manager. Any changes you make remain in effect for all future Web sessions.

For details on configuring Infrastructure Settings, see "Configure Infrastructure Settings to Set an LDAP Authentication Strategy" on page 87.

3 Create a Superuser in HP Business Availability Center that Matches an LDAP Superuser

If there are no LDAP superusers whose credentials match those of an HP Business Availability Center superuser, it is not possible to login to HP Business Availability Center as a superuser. Therefore, you should create a superuser in HP Business Availability Center that matches the username credentials of a superuser on the LDAP server to ensure that once user synchronization is enabled, you can login to HP Business Availability Center with a superuser.

If you did not do this before enabling user synchronization, create a superuser on the LDAP server whose credentials match those of the default HP Business Availability Center superuser. You can then login to HP Business Availability Center as a superuser.

4 Enable User Synchronization

Access the HP Business Availability Center Infrastructure Settings manager, by navigating to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, and select the **LDAP Configuration** context. In the LDAP Configuration - LDAP General table, locate the Enable User Synchronization entry and verify that the value is set to **True**.

5 Create HP Business Availability Center Groups

You must create local HP Business Availability Center groups that can be assigned to the remote LDAP server. For details on creating groups in HP Business Availability Center, see “Groups/Users Pane” on page 447.

6 Map LDAP Groups to HP Business Availability Center Groups

You map user groups on the LDAP server with groups in HP Business Availability Center to synchronize LDAP groups and HP Business Availability Center groups and enable management of your HP Business Availability Center groups via the LDAP server, as follows:

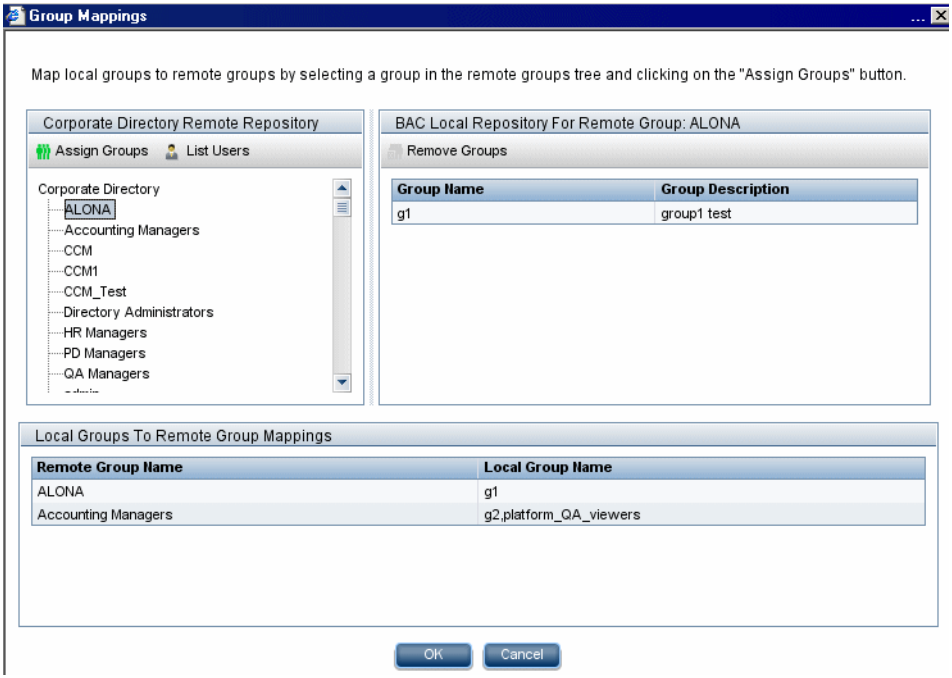
a On the Users and Permissions interface, navigate to the Groups/Users pane and click the **LDAP Synchronization** button and select **Group Mappings** to open the Group Mappings dialog box.

b In the **<Repository Name> Remote Repository** pane, select a remote LDAP server group and click **Assign Groups**.

The HP Business Availability Center groups synchronized with the selected LDAP group are displayed in the **BAC Local Repository for Remote Group: <group name>** pane.

Existing synchronization of all LDAP groups is displayed in the **Local Groups to Remote Groups Mapping** pane.

Note: If you have upgraded from a version prior to HP Business Availability Center 7.5, ensure that the **Enable User Synchronization** setting in the LDAP Configuration - LDAP General table is set to **false.**



For an explanation of the Group Mappings dialog box, see "Group Mappings Dialog Box" on page 527.

Delete Obsolete Users

This task describes how to delete HP Business Availability Center users who no longer exist on the LDAP server.

This option is enabled only if the following conditions are met:

- The LDAP setting in HP Business Availability Center Infrastructure settings is configured either to **Authentication** or **Mapping**.
- The user has delete permissions.

To delete obsolete users:

1 Select **Admin** > **Platform** > **Users and Permissions,** click the **Group Mappings** button in the Groups/Users pane, and select **Delete Obsolete Users**.

2 Select the user you want to delete.

Troubleshooting and Limitations

If you have configured HP Business Availability Center to use the LDAP Authentication Strategy and are unable to login to HP Business Availability Center, see the HP Software Self-solve knowledge base (http://h20230.www2.hp.com/selfsolve/document/KM547160). To enter the knowledge base, you must log in with your HP Passport ID.

7

Lightweight Single Sign-On Authentication - General Reference

This chapter provides general reference information on the Lightweight Single Sign-On (LW-SSO) authentication strategy, applicable to LW-SSO version 1.0.

This chapter includes:

- Inbound Configurations on page 132
- Inner Inbound Configuration Types on page 132
- Outbound Configurations on page 139
- Inner Outbound Configuration Types on page 139

Troubleshooting and Limitations on page 147

LW-SSO Requirements

The requirements for LW-SSO configuration, per application, are as follows:

Application	Version	Comments
Java	1.5 and higher	N/A
HTTP Sevlets API	2.1 and higher	N/A
Internet Explorer	6.0 and higher	Browser should enable HTTP session cookie and HTTP 302 Redirect functionality
FireFox	2.0 and higher	Browser should enable HTTP session cookie and HTTP 302 Redirect functionality
Tomcat Authentications	Standalone Tomcat 5.0.28 Standalone Tomcat 5.5.20	N/A
Acegi Authentications	Acegi 0.9.0 Acegi 1.0.4	N/A
Web Services Engines	Axis 1 - 1.4 Axis 2 - 1.2 JAX-WS-RI 2.1.1	N/A

HP Products Integrated with LW-SSO

The HP products that are currently integrated with the LW-SSO authentication strategy are:

- **Business Availability Center.** Version 7.50
- **Business Process Insight.** Version 7.5
- **Dashboard Foundation.** Version 4.1
- **Diagnostics.** Version 7.5
- **Service Center.** Version 6.2
- **TransactionVision.** Version 7.5

LW-SSO Infrastructure Configuration

LW-SSO Infrastructure Configuration is performed in the lwssofmconf.xml file, located at HPBAC\conf\settings\SingleSignOn\lwssofmconf.xml.

LW-SSO configuration contains the following attributes:

- **Enabled.** Configured whether the UI token validation is enabled or disabled. Parameters are set as follows: **enabled = true**, **disabled = false**.
- **Web LW-SSO.** Configures the behavior of LW-SSO UI.

The following table lists elements of Web LW-SSO:

Element	Use	Description
lwsso or Identity Management	Required	Describes a token that is used for LW-SSO UI. For sub-elements of the lwsso element, see “lwsso” on page 99.
logoutURLs	Optional	When an application requests one of these URLs, the LW-SSO infrastructure cleans the security context.

Element	Use	Description
nonsecureURLs	Optional	When application requests one from these URLs, the LW-SSO infrastructure does not check the SecurityToken.
protectedDomains	Optional	List of domains that allow multi domain support for the selected application.
reverseProxy	Optional	ReverseProxy configuration.
roleSecurityFramewOrkIntegration	Optional	Describes roles mapping support for Acegi integration.
groupSecurityFrameworkIntegration	Optional	Describes groups mapping support for Acegi integration.

You can make changes to the LW-SSO configuration, via the JMX Console. Click **Invoke** in the **invokeGetInternalLWConf** setting, to view the current LW-SSO Configuration. You can change the following settings:

- **Domain.** The Application domain, used by LW-SSO infrastructure for LW-SSO token (cookie) creation.
- **Enabled**
- **Expiration Period**
- **initString**
- **Protected Domains**

Web LW-SSO Sub-Elements - Description

This section provides a detailed description of the Web LW-SSO Elements, and their respective sub-elements.

lwsso

The following table describes the sub-elements of the lwsso element:

Sub-element	Use	Attributes	Description
N/A	required	startLWSSO	An attibute that allows creation of an LW-SSO token when the application calls to enableSSO. **Set to disabled on an application with weak authentication.**
domain	optional	N/A	The Application domain. Used by LW-SSO infrastructure for LW-SSO token (cookie) creation. **Required to configure the domain for Multidomain support and for Normalized URL Parameter functionality.**
crypto	required	N/A	Defines how the LW-SSO token is encrypted. For details on this element, see the table below.

Sub-element	Use	Attributes	Description
expirationPeriod	required	N/A	Defines (in minutes) the expiration time of the security token. **The recommended value is 60 minutes. For an application that does not require a high level of security, you can configure a value of 300 minutes.**

Attributes of crypto sub-element

The following table describes attributes of the crypto sub-element:

Name	Default Value	Permitted Values	Description
cipherType	symmetricBlockCipher	symmetricBlockCipher	N/A
engineName	AES	AES, Null	Use **AES** for a production environment. **Null** does not encrypt a token value and should be used only for POC. Do not use Null in a production environment.
paddingModeName	CBC	CBC	N/A
keySize	256	256	N/A
encodingMode	Base64Url	Base64Url	N/A

Name	Default Value	Permitted Values	Description
initString	N/A	N/A	It is not possible to use LW-SSO without setting the initString parameter. You must set it either in the configuration file or (for UI) in the ConfigurationManagerUtils API.

Example

```
<lwsso-config
 xmlns="http://www.hp.com/astsecurity/idmenablmentfw/lwsso/1.0">
 <webui enabled="true">
      <web-lwsso>
           <lwsso startLWSSO="enabled">
                <domain>mercury.global</domain>
                <crypto cipherType="symmetricBlockCipher"
                     engineName="AES" paddingModeName="CBC" keySize="256"
                     encodingMode="Base64Url" initString="This is a shared secret
passphrase"></crypto>
                <expirationPeriod>60</expirationPeriod>
           </lwsso>
      </web-lwsso>
 </webui>
</lwsso-config>
```

identity management

Identity Management configuration describes the mapping between an HTTP request and Security Context Data.

The following table describes the sub-elements of the identity management element:

Sub-element	Use	Attributes	Description
username	required	N/A	Name of the header in the request that contains the username.
customer	optional	N/A	Name of the header on the request that contains the customer.
token	optional	N/A	Name of the cookie on the request that contains the IDM token.
roles	optional	separator	Name of the header on the request that contains the list of roles. **separator** - a character that is used to separate between roles.
personalization -field	optional, unbounded	key	Name of the header on the request that contains the personalization field. **key** - key for the personalization field on the Security Context Data.

Example

```
<lwsso-config
 xmlns="http://www.hp.com/astsecurity/idmenablmentfw/lwsso/1.0">
 <webui enabled="true">
      <web-lwsso>
           <identity-management>
                <username>sm-user</username>
                <token>SMSESSION</token>
                <roles separator=";">sm-roles</roles>
                <personalization-field key="email">sm-mail</personalization-field>
                <personalization-field key="phone">sm-workphone</personalization-
field>
           </identity-management>
      </web-lwsso>
 </webui>
</lwsso-config>
```

loginURL

This element is not used in LW-SSO release 1.0.

logoutURLs

When one of these are requested by an application, the LW-SSO infrastructure cleans the security context, supports the optional parameters **parameterName** and **parameterValue**, and allows more flexibility for the URL configuration.

In the example below, LW-SSO infrastructure cleans the security context when the application requests **App1/logout.jsp?reallyLogout=yes** or **App2/logout.jsp**

Example

```
<logoutURLs>
 <url parameterName="reallyLogout" parameterValue="yes">App1/logout.jsp</url>
 <url>App2/logout.jsp</url>
</logoutURLs>
```

Note: The logoutURLs property is relevant only when the LW-SSO Filter is used.

---

nonsecureURLs

When one of these URLs is requested by an application, the LW-SSO infrastructure does not check the SecurityToken. It is recommended to add documentation, images, etc. to nonsecureURLs.

- nonsecureURLs supports the optional parameters, **parameterName** and **parameterValue**, and allows more flexibility for the URL configuration.
- The URL configured in nonsecureURLs is the URL after the server name (with a port number). For example, the string **App/Documentation** means <Any servername>/App/Documentation. Similarly, the following URLs are non-secured:

  http://flood.mercury.global:8080/App/Documentation/help.jsp

  http://flood.mercury.global:8080/App/Documentation/index.jsp

Example

```
<nonsecureURLs>
  <url>App/Documentation</url>
  <url>App/Images</url>
</nonsecureURLs>
```

Note: The nonsecureURLs property is relevant only when the LW-SSO Filter is used.

---

protectedDomains

The domains that allow multi-domain support for the application.

All domains, including the application domain, must be included in the list.

You must also add the correct domain in the **lwsso** element of the configuration.

Example

```
<protectedDomains>
 <url>mercury.global</url>
 <url>devlab.ad</url>
 <url>emea.hpqcorp.net</url>
</protectedDomains>
```

reverseproxy

The following table describes the sub-elements of the reverseProxy element:

Sub-element	Use	Attributes	Description
N/A	required	enabled	An attribute of the webui element that is configured whether the reverseProxy is enabled or disabled.
fullServerURL	enabled	N/A	The full reverseProxy server URL includes the schema (http or https) and port.
reverseProxyIPs	optional	N/A	List of the reverse proxy IPs .

Example

```
<fullServerURL>http://flood.mercury.global:88/</fullServerURL>
 <reverseProxyIPs>
       <url>16.59.45.143</url>
       <url>16.59.60.117</url>
 </reverseProxyIPs>
</reverseProxy>
```

roleSecurityFrameworkIntegration

This is an optional element that describes roles mapping support for Acegi integration.

The following table describes the attributes of the roleSecurityFrameworkIntegration element:

Name	Use	Permitted Values	Description
rolePrefix	optional	string	The prefix is added to a role name during conversion from **SecurityContext** to **Security Framework**. During a conversion of roles from **Security Framework** to **SecurityContext**, only roles with the prefix are converted to **SecurityContext**, and the prefix is removed.

Name	Use	Permitted Values	Description
fromLWSSOTo SecurityFramework	➤ internal ➤ external ➤ both	required	Describes how to take roles during the conversion from SecurityContext to Security Framework. Available options are (respectively): ➤ Take only Security Framework roles ➤ Take only SecurityContext roles ➤ Take both SecurityContext and Security Framework roles
fromSecurityFrameworkToLWSSO	➤ enabled ➤ disabled	required	Describes how to take roles during a conversion from **Security Framework** to **SecurityContext**. Available options are (respectively): ➤ Take Security Framework roles ➤ Do not take Security Framework roles
caseConversion	optional	➤ upperCase ➤ lowerCase	Describes how to convert roles (on both sides). Available options are (respectively): ➤ Convert role name to upperCase ➤ Convert role name to lowerCase

Example

```
<roleSecurityFrameworkIntegration
 rolePrefix="ROLE_"
 fromLWSSOToSecurityFramework="both"
 fromSecurityFrameworkToLWSSO="enabled"
 caseConversion="upperCase"/>
```

groupSecurityFrameworkIntegration

This is an optional element that describes groups mapping support for Acegi integration.

The following table describes the sub-elements for the **groupSecurityFrameworkIntegration** element:

Name	Use	Permitted Values	Description
groupPrefix	optional	string	The prefix is added to a group name during a conversion from **SecurityContext** to **Security Framework**. During a conversion of groups from **Security Framework** to **SecurityContext**, only groups with the prefix are converted to **SecurityContext**, and the prefix is removed.

Name	Use	Permitted Values	Description
fromLWSSOTOSecurityFramework	required	➤ internal ➤ external ➤ both	Describes how to take groups during a conversion from SecurityContext to Security Framework. Available options are (respectively): ➤ Take only Security Framework groups ➤ Take only SecurityContext groups ➤ Take both SecurityContext and Security Framework groups
fromSecurityFrameworkToLWSSO	required	➤ enabled ➤ disabled	Describes how to take groups during a conversion from **Security Framework** to **SecurityContext**. Available options are (respectively): ➤ Take Security Framework groups ➤ Do not take Security Framework groups
caseConversion	optional	➤ upperCase ➤ lowerCase	Describes how to convert groups (on both sides). Available options are (respectively): ➤ Convert group name to upperCase ➤ Convert group name to lowercase.

Example

```
<groupSecurityFrameworkIntegration
 groupPrefix="GROUP_"
 fromLWSSOToSecurityFramework="both"
 fromSecurityFrameworkToLWSSO="enabled"
 caseConversion="upperCase"/>
```

lwssofmconf.xml file example (LW-SSO Token)

This section displays an example of the lwssofmconf.xml file (LW-SSO Token):

Example

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Sample XML file generated by XMLSPY v5 rel. 3 U (http://www.xmlspy.com)-->
<lwsso-config
 xmlns="http://www.hp.com/astsecurity/idmenablmentfw/lwsso/1.0">
 <webui enabled="true">
       <web-lwsso>
            <lwsso startLWSSO="enabled">
                 <domain>mercury.global</domain>
                 <crypto cipherType="symmetricBlockCipher"
                      engineName="AES" paddingModeName="CBC" keySize="256"
                      encodingMode="Base64Url" initString="This is a shared secret
passphrase"></crypto>
                 <expirationPeriod>60</expirationPeriod>
            </lwsso>


            <loginURL>WebApp/login.jsp</loginURL>
```

```
<logoutURLs>
                <url parameterName="reallyLogout"
parameterValue="yes">WebApp/logout.jsp</url>
                <url>WebApp/logout.jsp</url>
            </logoutURLs>

            <nonsecureURLs>
                <url>WebApp/login</url>
            </nonsecureURLs>

            <protectedDomains>
                <url>mercury.global</url>
                <url>devlab.ad</url>
                <url>emea.hpqcorp.net</url>
            </protectedDomains>

                    <reverseProxy enabled="true">
                <fullServerURL>http://flood.mercury.global:88/</fullServerURL>
                <reverseProxyIPs>
                    <url>16.59.45.143</url>
                    <url>16.59.60.117</url>
                </reverseProxyIPs>
            </reverseProxy>

            <roleSecurityFrameworkIntegration
                rolePrefix="ROLE_"
                fromLWSSOToSecurityFramework="both"
                fromSecurityFrameworkToLWSSO="enabled"
                caseConversion="upperCase"/>


        </web-lwsso>
 </webui>
</lwsso-config>
```

lwssofmconf.xml file example (IdM Token)

This section displays an example of the lwssofmconf.xml file (IdM Token):

Example

```
<?xml version="1.0" encoding="UTF-8"?>
<lwsso-config
 xmlns="http://www.hp.com/astsecurity/idmenablmentfw/lwsso/1.0">
 <webui enabled="true">
       <web-lwsso>
            <identity-management>
                 <username>sm-user</username>
                 <token>SMSESSION</token>
                 <roles separator=";">sm-roles</roles>
                 <personalization-field key="email">sm-mail</personalization-field>
                 <personalization-field key="phone">sm-workphone</personalization-
field>
            </identity-management>

            <nonsecureURLs>
                 <url>lwssoDemoApp/login</url>
            </nonsecureURLs>

            <roleSecurityFrameworkIntegration rolePrefix="ROLE_"
                 fromLWSSOToSecurityFramework="both"
                 fromSecurityFrameworkToLWSSO="enabled"
caseConversion="upperCase" />

       </web-lwsso>

 </webui>
</lwsso-config>
```

LW-SSO Filter Configuration

You must add the following to the Web.xml file:

```
<filter>
 <filter-name>LWSSO</filter-name>
 <filter-class>
       com.hp.sw.bto.ast.security.lwsso.LWSSOFilter
 </filter-class>
</filter>
<filter-mapping>
 <filter-name>LWSSO</filter-name>
 <url-pattern>/*</url-pattern>
</filter-mapping>
```

Note: The filter should be first in the Web application chain.

LW-SSO Use Cases

This section describes use cases for the LW-SSO framework:

- **Web Single Sign-On (Web SSO).** A user logs in to the first BTO application using his credentials and then wants to access the second BTO application in the same browser. Based on his login information to the first application, LW - SSO enables the user to enter the second application without requiring him to interactively re-authenticate his credentials.
- **Web Services Single Sign-On (WS SSO).** During a user request to the first BTO application, a call must be executed to the second BTO application. LW - SSO transfers user data to the second BTO application.
- A WebService (WS) call must be executed from the first BTO application to the second BTO application using information from the non-interactive user. LW - SSO transfers user data to the second BTO application.
- Single Sign-On can also be used as an abstraction layer between the BTO applications and external Identity Manager (IdM) systems, simplifying the product integration with IdM and reducing its developmental cost.

Note:

- LW-SSO passes the user information between the BTO Application 1 and BTO Application 2, but it is the application itself which authenticates the user.
- LW-SSO functions differently than IDM-SSO and is not a replacement for IDM-SSO.
- LW-SSO is a symmetric solution: A user logs into BTO Application1 and then opens a link to BTO Application 2 and vice-versa (first logs in to BTO Application 2 and then opens a link to BTO Application 1).

LW-SSO Components

This section describes the components that are contained within the LW-SSO infrastructure:

SecurityContextFactory

SecurityContextFactory is a native library which creates SecurityContext from user data.

SecurityContextFactory contains the following API:

```
public interface SecurityContextFactory {
    public SecurityContext createSecurityContext(String userName);
    public SecurityContext createSecurityContext(String userName, PropertyOrigin[]
roles, PropertyOrigin[] groups);
    public SecurityContext createSecurityContext(String userName, PropertyOrigin[]
roles, PropertyOrigin[] groups, Map<String,String> attributes);
    public SecurityContext createSecurityContext(String userName,  String customer);
    public SecurityContext createSecurityContext(String userName,  String customer ,
PropertyOrigin[] roles, PropertyOrigin[] groups);
    public SecurityContext createSecurityContext(String userName,  String customer,
PropertyOrigin[] roles, PropertyOrigin[] groups, Map<String,String> attributes);
}
```

ConfigurationManagerUtils

ConfigurationManagerUtils is a native library Responsible for loading, reloading and updating the LW-SSO framework configuration.

ConfigurationManagerUtils contains the following API:

```
public class ConfigurationManagerUtils implements ConfigurationManager {

    /**
 * The following methods load a configuration.
 * If application calls to init(), ConfigurationManagerUtils
 * looks for the lwssofmconf.xml file in the classpath and tries to load it
 */
public void init();
public void init(String fileName) throws FileNotFoundException;
public void init(InputStream inputStream) ;
public void initFromString(String theWholeConfiguration) ;
```

```
/**
 * The following methods will load a configuration.
 * If application calls to reload(), ConfigurationManagerUtils
 * looks for the lwssofmconf.xml file in the classpath and tries to reload it
 */

public void reload();
public void reload(String fileName) throws FileNotFoundException ;
public void reload(InputStream inputStream);
public void reloadFromString(String theWholeConfiguration);
```

```
/**
 *  The following methods return the LW-SSO framework build information:
 */
      public static String getBuildTime();
public static String getBuildVersion();
public static String getVersion() ;
public static String getName();
```

```
/**
  * The function returns the XML file string representing the LW-SSO configuration
  */
 public String getConfigurationString();
```

```
/**
  * The following functions can update the configuration.
  */

 void setEnabled(boolean enabled);
 boolean isEnabled();


 String getDomain();
 void setDomain(String domain);

 void setExpirationPeriod(int expirationPeriod);
 int getExpirationPeriod();


 String getInitString();
```

```
        * Allows setting initStringParam to LW-SSO before the loading of the
configuration.
       * Note: If you change initString by these API LWSSO will not save it in the
configuration file.
        * Why?
       * Because if application decide to save initString in its storage and not in the
configuration file.
       * Then, application only wants to update LW-SSO, so LWSSO will not persist it in
the file.
       * Please use method setAndPersistInitStringAndRecreateCrypto if you want to
persist initString
```

```
public static void setInitString(String initStringParam);

 /**
         * Allows setting initStringParam to LW-SSO after loading the configuration.
         * Additionally, encryptor and decryptor objects are recreated.
         * Note: If you change initString by these API LWSSO will not save it in the
configuration file.
         * Why?
         * Because if application decide to save initString in its storage and not in the
configuration file.
         * Then, application only wants to update LW-SSO, so LWSSO will not persist it in
the file.
         * Please use method setAndPersistInitStringAndRecreateCrypto if you want to
persist initString
        */
 void setInitStringAndRecreateCrypto(String initStringParam);
```

```
/**
         * Allows setting initStringParam to LW-SSO after loading the configuration.
         * The initStringParam parameter is persisted at the LW-SSO configuration file.
         * Additionally, encryptor and decryptor objects are recreated.
        */
    void setInitStringAndPersistAndRecreateCrypto(String initStringParam);


       boolean isStartLWSSOEnabled();
       void setStartLWSSOEnabled(boolean startLWSSOEnabled);


       void clearProtectedDomains();
       void addProtectedDomain(String protectedDomain);
       String[] getProtectedDomains();


       boolean isReverseProxyEnabled();
       void setReverseProxyEnabled(boolean reverseProxyEnabled);
       void setReverseProxy(String fullServerURL, String[] reverseProxyIPs);
       String getFullServerURL();
       String[] getReverseProxyIPs();
```

LW-SSO Filter

LW-SSO Filter is responsible for SecurityToken validation. It is an HTTP Servlet Filter and must be configured as the first filter in the Application chain. For details, see "LW-SSO Infrastructure Configuration" on page 97.

LW-SSO Utility

LW-SSO Utility is a native library that is responsible for enabling SSO and populating the SecurityContext within BTO Applications.

LW-SSO Utility contains the following API:

```
public class LWSSOUtils {
 /**
  * The function should be called when application wants to enable SSO.
```

```
* Generally it happens after the application authenticate a user and
  * create the user SecurityContext:
  * 1) The application authenticates a user
  * 2) The application creates user context with SecurityContextFactory :
  * SecurityContext securityContext = factory.createSecurityContext(userName);
  * 3) Application enables SSO
  * LWSSOUtils.enableSSO(servletRequest, servletResponse, securityContext);
  */
 public boolean enableSSO(HttpServletRequest httpServletRequest,
HttpServletResponse httpServletResponse,  SecurityContext securityContext);
```

```
/**
  * The function should be called when application wants to enable SSO.
  * Difference from the previous function is additional parameter domain.
  * The parameter passed here overrides the domain setting in the configuration
  * Generally it happens after the application authenticate a user and
  * create the user SecurityContext:
  * 1) The application authenticates a user
  * 2) The application creates user context with SecurityContextFactory :
  * SecurityContext securityContext = factory.createSecurityContext(userName);
  * 3) Application enables SSO
  * LWSSOUtils.enableSSO(HttpServletRequest, HttpServletResponse,
securityContext, domain);
  */

 public boolean enableSSO(HttpServletRequest httpServletRequest,
HttpServletResponse httpServletResponse,  SecurityContext securityContext, String
domain);
```

```
/**
  * Application should call the function when it needs to use SecurityContext.
  * SecurityContext securityContext =
LWSSOUtils.getSecurityContext(HttpServletRequest);
        */

 public SecurityContext getSecurityContext(HttpServletRequest httpServletRequest);
```

```
/**
  * Application should call the function when it needs to check if the request is secured.
  * The function should be used when LWSSOUtils.getSecurityContext returns null and
application
  * want to distinguish the in the following use cases:
  * 1)User wants to access some protected resource in the application without
authentication and a login screen should be shown
  * 2)User wants to access the login page or some resource that should not be
protected (for example, some help documents).
  * By default, all URL are secured.
  * LW-SSO infrastructure has its configuration with nonsecureURLs.
  * If user access these URLs the function isRequestSecured will always return false.
  * Otherwise, it will return true.
  * Note: The method will return correct answer only when LW-SSO Filter is used.
  */
 public boolean isRequestSecured (HttpServletRequest httpServletRequest);
```

```
/**
  * Application should call the function when it needs to check if LWSSO UI is enabled
        */

 public boolean isEnabled();

        /**
  * Application should call the function when it needs to add SecurityContext information
  * to request as request parameter. The function will create encrypted token from
SecurityContext,
  * and will return string with the value "LWSSO_PARAM_NAME=TOKEN".
     * When the request will be passed to a
  * Second application LWSSO framework will take this parameter and will create
SecurityContext
  * from it.
        */
       public static String getNormalizedUrlParam(SecurityContext securityContext,
SecurityContextType securityContextType)
}
```

Data Objects in the LW-SSO Framework

This section describes the various data objects contained in the LW-SSO framework.

SecurityContext

This object holds the entire SecurityContextData object.

Additionally, **validate()** is the method used to validate the SecurityToken before it is verified as legitimate (used by the LW-SSO infrastructure) and kept. The application creating the SecurityContext is responsible for propagating the information required by the other application in the integration, if required (for example, Groups, Roles). The SecurityContext object resides only in an application session and not in a transfer.

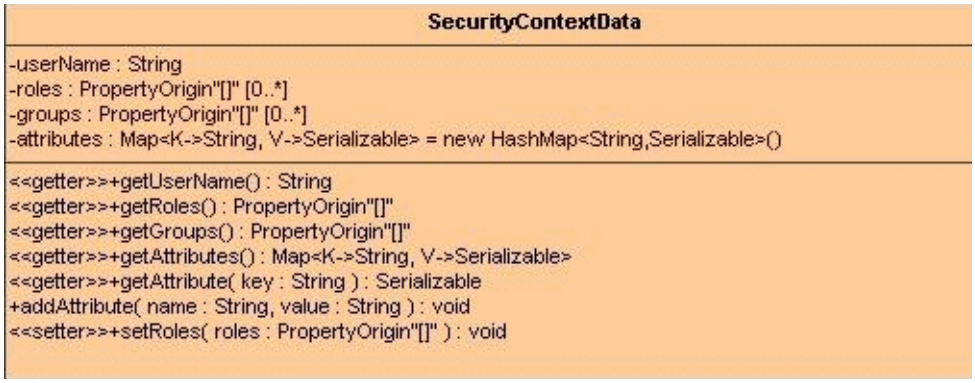
SecurityContextData

The application gets all information using getters from the SecurityContextData object.

The application (during authentication) cannot create the object directly but rather, it can create only the SecurityContext object. Additionally, during SSO, the application obtains the object from the SecurityContext.

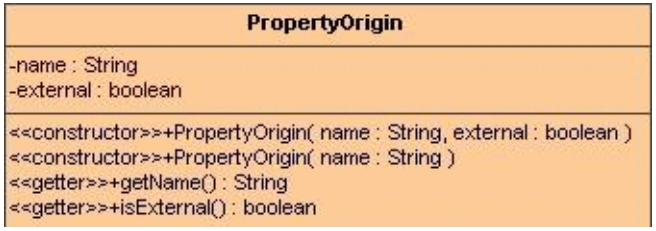
All of the user information related to the application can be used for session creation, authorization, and personalization, such as the username, the user's groups and roles, and the user's attributes (for example, email).

Only external groups and roles are transferred to the second application.



Property Origin

The string - boolean pair holds information on groups and roles. The boolean value indicates whether the group or role is external (received by the application from LDAP or IdM) or internal (received by the application directly). Only external groups and roles are transferred to the secondary applications.



Web Single Sign-On - Use Cases

This section describes use cases of single sign-on via the web.

This section includes:

Login Use Case

- The application authenticates the user.
- The application creates a user context using one of the SecurityContextFactory methods:

```
// The application creates user context with SecurityContextFactory.
// Please find below one example. Application can use any API of
SecurityContextFactory
String userName = "Bob";
SecurityContextFactory factory =
SecurityContextFactoryUtils.getSecurityContextFactory();
SecurityContext securityContext = factory.createSecurityContext(userName);
```

- The application enables Single Sign-On.

```
LWSSOUtils.enableSSO(servletRequest, servletResponse, securityContext);
```

Note: The weakest authentication framework used by the LW-SSO integrated applications determines the level of authentication security for all of the applications. It is recommended that only applications using strong and secure authentication frameworks issue an LW-SSO token.

Logout Use Case

A logout is declarative in LW-SSO. The logout pages are configured in the LW-SSO infrastructure configuration file. For details, see "LW-SSO Infrastructure Configuration" on page 97.

When an application requests a logout URL, LW-SSO cleans the security context.

Application Checks if Request is Secured - isRequestSecured

The application uses the **isRequestSecured** function to verify that the request is secured. This function is used when the **LWSSOUtils.getSecurityContext** returns a value of **null**, and the application wants to distinguish the following:

- You want to access a protected resource in the application without being authenticated, and a login screen is shown.
- You want to access the login page or a resource that is not be protected (for example, help documents).

```
boolean isSecured = LWSSOUtils.isRequestSecured(servletRequest);
```

By default, all URLs are secured, but LW-SSO infrastructure has its configuration with non-secure URLs.

If user accesses the non-secure URLs, the function returns a value of **false**.

If secure URLs are accessed, it returns a value of **true**.

Note: The method returns the correct answer only when the LW-SSO Filter is used.

For details, see "LW-SSO Infrastructure Configuration" on page 97.

Rules for Successful Integration

For successful integration with the LW-SSO Infrastructure, your application must adhere to the following pseudo code:

```
SecurityContext securityContext =
LWSSOUtils.getSecurityContext(httpServletRequest);
SecurityContext securityContext =
LWSSOUtils.getSecurityContext(httpServletRequest);
 if (securityContext != null) {
      if (APPLICATION_USER_SESSION == null) {
           // An application can use securityContext to create an application User session
      } else {
           // An application should check if securityContext user is updated
           // and to update the application User session
           // This use case can happens only if the other application has performed
logged out
           // and then logged in with a different user.
      }
} else {
      if (APPLICATION_RESPONSIBLE_FOR_AUTHENTICATION) {
           if (APPLICATION_USER_SESSION == null) {
                // In case there is no a securityContext and there is no an application
                // User session is a login use case.
                // The application opens the application login page
           } else {
                // In case there is no securityContext and there is an application User
session,
                // the other application already has performed logout,
                // and the application must perform the entire required logout process:
                // at least to clean the application User session.
                // Optionally, the application can open the application login page.
           }
      } else if (IDENTITY_MANAGER_RESPONSIBLE_FOR_AUTHENTICATION) {
           // In case there is no securityContext and the application works
           // in IdM mode (integration with IdM), the  application should show the error
page
           // without the option to continue. Please note, that if the request has come
           // to the application, the user has already been  authenticated by IdM.
           // In this case only one option that securityContext is null:
           // Application configures the LW-SSO framework to take some information
from IdM,
           // but IdM does not send this information.}}
```

LW-SSO Security Warnings

This section describes security warnings that are relevant to LW-SSO configuration:

- LW-SSO should be disabled unless it is specifically required.
- The weakest authentication framework used by the LW-SSO integrated applications determines the level of authentication security for all of the applications.

  It is recommended that only applications using strong and secure authentication frameworks issue an LW-SSO token.

- **Confidential InitString parameter in LW-SSO.** Lightweight SSO uses Symmetric Encryption to validate and create a token. The initString parameter within the configuration is used for initialization of the secret key. An application creates a token, and each application using the same initString parameter validates the token.
- **Symmetric encryption implication.** LW-SSO uses symmetric cryptography for issuing and validating LW - SSO tokens. Therefore, any application using LW-SSO can issue a token to be trusted by all other applications sharing the same initString. This potential risk is relevant when an application sharing an initString either resides or is accessible in an untrusted location.
- **User mapping (Synchronization).** The LW-SSO framework does not ensure user mapping between the integrated applications. Therefore, the integrated application must monitor user mapping. It is recommended that you share the same user registry (as LDAP/AD) among all integrated applications. Failure to map users may cause security breaches and negative application behavior, such as the same user name being assigned to different real users in the various applications.
- **Identity Manager.** Used for authentication purposes, all unprotected resources in the Identity Manager must be configured with the **nonsecureURLs** setting in the LW-SSO configuration.

Advanced Features

The following advanced features are available in the LW-SSO configuration:

- **Multi-domain support.** To work in a multi domain environment, you must configure the list of all domains (including the application domain) and the correct domain in the LW-SSO element of the configuration. For details, see "LW-SSO Infrastructure Configuration" on page 97.
- **Reverse Proxy support.** You must configure the Reverse Proxy in the configuration. For details, see "LW-SSO Infrastructure Configuration" on page 97.
- **Identity Manager (IdM) Systems abstraction layer.** You must configure the identity-management element in the configuration. For details, see "LW-SSO Infrastructure Configuration" on page 97.

➤ **Normalized URL Parameter Functionality: Add SecurityContext Information as Request Parameter.** This function creates an encrypted token from SecurityContext, and returns a string with the value **LWSSO_PARAM_NAME=TOKEN**. The application must add a parameter to the request string. When the request is passed to a secondary application, the LW-SSO framework takes this parameter and creates **SecurityContext** from it.

```
//1) The application creates a user context with SecurityContextFactory
// or obtain the existing security context
// Below is one example of the context creation. The application can use any API of
SecurityContextFactory
String userName = "Bob";
SecurityContextFactory factory =
SecurityContextFactoryUtils.getSecurityContextFactory();
SecurityContext securityContext = factory.createSecurityContext(userName);

// Below is one example of obtaining of the existing security context.
SecurityContext securityContext = LWSSOUtils.getSecurityContext(servletRequest);


// 2) Application creates an additional parameter
String param = LWSSOUtils.getNormalizedUrlParam(securityContext,
SecurityContextType.LWSSO);

// 3) Application adds a parameter to the request string
// 4) Application sends the request
```

Tomcat and Acegi Authentication

This section describes Tomcat and Acegi Authentication in an LW-SSO environment.

Tomcat Authentication

Use of LW-SSO is fully transparent for applications that use Tomcat Container authentication.

The logout page is configured via the application. For details, see “LW-SSO Infrastructure Configuration” on page 97.

If a user accesses the application without an LW-SSO token, the LW-SSO Authenticator authenticates the user and enables SSO with the user name and the user's roles.

If a user accesses the application with an LW-SSO cookie, the LW-SSO Authenticator creates a J2EE User from the token (the J2EE application calls the **getUserPrinciple** function).

Acegi Authentication

Usage of LW-SSO is partially transparent for an application that uses Acegi authentication.

The application should configure logout pages, role mapping (via the **roleSecurityFrameworkIntegration** element) and, if required, group mapping (via the **groupSecurityFrameworkIntegration** element). For details, see "LW-SSO Infrastructure Configuration" on page 97.

If a user accesses the application without the LW-SSO token, Acegi authenticates the user and the LWSSO Acegi filter enables SSO with the user name and the user's roles.

If a user accesses the application with an LW-SSO cookie, the LW-SSO Acegi filter creates an Acegi User from the token (Acegi application can access the Acegi user).

Web Services Single Sign-On and WS Security

This section describes the Security Types supported by LW-SSO for inbound and outbound Web Service calls:

Security Types Supported for Inbound Web Service Calls

- LW - SSO cookie
- IdM cookie
- Basic Authentication
- Basic Authentication used for trust with effective user passed by SAML (1.1)
- SAML (1.1)

Each inbound Web Service can be configured to support any combination of security levels, including those of the same type.

If the first handler successfully creates **SecurityContext**, the other handlers cannot create **SecurityContext**.

You can optionally add a validation handler: If **SecurityContext** was created, access to Web Services is enabled. If it was not, access to Web Services is denied.

Security Types Supported for Outbound Web Service Calls

- LW - SSO cookie
  - Reuses a UI cookie (WS-SSO) - the application must save the UI **SecurityContext** component.
  - Creates a new token with a configured, non-interactive user.
- IdM cookie
  - Reuses a UI cookie (WS SSO) - the application must save the UI **SecurityContext** component.
- Basic Authentication
  - Creates a new token with a configured, non-interactive user.
- Basic Authentication used for trust with effective user passed by SAML (1.1)
  - Creates a new token with a configured, non-interactive user.
- SAML (1.1)
  - Creates a new token with a configured, non-interactive user.

Web Services Configuration

The security of Web Services is configured under the **web-service** element. This is an optional element, as the web services may have no security at all.

Under the **web-service** element, you can invoke the inbound sub-element, the outbound sub-element, or both. The inbound sub-element configures incoming calls, and the outbound sub-element configures outgoing calls.

Example

```
<?xml version="1.0" encoding="UTF-8"?>
<lwsso-config
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xmlns="http://www.hp.com/astsecurity/idmenablmentfw/lwsso/1.0">
 <web-service>
      <inbound>
           <default>
                <in-saml certificateAlias="symphony" keyStorePassword="password"
keyStoreFileName="my.keystore">
                          </in-saml>

                <in-validate />
           </default>
      </inbound>
      <outbound>
           <default>
                <out-lwsso />
           </default>
           <service service-pattern="IncidentActions.*">
                <out-saml
                     issuer="TestAxisClient"
                     keyStoreFileName="my.keystore"
                     privateKeyAlias="symphony"
                     keyStorePassword="password"
                     privateKeyPassword="password">
                </out-saml>
           </service>
      </outbound>
 </web-service>
</lwsso-config>
```

Inbound Configurations

The Inbound sub-element configures security types for the incoming calls. It has a default configuration, and may also have a specific configuration per service or per several services.

Default Configuration

The default configuration of the incoming web-service calls is applied if no specific configuration is defined. You must define this element once the inbound element is used. Once a specific configuration is defined, the default configuration is ignored.

Service Specific Configuration

You can override the default configuration using a service specific configuration. The service specific configuration is defined per service name, and the service name is defined using java regular expressions.

Inner Inbound Configuration Types

Each inbound WS may be configured to support any combination of security levels, including those of the same type.

If the first handler successfully creates **SecurityContext**, the other handlers cannot create **SecurityContext**.

You can optionally add a validation handler (**in-validate element**): If **SecurityContext** was created, access to WS is enabled. If it was not, access to WS is denied.

This section describes the Inner Inbound Configuration Types, as follows:

- "LW-SSO Inbound Configuration" on page 133
- "Basic Authentication Inbound Configuration" on page 135
- "IdM Inbound Configuration" on page 136
- "SAML Inbound Configuration" on page 138

LW-SSO Inbound Configuration

This section describes the LW-SSO Inbound Configuration sub-elements.

Name	Use	Attributes	Description
N/A	required	startLWSSO	Allows creation of an LW-SSO token when the application calls to **enableSSO**. Set to **disabled** for an application with weak authentication.
domain	optional	N/A	The Application domain. Used by the LW-SSO infrastructure for the LW-SSO token (cookie) creation. You must configure the domain for Multidomain support and for Normalized URL Parameter functionality.
crypto	required	N/A	Defines how the LW-SSO token is encrypted.
expirationPeriod	required	N/A	Defines (in minutes) the expiration time of the security token. **The recommended value is 60 minutes. For an application that does not require a high level of security, you can configure a value of 300 minutes**.

crypto sub-element

This is a sub-element of the lw-sso element. The following table describes attributes for the crypto element:

Name	Default Values	Permitted Values	Description
cipherType	symmetricBlockCipher	symmetricBlockCipher	N/A
engineName	AES	➤ AES ➤ Null	Use AES for a production environment. Null does not encrypt a token value and should be used for POC only. **Do not use Null in a production environment.**
paddingModeName	CBC	CBC	N/A
keySize	256	256	N/A
encodingMode	Base64Url	Base64Url	N/A
initString	N/A	N/A	You cannot use LW-SSO without setting the initString parameter. You can set it either in the configuration file or in the ConfigurationManagerUtils API.

Example

```
<in-lwsso>
 <lwsso startLWSSO="enabled">
      <domain>mercury.global</domain>
      <crypto
           cipherType="symmetricBlockCipher"
           engineName="AES"
           paddingModeName="CBC"
           keySize="256"
           encodingMode="Base64Url"></crypto>
      <expirationPeriod>50</expirationPeriod>
 </lwsso>
</in-lwsso>
```

Basic Authentication Inbound Configuration

The following table describes attributes of the Basic Authentication Inbound Configuration:

Name	Default Values	Permitted Values	Description
parseUserDetails	ifexists	➤ always ➤ ifexists ➤ never	**always** - The token with user details is required in the message and must be parsed. If it is not found, an exception is thrown. **ifexists** - The token is parsed, if it exists. **never** - The token is never parsed, even if exists.

Name	Default Values	Permitted Values	Description
initString	N/A	N/A	You cannot use LW-SSO without setting the initString parameter. You can set it either in the configuration file or in the ConfigurationManagerUtils API. **Note:** This element is optional.

Note: These parameters are optional.

Container Level Security

Container level security is the preferred way to work with Basic Authentication.

When using container level security, authentication is done at the container level and not by the application. This means that the application doesn't need to code anything relating to authentication and needs only to configure the container.

IdM Inbound Configuration

IdM Inbound Configuration describes the mapping between an HTTP Request and Security Context Data.

The following table describes the sub-elements of IdM Inbound Configuration:

Name	Use	Attributes	Description
username	required	N/A	The header on the request containing the username.

Name	Use	Attributes	Description
customer	optional	N/A	The header on the request containing the customer.
token	optional	N/A	The cookie on the request containing the IdM token.
roles	optional	separator	Name of the header on the request containing the list of roles. **separator** - a character that is used to separate between roles.
personalization-field	optional, unbounded	key	Name of the header on the request containing the personalization field. **key** - the name of personalization field in the **SecurityContextData**.

Example

```
<in-identity-management>
   <identity-management>
      <username>sm-user</username>
      <roles separator=";">sm-roles</roles>
      <token>SMSESSION</token>
      <personalization-field key="email">sm-mail</personalization-field>
      <personalization-field key="phone">sm-workphone</personalization-field>
   </identity-management>
<in-identity-management>
```

SAML Inbound Configuration

The following table describes the attributes of SAML Inbound Configuration:

Name	Default Values	Permitted Values	Description
issuer	N/A	string	When defined, the issuer is validated to match the issuer.
keyStoreFileName	N/A	string	Path to the keystore file.
keyStorePassword	N/A	string	Password of the keystore file.
certificateAlias	N/A	string	Alias of the certificate containing the public key.
validateUsingEmbededKey	false	boolean	When value is **true** and if keystore is **undefined**, the verification checks if the assertion includes an embedded certificate. If found, it performs verification using this certificate.

Note: These attributes are optional.

Example

```
<saml keyStoreFileName="symphony.keystore"
    keyStorePassword="password"
    certificateAlias="symphony" />
```

Outbound Configurations

The Outbound element configures security types for the outgoing calls. It has a default configuration and may also have a specific configuration per service or per several services.

Default Configuration

The default configuration of the outgoing web-service calls is invoked if no specific configuration is defined. You must define this element once the outbound element is used. Once a specific configuration is defined, the default configuration is ignored.

Service Specific Configuration

You can override the default configuration using a service specific configuration. The service specific configuration is defined per service name, and the service name is defined using java regular expressions.

Inner Outbound Configuration Types

This section describes the Inner Outbound Configuration Types. Only one outbound configuration can be defined.

The Inner Outbound Configuration Types are as follows:

- "LW-SSO Outbound Configuration" on page 139
- "Basic Authentication Outbound Configuration" on page 144
- "IdM Outbound Configuration" on page 145
- "SAML Outbound Configuration" on page 145

LW-SSO Outbound Configuration

No attributes exist at the root element.

LW-SSO Outbound Configuration Sub-elements

➤ **Effective User.** This is an optional sub-element. The following table describes the attributes of the Effective User sub-element:

Name	Use	Permitted Values	Description
username	required	string	Username
customer	optional	string	Customer

➤ **LW-SSO.** This is an optional sub-element. The following table describes the attributes of the LW-SSO sub-element:

Name	Use	Attributes	Description
N/A	required	startLWSSO	Allows creation of the LW-SSO token when the application calls to enable SSO. Set to disabled on an application with weak authentication.
domain	optional	N/A	The Application domain. Used by LW-SSO infrastructure for LW-SSO token (cookie) creation. You must configure the domain for Multidomain support and for Normalized URL Parameter functionality.
crypto	required	N/A	Defines how the LW-SSO token is encrypted.

Name	Use	Attributes	Description
expirationPeriod	required	N/A	Defines (in minutes) the expiration time of the security token. The recommended value is 60 minutes. For an application that does not require a high level of security, you can configure a value of 300 minutes.

crypto sub-element

This is a sub-element of the lw-sso element. The following table describes attributes for the crypto element:

Name	Default Values	Permitted Values	Description
cipherType	symmetricBlockCipher	symmetricBlockCipher	N/A
engineName	AES	➤ AES ➤ Null	Use AES for a production environment. Null does not encrypt a token value and should be used for POC only. **Do not use Null in a production environment.**
paddingModeName	CBC	CBC	N/A
keySize	256	256	N/A
encodingMode	Base64Url	Base64Url	N/A
initString	N/A	N/A	You cannot use LW-SSO without setting the initString parameter. You can set it either in the configuration file or in the ConfigurationManagerUtils API. **Note:** This element is optional.

Example 1

When LW-SSO is used in the UI, the same cookie can be sent: <out-lwsso />

Example 2

New Cookie. If LW-SSO is not used in the UI, or if a cookie with a different encryption level is expected at the server side, a new cookie is created:

```
<out-lwsso>
 <lwsso startLWSSO="enabled">
      <domain>mercury.global</domain>
      <crypto
           cipherType="symmetricBlockCipher"
           engineName="AES"
           paddingModeName="CBC"
           keySize="256"></crypto>
      <expirationPeriod>50</expirationPeriod>
 </lwsso>
</out-lwsso>
```

Example 3

New Cookie + Effective User.

```
<out-lwsso>
 <lwsso startLWSSO="enabled">
      <domain>mercury.global</domain>
      <crypto
           cipherType="symmetricBlockCipher"
           engineName="AES"
           paddingModeName="CBC"
           keySize="256"></crypto>
      <expirationPeriod>50</expirationPeriod>
 </lwsso>
 <effective-user username="Yoyo" />
</out-lwsso>
```

Basic Authentication Outbound Configuration

The following table describes attributes of the Basic Authentication Outbound Configuration:

Name	Default Values	Permitted Values	Description
includeUserDetails	false	➤ true ➤ false	When value is **true**, a token with user details is added to the message's header.
username	N/A	String with username	The username of the static credentials. Once populated, the **password** field must also be populated.
password	N/A	Password	The password of the static credentials. Once populated, the **username** field must also be populated.
alwaysUseStaticCredentials	false	➤ true ➤ false	If the value is **true**: ➤ You must always use static credentials. ➤ Both the username and password fields must be populated. If the value is **false**, dynamic credentials will be used, if populated.

Basic Authentication Outbound Configuration Sub-elements

Effective User. The following table describes the attributes of the Effective User sub-element:

Name	Use	Permitted Values	Description
username	required	string	Username
customer	optional	string	Customer

Example

```
<out-basic-authentication
 includeUserDetails="true"
 username="username"
 password="password">
 <effective-user
       username="Yoyo"
       customer="Customer.ORG" />
</out-basic-authentication>
```

IdM Outbound Configuration

Configure the syntax as follows: `<out-identity-management/>`

SAML Outbound Configuration

The following table describes the attributes of the SAML Outbound Configuration. All attributes are required, unless otherwise noted:

Name	Default Values	Permitted Values	Description
issuer		string	The assertion's issuer
keyStoreFileName	N/A	string	The keystore path's file
keyStorePassword	N/A	string	The keystore's password

Name	Default Values	Permitted Values	Description
certificateAlias	N/A	string	The public key certificate's alias. When defined, the certificate is added to the outbound message. **Note:** This is an optional attribute.
validityPeriodInMilli	900000	long	Validity of the assertion in milliseconds. **Note:** This is an optional attribute.
validityToSendInPercent	30	int	Validity to send the assertion, defined in percentage of the validity period. Once the assertion has been issued within the valid time frame of the sent period, it can be reused. **Note:** This is an optional attribute.
sigalg	http://www.w3.org/2000/09/xmldsig#dsa-sha1	URI	Signature algorithm. **Note:** This is an optional attribute.
privateKeyAlias	N/A	string	Alias of the keystore's private key.
privateKeyPassword	N/A	string	Password of the keystore's private key.

SAML Outbound Configuration Sub-elements

Effective User. The following table describes the attributes of the Effective User sub-element:

Name	Use	Permitted Values	Description
username	required	string	Username
customer	optional	string	Customer

Example

```
<saml issuer="Symphony" keyStoreFileName="symphony.keystore"
    keyStorePassword="password" privateKeyAlias="private"
    privateKeyPassword="keypassword" />
```

Troubleshooting and Limitations

This section describes limitations of the LW-SSO configuration:

- The client must access the application with the Fully Qualified Domain Name (FQDN) in the login URL, for example: http://flood.mercury.global:8080/WebApp

  LW-SSO does not support URLs with an IP Address.

- Applications can leverage and use LW-SSO capabilities only if integrated within the LW-SSO framework in advance.
- BTO Application1 and BTO Application2 can use either the same user storage or separate user storages. However, if using separate user storages, they need to be able to synch user names, which is not handled in the LW - SSO framework.
- The JAAS Realm in Tomcat is not supported.
- Using spaces in Tomcat directories is not supported.

  It is not possible to use LW-SSO when a Tomcat installation path (folders) includes spaces (for example, Program Files) and the LW-SSO configuration file is located in the common\classes Tomcat folder.

- **Load Balancer Configuration.** A load balancer deployed with LW-SSO must be configured to use sticky sessions.
- **Reverse Proxy Configuration.** LW-SSO can support multiple symmetric reverse proxy virtual nodes, and can support only one asymmetric reverse proxy virtual node.

Example

- The following reverse proxy configurations are supported by LW-SSO:

  Example1:

  ProxyPass /App1 http://APP_server/App1

  ProxyPass /App2 http://APP_server/App2

  ...

  ProxyPass /AppN http://APP_server/App2N

  Example 2:

  ProxyPass Node1/App1 http://APP_server/App1

  ProxyPass Node1/App2 http://APP_server/App2

  ...

  ProxyPass Node1/AppN http://APP_server/AppN

- The following reverse proxy configuration is **not** supported by LW-SSO:

  ProxyPass Node1/App1 http://APP_server/App1

  ProxyPass Node2/App2 http://APP_server/App2

  …

  ProxyPass NodeN/AppN http://APP_server/AppN

- **Multi Domain Support.**

- Multi domain functionality is based on the HTTP referrer. Therefore, LW-SSO supports links from one application to another and does not support typing a URL into a browser window, except when both applications are in the same domain.
- All domains must be on the protected domain list in the JMX console.
- The first cross domain link using **HTTP POST** is not supported.

  Multi domain functionality does not support the first **HTTP POST** request to a second application (only the **HTTP GET** request is supported). For example, if your application has an HTTP link to a second application, an **HTTP GET** request is supported, but an **HTTP FORM** request is not supported. All requests after the first can be either **HTTP POST** or **HTTP GET**.

- LW-SSO Token size:

  The size of information that LW-SSO can transfer from one application in one domain to another application on another domain is limited to 15 Groups/Roles/Attributes (note that each item may be an average of 15 characters long).

- Linking from Protected (HTTPS) to Non protected (HTTP) in a Multi domain scenario:

  Multi domain functionality does not work when linking from a protected (HTTPS) to a non protected (HTTP) page. This is a browser limitation where the referring header is not sent when linking from a protected to a non-protected resource. For an example, see: http://support.microsoft.com/support/kb/articles/Q178/0/66.ASP

- Third-Party cookies behavior in Internet Explorer:

  Microsoft Internet Explorer 6 contains a module that supports the "Platform for Privacy Preferences(P3P) Project", meaning that cookies coming from a Third Party domain are by default blocked in the "Internet" security zone. Session cookies are also considered Third party cookies by IE, and therefore are blocked, causing LW - SSO to stop working. For details, see: http://support.microsoft.com/kb/323752/en-us.

To solve this issue, add the launched application (or a DNS domain subset as ***.mydomian.com**) to the "Intranet"/"Trusted" zone on your computer (on Microsoft Internet Explorer, select **Menu -> Tools -> Internet Options -> Security -> Local Intranet -> Sites -> Advanced**), which causes the cookies to be accepted.

Important: The LW-SSO session cookie is only one of the cookies used by the Third party application that are blocked.

LW-SSO Problems and Solutions

The following table describes potential problems that can occur with LW-SSO, and possible solutions for these problems:

Problem Description	Cause of Problem	Solution
LW-SSO fails to run the **enableSSO** function	A domain is not defined properly in the lwsso element of the configuration, or a domain that passed as a parameter to the **enableSSO** function is incorrect	1. Ensure that the domain is equal to the application's domain. 2. Ensure that the domain is either defined in the lwsso element of the configuration, or passed as a parameter to the enableSSO function.
LWSSO fails to receive information from the **NormalizedUrl** Parameter	A domain is not defined well in the lwsso element of the configuration	Ensure that the domain is equal to the application domain and is defined in the lwsso element of the configuration.
LW-SSO fails to transfer user information	Two applications have different initString parameters in the crypto element of the configuration.	Use the same initString in both applications

Problem Description	Cause of Problem	Solution
LW-SSO fails to transfer user information in a multi domain environment	A domain is not defined properly in the lwsso element in the configuration of one of the applications.	A domain must be equal to the application domain and be defined in the lwsso element of the application's configuration.
	A domain is not defined in the protectedDomains list in the configuration of one of the applications.	Define domains in the protectedDomains list in all of the applications' configurations.
	Browser is IE 6.0 and domains are not added to the "Intranet"/"Trusted" zone.	Add all domains to the "Intranet"/"Trusted" zone
	Two applications have different initString parameters in the crypto element of the configuration.	Use the same initString in both applications

Part II

Setup and Maintenance

8

Downloads and Licenses

This chapter provides details on downloading components to HP Business Availability Center, and updating license information.

This chapter includes:

Concepts

Tasks

Reference

Downloads Overview

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.

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.

License Management Overview

Note to HP Software-as-a-Service 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.

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 “Update Your License Key or Maintenance Number” on page 157.

Update Your License Key or Maintenance Number

Updating your license key or maintenance number is done differently in Solaris that it is in Windows. For details on updating your license key in Windows, see "License Management Page" on page 160.

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 **<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
```

Downloads and Licenses User Interface

This section describes:

Download Components Page

Description	Lists the HP Business Availability Center components available for download, including tools for monitoring your enterprise and recording business processes. **To Access:** Select **Admin** > **Platform** > **Setup and Maintenance** > **Downloads.**
Important Information	➤ 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. ➤ You can filter the downloadable components either by category or by system. ➤ To download components on the Download Components page, perform the following steps: ➤ Click the component you want to download. ➤ Save the component's setup file to your computer. ➤ Run the component's setup file to install the component.
Useful Links	"Downloads Overview" on page 155

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Category	The downloadable component's category. Available categories are: ➤ **Business Process Insight.** Downloadable files that enable you to install and run Business Process Insight components on HP Business Availability Center. ➤ **Business Process Monitor.** Downloadable files that enable you to install and run Business Process Monitor components on HP Business Availability Center. ➤ **Dashboard Ticker.** The HP Dashboard Ticker downloadable file that enables you to install and run the Dashboard Ticker component on HP Business Availability Center. ➤ **Diagnostics.** Downloadable files that enable you to install and run Diagnostics components on HP Business Availability Center. ➤ **Discovery Probe.** The Discovery Probe downloadable file that enables you to install and run the Discovery Probe component on HP Business Availability Center. ➤ **Real User Monitor.** Downloadable files that enable you to install and run Real User Monitor components on HP Business Availability Center. ➤ **SiteScope.** The SiteScope downloadable file that enables you to install and run SiteScope component on HP Business Availability Center. **Note:** Ensure that you have selected the file that corresponds to the Operating System you are working with. ➤ **TransactionVision.** Downloadable files that enable you to install and run TransactionVision components on HP Business Availability Center. ➤ **TransactionVision or Diagnostics.** Downloadable files that enable you to install and run the HP Diagnostics/TransactionVision Agent for Java file on HP Business Availability Center. **Note:** Ensure that you have selected the file that corresponds to the Operating System you are working with.
Description	An explanation of the specific downloadable file.

GUI Element (A-Z)	Description
Document	A link to the PDF describing the component. **Note:** Not all components have a corresponding PDF document available.
File Name	The name of the specific file available for download.
System	The operating system on which the HP Business Availability Center components are to run.

License Management Page

Description	Displays information on general license properties, Business Process Monitor and Script Assignment license and general information, and the license status of various HP Business Availability Center applications. Enables you to update your license key or maintenance number, as necessary. **To Access:** Select **Admin** > **Platform** > **Setup and Maintenance** > **License Management.**
Important Information	The initial license key and maintenance number are installed during the installation process. Do not use Platform Administration to install them. HP Business Availability Center posts a license expiration reminder on the login page of the Web site seven days before license expiration. To review the status of your maintenance number and license key, select **Help** > **About HP Business Availability Center.**
Useful Links	"License Management Overview" on page 156

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
New License Key	Click to update your license key.
New Maintenance Number	Click to update your maintenance number.

General License Properties Pane

Description	Displays information on general license properties in HP Business Availability Center. The General License Properties pane provides the following information: ➤ License Key ➤ License Host ID ➤ Maintenance Number ➤ License Type ➤ Expiration Date **To Access:** Select **Admin** > **Platform** > **Setup and Maintenance** > **License Management**
Useful Links	"License Management Overview" on page 156

Business Process Monitor Pane

Description	Displays license and general information on the Business Process Monitor data collector(s) installed in HP Business Availability Center. **To Access:** Select **Admin** > **Platform** > **Setup and Maintenance** > **License Management**
Important Information	The Business Process Monitor pane provides the following information: ➤ **Allowed transactions.** The maximum number of transactions allowed to run simultaneously under the current license key. ➤ **Running transactions.** The number of transactions currently running in all profiles. ➤ **Total transactions.** The total number of transactions currently in the database.
Useful Links	"License Management Overview" on page 156

Scripts Assignments Pane

Description	Displays license and general information on the scripts assignments in HP Business Availability Center. **To Access:** Select **Admin** > **Platform** > **Setup and Maintenance** > **License Management**
Important Information	The Scripts Assignments pane provides the following information: ➤ **Allowed scripts assignments.** The maximum number of scripts allowed to run simultaneously under the current license key. ➤ **Running scripts assignments.** The number of scripts assignments currently running in all profiles. ➤ **Total scripts assignments.** The total number of transactions currently in the database.
Useful Links	"License Management Overview" on page 156

Applications Pane

Description	Displays the validity of licenses for applications in HP Business Availability Center. **To Access:** Select **Admin** > **Platform** > **Setup and Maintenance** > **License Management**
Important Information	The Applications Pane displays the validity of the licenses for the following areas of HP Business Availability Center: ➤ Dashboard ➤ Service Level Management ➤ End User Management ➤ Real User Monitor ➤ System Availability Management ➤ Business Availability Center for Siebel Applications ➤ Diagnostics ➤ Business Availability Center for SAP Applications ➤ Automatic Discovery ➤ Business Availability Center for SOA ➤ Problem Isolation ➤ Application Performance Lifecycle
Useful Links	"License Management Overview" on page 156

9

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.

This chapter includes:

Concepts

Tasks

Reference

Database Management - Overview

Note to HP Software-as-a-Service 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 different types of profiles (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 Microsoft 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 174.
- **Oracle Server.** This database runs on Windows or Solaris operating systems – for details, see page 174.

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 Microsoft SQL Server or Oracle Server for your organization's particular environment, follow the instructions in "Introduction to Preparing the Database Environment" 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.

Partitioning and Purging Historical Data from Profile Databases

Note to HP Software-as-a-Service customers: HP Operations administers these pages and the interface is hidden from your view.

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

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

When enabled together, 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.

Once enabled, the Partition and Purging Managers partition and later remove data according to the time period listed for the database table. After the retention time period set for each table has completed, the Purging Manager removes data that has been aggregated.

The size of each partition is determined by the EPM (events per minute) that you configured. Optionally, you may want to adjust the EPM value, if necessary:

- If data partitions are too large (accumulating much more than 1 million rows), raise the EPM value to create new partitions more frequently.
- If data partitions are too small (accumulating much less than 1 million rows), lower the EPM value to create new partitions less frequently.

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.

The Partition and Purging Manager runs every hour to check if a new data partition needs to be created. 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.

For guidelines and tips on using the Partition and Purging Manager, see "Guidelines and Tips for Using the Partition and Purging Manager" on page 171.

The Purging Manager page is divided into the following tabs:

- **Template and Multiple Databases.** Used to modify the template configurations, as well as database configurations in multiple databases. Any databases added at a later time adopt the template configurations.

  Once you have made changes, the settings displayed in the Template & Multiple Databases tab remain the template settings, even if you did not make changes to the template and have manually changed settings for specific databases. Once those manual changes are applied, the settings displayed revert to the template settings. To see the settings you changed for specific databases, navigate to the **Database Specific** tab and select the appropriate database.

- **Database Specific.** Displays the configurations for the specified database.

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

Partitioning Types

The HP Business Availability Center Purging Manager supports the following partitioning types:

- **Native Partitioning.** Used by databases and user schema that enable partitioning and purging separately. In Native Partitioning databases, partitioning and purging are automatically enabled. These databases run based on the **Enterprise** template on the Template and Multiple Databases tab in the Purging Manager.

➤ **View Partitioning.** Used by databases and user schema that enable partitioning and purging together. HP strongly recommends that you enable the Partition and Purging Manager. These databases run based on the **Standard** template on the Template and Multiple Databases tab in the Partition and Purging Manager.

For details on partitioning and purging capabilities according to database type, see "Partitioning by Database Type" on page 170.

Note: If there are no profile databases configured, the purging manager displays the template settings for the system (Enterprise or Standard), based on the template configured on the management database.

Partitioning by Database Type

Depending on the type of partitioning that is enabled, the Partition and Purging Manager can be used with profile databases located on specific database servers, as follows:

Database Server Type	View Partitioning	Native Partitioning
Oracle	Any Oracle Server version supported by HP Business Availability Center	Any Oracle Server version supported by HP Business Availability Center, except standard editions of each version
MS SQL	➤ MS SQL Server 2000 Standard Edition ➤ Microsoft SQL Server 2000 Enterprise editions (Microsoft SQL Server 7.0 and MSDE are not supported)	Microsoft SQL Server 2005 Enterprise Edition

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 Template and Multiple Databases 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 Template and Multiple Databases tab, data is kept in the tables of that new profile database for the time periods now listed under Template and Multiple Databases for all tables.

Removing Unwanted Data from the Profile Database

Note to HP Software-as-a-Service customers: This section is not relevant to HP Software-as-a-Service 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. This filters out unwanted data and enables HP Business Availability Center to display only the most relevant data for the specified time period.

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 the marked data is not displayed. The Data Marking utility also enables you to re-aggregate a defined set of data without marking it as unavailable. For details, see “Enable the Re-aggregation-Only Option” on page 178.

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.

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.

Configure a Profile Database on a Microsoft SQL Server

This task describes how to configure one or more Profile databases on a Microsoft SQL Server.

This task includes the following steps:

- "Prerequisites" on page 173
- "Add a Database" on page 174

1 Prerequisites

Before you begin, make sure that you have the following connection parameters to the database server:

a **Server name.** The name of the machine on which Microsoft SQL Server is installed.

b **Database user name and password.** The user name and password of a user with administrative rights on Microsoft SQL Server (if using SQL server authentication).

c **Server port.** The Microsoft 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.

2 Add a Database

a Access the Database Management page, located at **Admin** > **Platform** > **Setup and Maintenance** > **Manage Profile Databases**.

b Select **MS SQL** from the dropdown list, and click **Add**.

c Enter the parameters of your database on the **Profile Database Properties - MS SQL Server** page. For details on the Profile Database Properties - MS SQL Server page, see “Profile Database Properties - MS SQL Server Page” on page 181.

Configure a User Schema On an Oracle Server

This task describes how to configure one or more profile user schemas on your Oracle Server.

1 Prerequisites

Before you begin, make sure that:

a You have created a dedicated default tablespace for profile user schemas (and a dedicated temporary tablespace, if required).

b 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.

2 Gather connection parameters

Make sure that you have the following connection parameters to the database server:

a **Host name.** The name of the machine on which the Oracle Server is installed.

b **SID.** The Oracle instance name that uniquely identifies the instance of the Oracle database being used, if different from the default value, **orcl**.

c **Port.** The Oracle listener port, if different from the default value, **1521**.

d **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.

e **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**.

f **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**.

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

3 Add a User Schema

a Access the Database Management page, located at **Admin** > **Platform** > **Setup and Maintenance** > **Manage Profile Databases**.

b Select **Oracle** from the dropdown list, and click **Add**.

c Enter the parameters of your user schema on the **Profile Database Properties - MS SQL Server** page. For details on the Profile Database Properties - MS SQL Server page, see "Profile User Schema Properties - Oracle Server Page" on page 183.

Work with the Purging Manager

This task describes how to work with the Purging Manager.

1 Prerequisites

Ensure that you have at least one profile database configured in your HP Business Availability Center system. For details on configuring a profile database on a Microsoft SQL Server, see "Configure a Profile Database on a Microsoft SQL Server" on page 173.

For details on configuring a user schema on an Oracle Server, see "Configure a User Schema On an Oracle Server" on page 174.

2 Change the Database Template

To change settings for the database template, follow these steps:

a Access the Template and Multiple Databases tab on the Purging Manager page.

b Select the check box next to the setting you want to change. You can select multiple check boxes at once.

c Modify the specified setting accordingly in the **Keep Data for** and **Change to EPM** fields, and click **Apply**.

d Click the **Apply to** link and ensure that the appropriate template (**Enterprise** for Native Partitioning databases, or **Standard** for View Partitioning databases) is selected.

e Click **OK** to register your changes to the template.

Note: Once you have made changes, the settings displayed in the Template & Multiple Databases tab remain the template settings, even if you did not make changes to the template and have manually changed settings for specific databases. Once those manual changes are applied, the settings displayed revert to the template settings. To see the settings you changed for specific databases, navigate to the **Database-Specific** tab and select the appropriate database.

---

3 Change Settings for Multiple Databases

To change settings for multiple databases at once, follow these steps:

a Access the Template and Multiple Databases tab on the Purging Manager page.

b Select the check box next to the setting you want to change. You can select multiple check boxes at once.

c Modify the specified setting accordingly in the **Keep Data for** and **Change to EPM** fields, and click **Apply**.

d Click the **Apply to** link and ensure that the appropriate databases are selected. Clear the check box next to the template if you do not want your changes to apply to the template.

e Click **OK** to register your changes to the selected databases.

Note: Changes made to the databases are displayed only on the Database Specific tab, after the relevant database has been selected in the **Select a profile database** dropdown.

---

4 Change Settings for Individual Databases

To change settings for individual databases, follow these steps:

a Access the Database Specific tab on the Purging Manager page.

b Select the checkbox next to the settings you want to change.

c Select the profile database that you want your changes to apply to in the **Select a profile database** field.

d Modify the specified setting accordingly in the **Keep Data for** and **Change to EPM** fields, and click **Apply**.

Enable 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 re-aggregate 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 re-aggregation process when clicking the **Start** button.

To run data re-aggregation only:

1. Define the set of data you want to re-aggregate, as described in "Removing Unwanted Data from the Profile Database" on page 172.
2. Click the **Advanced** button. The Advanced window opens.
3. Select the **Run re-aggregation only** check box.
4. Select the categories of data for the re-aggregation and click **OK** to confirm selection.
5. Click **Start**.

Determine the Events Per Minute (EPM) for Data Arriving in HP Business Availability Center

You can determine the amount of data per minute that is arriving in HP Business Availability Center. You enter this number in the **Change to EPM** box at the bottom of the **Enable/Disable Purging Manager** page.

To determine the Events Per Minute for the selected data type:

1 Open the file located at:

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

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

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

3 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. If you have more than one Gateway Server, you must total the values obtained from each server.

Database Administration User Interface

This section describes:

Database Management Page

Description	Enables you to maintain and administer the databases HP Business Availability Center uses to store profile and monitoring data. **To Access:** Select **Admin** > **Platform** > **Setup and Maintenance** > **Manage Profile Databases.**
Important Information	You can create a database on the following servers: ➤ **Microsoft SQL server.** For details, see "Profile Database Properties - MS SQL Server Page" on page 181. ➤ **Oracle server.** For details, see "Profile User Schema Properties - Oracle Server Page" on page 183. **Note:** A database on Oracle server is referred to as a **user schema**.
Useful Links	"Audit Log - Overview" on page 331

The Database Management page includes the following elements (listed alphabetically):

GUI Element	Description
	Click to disconnect the database or user schema. **Note:** You cannot delete the default profile database or a database which is in use.
Add	Click to add a Microsoft SQL Server database or Oracle Server user schema, as specified in the dropdown database list.
Database Name	The name of the database.
Database Type	The type of database, either Microsoft SQL or Oracle.
Server Name	The name of the server that the database is running on.

Profile Database Properties - MS SQL Server Page

Description	Enables you to configure a new or existing profile database on Microsoft SQL Server. **To Access:** Select **Admin** > **Platform** > **Setup and Maintenance** > **Manage Profile Databases**, select **Microsoft SQL** from the dropdown database list and click **Add**.
Important Information	➤ It is recommended that you configure Microsoft SQL Server databases manually, and then connect to them in the Database Management page. For details on manually configuring Microsoft SQL Server databases, see "Overview of Microsoft SQL Server Deployment" in the *HP Business Availability Center Database Guide* PDF. ➤ Database creation can take several minutes.
Included in Tasks	"Configure a Profile Database on a Microsoft SQL Server" on page 173
Useful Links	"Database Management - Overview" on page 166

The Profile Database Properties page includes the following elements (listed alphabetically):

GUI Element	Description
Create database and/or tables	Select or clear 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.
Database name	➤ If you are configuring a new database, type a descriptive name for the database. ➤ If you are connecting to a database that was previously created, type the name of the existing database.

GUI Element	Description
Disconnect	Click to disconnect the database from HP Business Availability Center. **Note:** This button only appears after you have clicked the Disconnect Database button  on the Database Management page.
Make this my default profile database (required for custom data types)	Select or clear as required. **Note:** ➤ 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 363. ➤ If a default profile database already exists, selecting this check box overwrites the existing database.
Password	➤ If you are using Windows authentication, enter the password that runs the HP Business Availability Center service on the current machine. ➤ If you are using SQL server authentication, enter the password of a user with administrative rights on Microsoft SQL Server.
Port	Enter the port number if the Microsoft SQL Server's TCP/IP port is configured to work on a port different from the default (1433).
Server name	Enter the name of the machine on which the Microsoft SQL Server is installed.
SQL server authentication	Select if the Microsoft SQL Server is using SQL server authentication.

GUI Element	Description
User name	➤ If you are using Windows authentication, enter the user name that runs the HP Business Availability Center service on the current machine. ➤ If you are using SQL server authentication, enter the user name of a user with administrative rights on Microsoft SQL Server.
Windows authentication	Select if the Microsoft SQL Server is using Windows authentication.

Profile User Schema Properties - Oracle Server Page

Description	Enables you to configure one or more profile user schemas on your Oracle server. **To Access:** Select **Admin** > **Platform** > **Setup and Maintenance** > **Manage Profile Databases**, select **Oracle** from the dropdown database list and click **Add**.
Important Information	➤ 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. ➤ 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.
Included in Tasks	"Configure a User Schema On an Oracle Server" on page 174
Useful Links	"Database Management - Overview" on page 166

The Profile User Schema Properties page includes the following elements (listed alphabetically):

GUI Element	Description
Create database and/or tables	Select or clear 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 this check box disables the database administrator connection parameter and tablespace fields on the page, and instructs the platform to ignore the information in these fields when connecting to the Oracle Server machine.
Database administrator password	Enter the password of a user with administrative permissions on Oracle Server. **Note:** This field is only enabled if you selected the **Create database and/or tables** check box.
Database administrator user name	Enter the user name and password of a user with administrative permissions on Oracle Server. **Note:** This field is only enabled if you selected the **Create database and/or tables** check box.
Default tablespace	Enter the name of the default tablespace designated for use with profile user schemas. **Default Value:** users
Disconnect	Click to disconnect the user schema from HP Business Availability Center. **Note:** This button only appears after you have clicked the **Disconnect Database** button  on the Database Management page.
Host name	Enter the name of the machine on which the Oracle Server is installed.

GUI Element	Description
Make this my default profile database (required for custom data types)	Select or clear as required. **Note:** ➤ 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 363. ➤ If a default profile database already exists, selecting this check box overwrites the existing database.
Port	Enter the required Oracle listener port, or accept the default value.
Retype password	Retype the user schema password.
SID	Enter the required Oracle instance name, or accept the default value.
Temporary tablespace	Enter the name of the temporary tablespace designated for use with profile user schemas. **Default Value:** temp
User schema name	➤ If you are configuring a new user schema, enter a descriptive name for the user schema. ➤ If you are connecting to a user schema that was previously created, enter the name of the existing user schema.
User schema password	➤ If you are configuring a new user schema, enter a password that enables access to the user schema. ➤ If you are connecting to a user schema that was previously created, enter the password of the existing user schema. **Note:** You must specify a unique user schema name for each user schema you create for HP Business Availability Center on Oracle Server.

Purging Manager Page

Description	From the Purging Manager page, you can enable or disable the Partition and Purging Manager to instruct HP Business Availability Center to begin or stop the process of partitioning the data. **To Access:** ➤ For servers with view partitioning: Select **Admin** > **Platform** > **Setup and Maintenance** > **Data Partitioning and Purging**.
Important Information	➤ The purging manager consists of the following tabs: ➤ **Template and Multiple Databases.** Select to change the template settings, or to change settings for more than one database. ➤ **Database Specific.** Select to change settings for one database. ➤ When working with an Oracle standard edition 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.
Useful Links	“Partitioning and Purging Historical Data from Profile Databases” on page 168

The Purging Manager page includes the following elements (listed alphabetically):

GUI Element	Description
Apply to	Click to select the databases and template you want the configurations on the Template and Multiple Databases tab to apply to. You can clear all databases to make changes only to the selected template.
Change to EPM	The amount of data per minute to arrive in HP Business Availability Center. **Note:** Leave this field empty to retain the existing EPM value. For details on determining this value, see "Determine the Events Per Minute (EPM) for Data Arriving in HP Business Availability Center" on page 179.
Database Specific	Select this tab to change the time range for purging data in a table per individual profile database.
Description	Describes the corresponding database table.
Disable	Click to disable the Partition and Purging Manager. **Note:** This button is displayed only when a database that supports **View** partitioning has been configured.
Enable	Click to enable the Partition and Purging Manager. **Note:** This button is displayed only when a database that supports **View** partitioning has been configured.
Epm Value	The amount of data per minute that is arriving in HP Business Availability Center. For details on determining this value, see "Determine the Events Per Minute (EPM) for Data Arriving in HP Business Availability Center" on page 179.

GUI Element	Description
Template and Multiple Databases	Select this tab to: ➤ Change the partitioning and purging parameters for multiple profile databases. ➤ Change the database template, for parameters to be adopted by new databases added in the future. **Note:** Once you have made changes, the settings displayed in the Template & Multiple Databases tab remain the template settings, even if you did not make changes to the template and have manually changed settings for specific databases. Once those manual changes are applied, the settings displayed revert to the template settings. To see the settings you changed for specific databases, navigate to the **Database-Specific** tab and select the appropriate database.
Keep Data for	The time range for keeping data in the database tables whose check box is selected. This element appears in two places: ➤ **Dropdown list.** On the bottom of the page, set the time range for how long you want data kept in the selected database tables. ➤ **Column heading.** Displays the time range for keeping data in each database table. This value is configured in the **Keep Data for** dropdown list on the bottom of the page. **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.

GUI Element	Description
Name of Table in Database	The name of the table in the database. Database tables are listed by the data collector from which the data was gathered. The following data types are available: ➤ Business Logic Engine ➤ Business Process Monitor ➤ Diagnostics ➤ Real User Monitor ➤ SOA (Service Oriented Architecture) ➤ Service Level Management ➤ SiteScope ➤ UDX (custom data) ➤ WebTrace
Select a profile database	Select a profile database for which you want to modify time range configurations for purging data. **Note:** This field is only visible on the Database Specific tab.

Data Marking Utility Page

Description	Enables you to select sets of data for removal by profile or by location for Business Process Monitordata, and by SiteScope target machine for SiteScope data. **To Access:** 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. Enter the user name and password of an HP Business Availability Center user with superuser privileges.
Important Information	➤ You must have superuser privileges to access the Data Marking Utility page. ➤ 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. ➤ Do not run more than one instance of the Data Marking utility at one time as this can affect the re-aggregation 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 re-aggregation process.
Useful Links	"Removing Unwanted Data from the Profile Database" on page 172 "Data Marking Utility Limitations" on page 194

The Data Marking Utility page includes the following elements (listed alphabetically):

GUI Element	Description
Duration	Select the period of time, starting from the specified start time, for the utility to mark data as unavailable. **Note:** You can set a maximum duration of up to 6 hours and 59 minutes for each data marking run. For details on customizing this value, see
Get Info	Click before running the Data Marking Utility to view the number of data rows to be marked.
Locations	List of locations you can mark as obsolete.
Mark data as obsolete	Click to mark the filtered criteria (i.e. - Profiles, Transactions, Locations, or SiteScope Targets) as obsolete.
Mark data as valid (undo mark as obsolete)	Click to make selected data available again after having been marked as obsolete.
Profiles	List of profiles you can mark as obsolete.
Progress	Displays the progress of the data marking process and re-aggregation process.
SiteScope Targets	List of SiteScope target machines (i.e. - machines being monitored by SiteScope) you can mark as obsolete. **Note:** This field is only visible in the SiteScope view (i.e. - if you chose **SiteScope View** in the **View by** dropdown).
Start	Click to activate the Data Marking Utility and mark data as obsolete.
Start Time	Select a starting data and time for data to be marked as unavailable.

GUI Element	Description
Transactions	List of transactions you can mark as obsolete. **Note:** This field is only visible in the Profile view (i.e. - if you chose **Profiles** in the **View by** dropdown).
View by	Select the type of view to be visible in the Data Marking Utility.

Data Marking Information Window

Description	Displays the data to be marked as obsolete by the Data Marking Utility. **To access:** Click the **Get Info** button on the Data Marking Utility page.
Important Information	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 187 in Service Level Management.
Useful Links	"Removing Unwanted Data from the Profile Database" on page 172 "Data Marking Utility Limitations" on page 194

The Data Marking Information Window includes the following elements (listed alphabetically):

GUI Element	Description
Number of Rows to Update	The number of data rows to be marked as obsolete.

GUI Element	Description
Profile Name	The name of the profile to be marked as obsolete.
Total Rows to Update	The total number of rows available to be marked as obsolete. This number can differ from the value of the Number of Rows to Update field. For details, see "Data Marking Utility Limitations" on page 194.

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.

Troubleshooting and Limitations

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 re-aggregate 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

Following are limitations associated with the Data Marking utility:

- 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.

10

Infrastructure Settings

Note to HP Software-as-a-Service 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.

This chapter includes:

Concepts

Tasks

Reference

Infrastructure Settings Manager - Overview

HP Business Availability Center enables you to define the value of many settings that determine how HP Business Availability Center and its applications run.

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 HP Software Support or your HP Services representative.

In the Infrastructure Settings Manager, you can select different contexts from which to view and edit 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.

  Descriptions of the individual settings appear in the **Description** column of the table on the Infrastructure Settings page.

Modify the Ping Time Interval

Note: This Infrastructure Settings task is performed outside the Infrastructure Settings Manager.

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.

Modify the Location and Expiration of Temporary Image Files

Note: This Infrastructure Settings task is performed outside the Infrastructure Settings Manager.

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 "Modify the Directory in Which Temporary Image Files Are Stored" on page 201.

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

  For details, see "Modify the Length of Time that HP Business Availability Center Keeps Temporary Image Files" on page 206.

- **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 "Specify the Directories from Which Temporary Image Files Are Removed" on page 210.

Modify 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 "Access Temp Directory with Multiple Gateway Server Machines" on page 202.

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 HP Software 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.

Access 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.

Modify 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 HP Software 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.

Specify 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.

Infrastructure Settings User Interface

This section describes:

➤ Infrastructure Settings Manager Page on page 211

Infrastructure Settings Manager Page

Description	Enables you to define the value of many settings that determine how HP Business Availability Center and its applications run. **To Access:** Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings.**
Important Information	➤ 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 HP Software Support or your HP Services representative. ➤ There are some infrastructure settings which are configured directly in files. For details, see the following: ➤ "Modify the Ping Time Interval" on page 199 ➤ "Modify the Location and Expiration of Temporary Image Files" on page 200
Useful Links	"Infrastructure Settings Manager - Overview" on page 198

The Infrastructure Settings Manager page includes the following elements (listed alphabetically):

GUI Element	Description
All	Select to view all the settings for both Applications and Foundations.
Applications	Select to edit one of the HP Business Availability Center applications.
Description	Describes the specific infrastructure setting. **Note:** This field is visible on both the Infrastructure Settings Manager page, and the Edit Setting dialog box after clicking the **Edit** button  next to the relevant setting.
Foundations	Select to edit one of the HP Business Availability Center foundations.

GUI Element	Description
Name	The name of the setting. **Note:** This field is visible on both the Infrastructure Settings Manager page, and the Edit Setting dialog box after clicking the **Edit** button  next to the relevant setting.
Restore Default	Click to restore the default value of the setting. **Note:** This button is visible on the Edit Setting dialog box after clicking the **Edit** button  next to the relevant setting.
Value	The current value of the given setting. **Note:** This field is visible on both the Infrastructure Settings Manager page, and the Edit Setting dialog box after clicking the **Edit** button  next to the relevant setting.

11

System Health

This chapter includes the main concepts of System Health.

This chapter includes:

Concepts

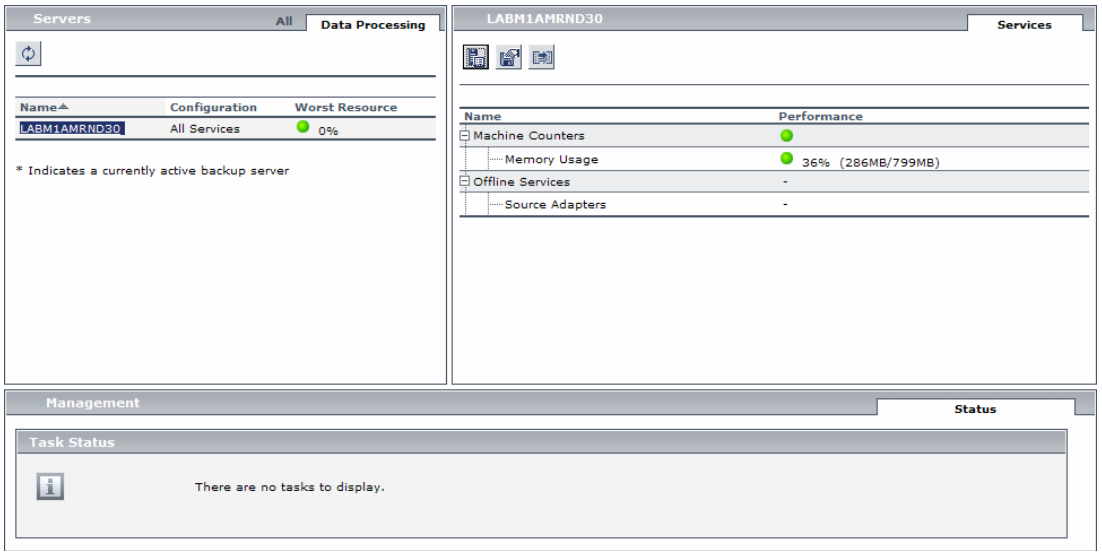
Tasks

Reference

System Health - Overview

System Health uses the SiteScope monitoring system to enable you to monitor the servers, databases, and data collectors running as part of your HP Business Availability Center system.

Note: If you do not deploy the new System Health interface, your system defaults to the Legacy System Health application. To view the Legacy System Health interface, see below. For details on Legacy System Health, see "Legacy System Health" on page 303.



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 format (displaying current status) and Quick Report format (displaying status of past 24 hours).

System Health Setup Wizard - Overview

You configure the System Health Setup Wizard to create remote connections to the servers which System Health monitors. If remote connections are not created, many of the monitors do not work.

Important: It is not possible for another user to access the System Health interface while you are configuring the System Health Setup Wizard.

For details on configuring the System Health Setup Wizard, see "Ensure the Health of Your HP Business Availability Center System" on page 228.

For details on the pages and elements contained in the System Health Setup Wizard, see "System Health Setup Wizard" on page 235.

Accessing 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 **Soft Sync** button on the System Health Dashboard Toolbar or the Inventory Tab Toolbar.

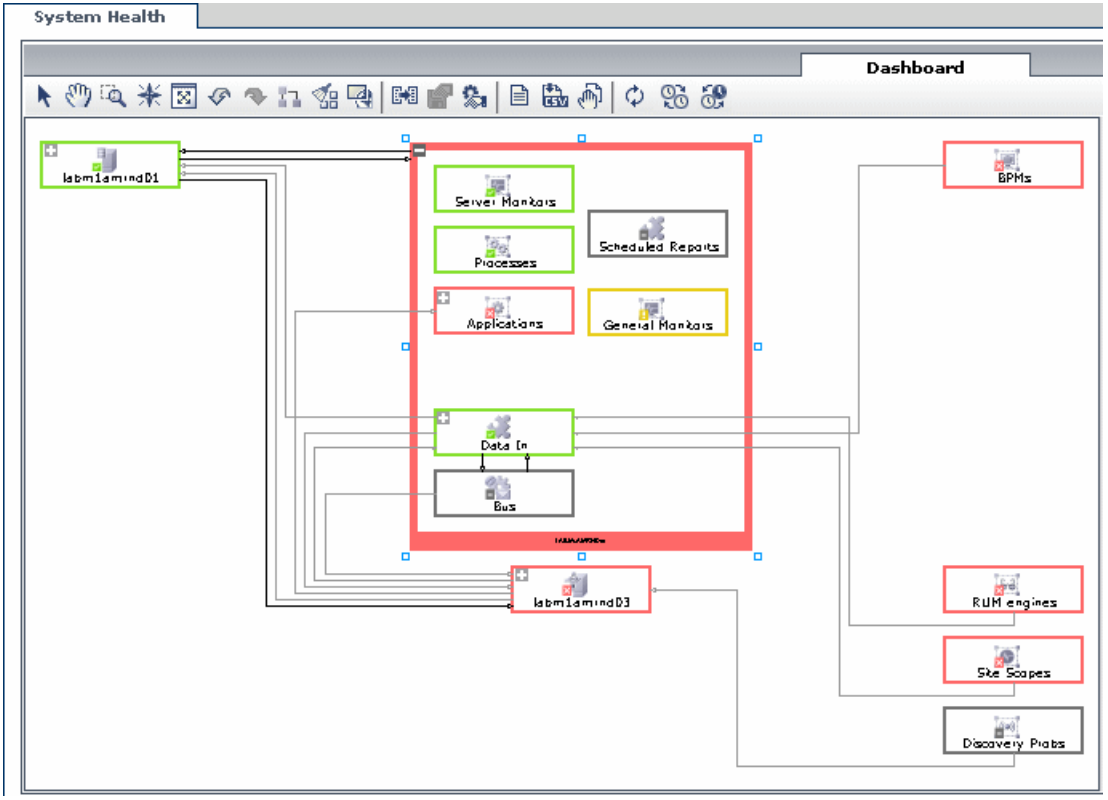
➤ Clicking the **Full Model Synchronization** button on the System Health Dashboard Toolbar or the Inventory Tab Toolbar.

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.

System Health Displays

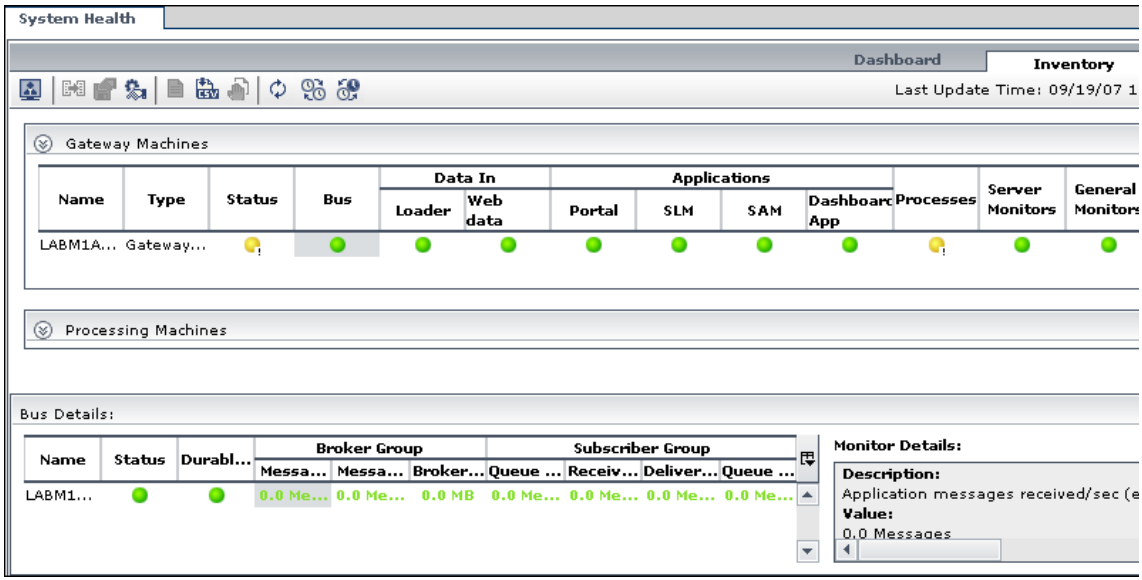
You can view the status of the HP Business Availability Center components in the following formats:

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



➤ **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.



For a description of the colored icons appearing on the Dashboard Tab and Inventory Tab, see "Monitor Status and Description" on page 300.

Understanding Service Reassignment

You may want to reassign services running on HP Business Availability Center servers, if a certain Data Processing Server machine is not functioning properly or requires downtime for servicing. Additionally, you can also preconfigure a specific Data Processing Server to automatically fail over to a specific backup machine, to ensure that your data is not lost in the event of system downtime.

Note: Service Reassignment can be performed only by an administrator.

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, at which point the system is in downtime.

For details on reassigning services, see “Service Manager Dialog Box” on page 256.

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, at which point the system is in downtime.

For details on reassigning services, see “Service Manager Dialog Box” on page 256.

Flow Table

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.

	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

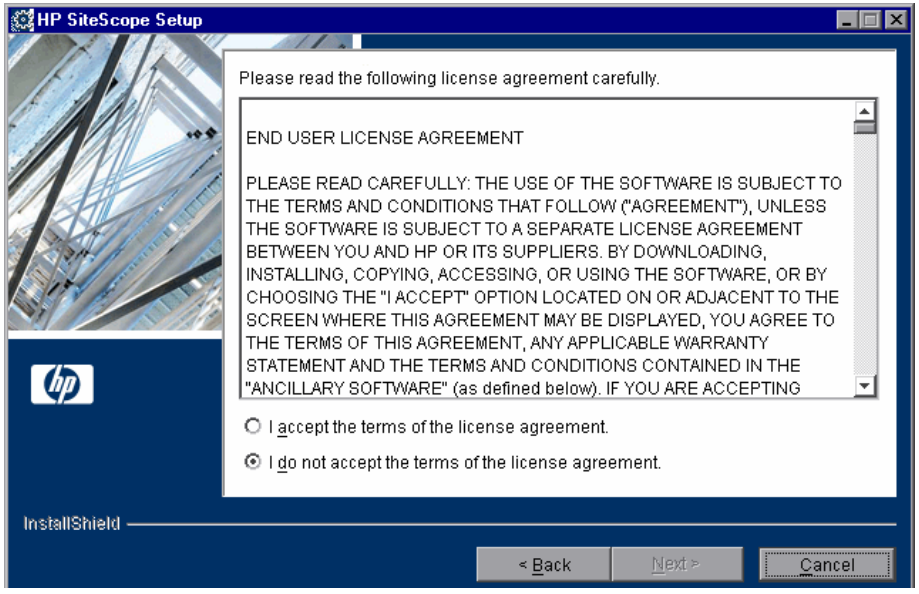
You deploy System Health either on a standalone machine with access to HP Business Availability Center (recommended so that System Health continues to run if HP Business Availability Center servers are down) or on any HP Business Availability Center Gateway Server (should only be done if a standalone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

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.

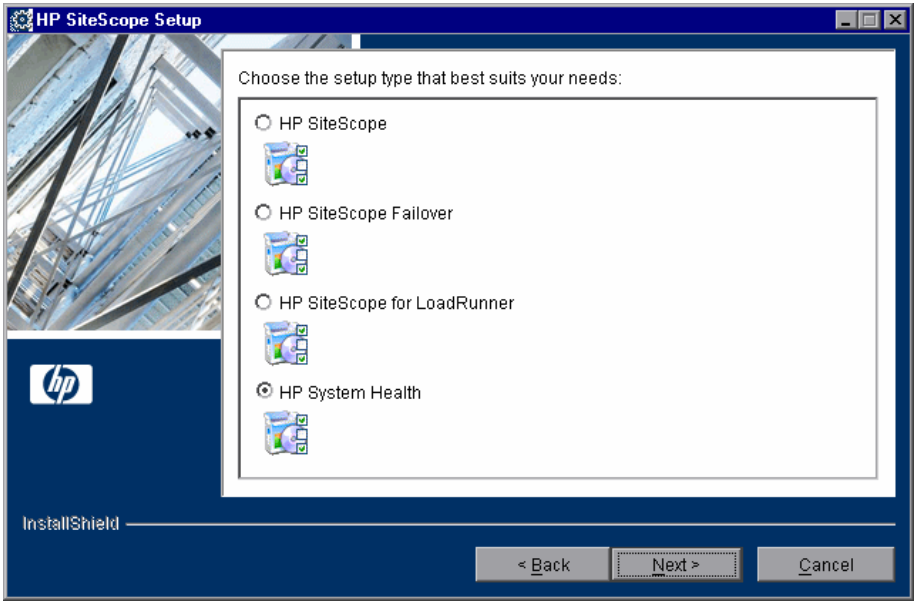
To deploy System Health:

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**.

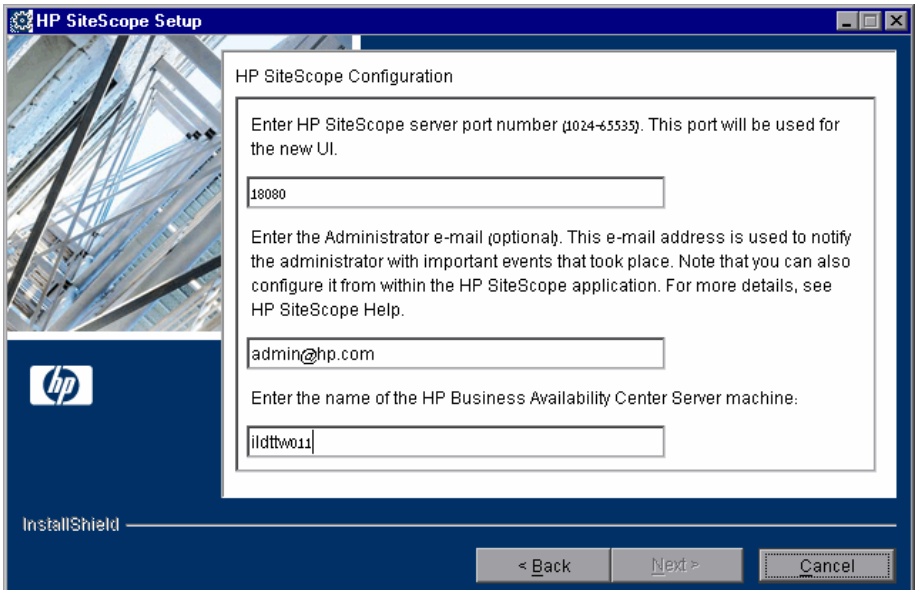


4 Enter a directory to install SiteScope on, or accept the default **C:\SiteScope**, and click **Next**.

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 on your HP Business Availability Center machine.

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 can access System Health:

- directly, via a Web browser using the syntax: **http://<server_name>.<domain_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.

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

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 "Log In and Out" on page 23.

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 login to 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. For details on the System Health username and password, see step 3 on page 226.
- 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. You can also 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.

1 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 235.

2 Monitor Performance of HP Business Availability Center Components

You can monitor the performance of the servers, databases, and data collectors running as part of 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 217.

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 251.

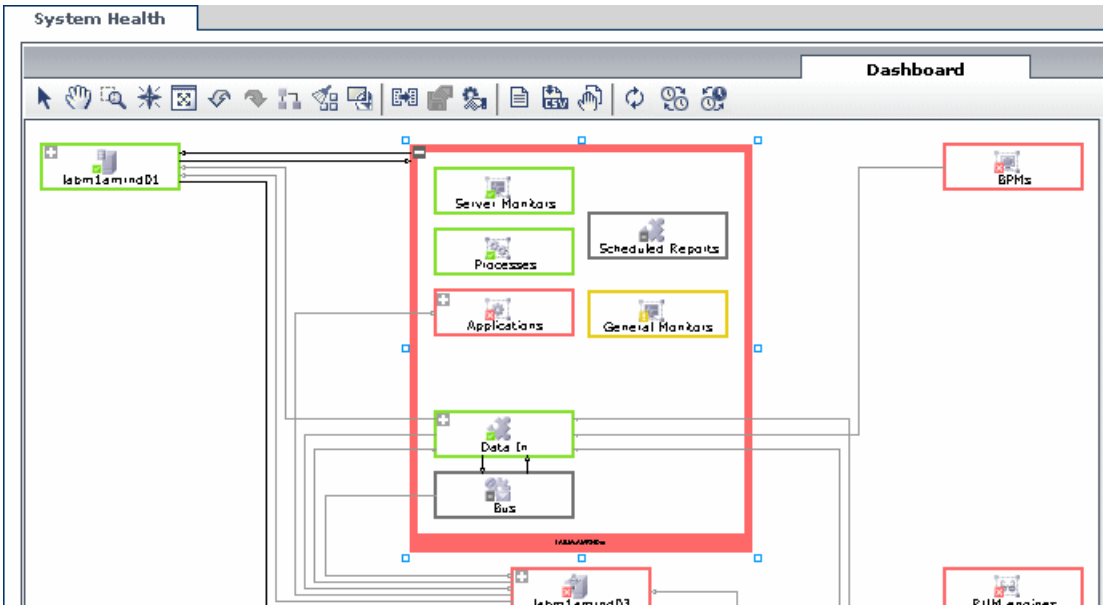
A component's status is indicated by both its outlined color and status icon color.

For details on the components' outlined colors, see "Map of HP Business Availability Center System and Components" on page 262.

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.

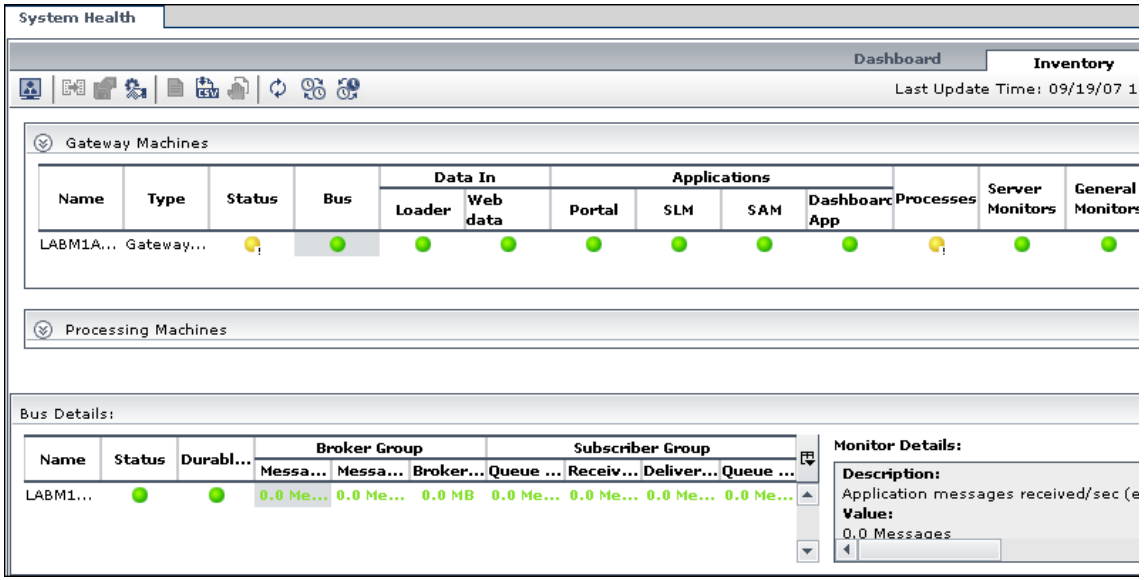


➤ **Inventory Tab**

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 "Monitor Status and Description" on page 300.

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



3 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 256.

Example

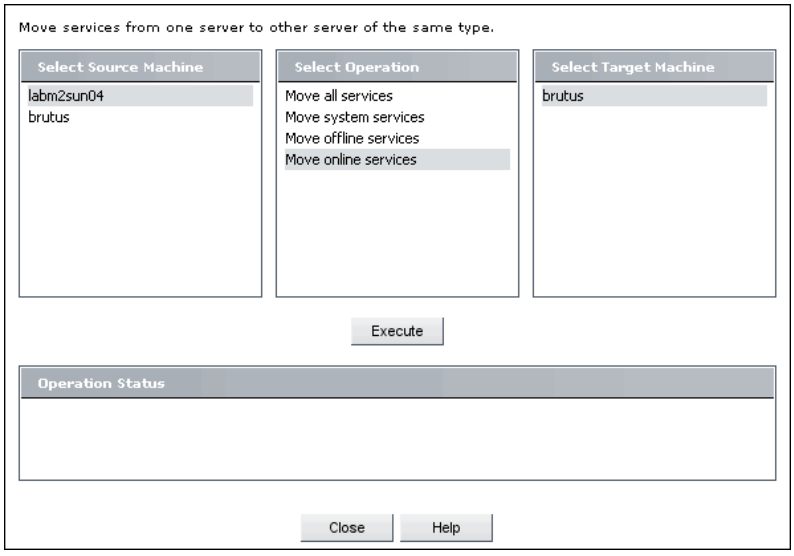
a On the Toolbar on either the System Health Dashboard or the Inventory Tab, click the **Service Manager button**.

b In the **Select Source Machine** window, select the machine that you want to move services from.

c In the **Select Operation** window, select the operation you want to perform.

d In the **Select Target Machine** window, select the machine you want to move services to.

e Click the **Execute** button. The **Operation Status** window indicates whether or not the operation request was sent successfully.



4 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 257.

Example

a On the Toolbar on either the System Health Dashboard or the Inventory Tab, click the **Backup Server Configuration** button.

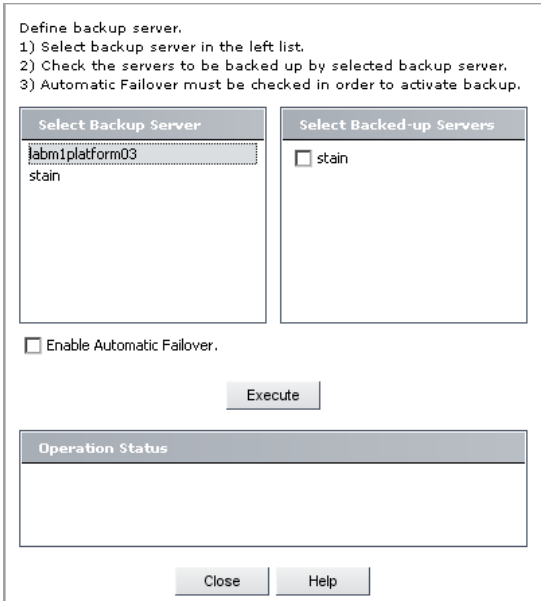
b In the left pane, select a backup server.

c In the right pane, select a server to be backed-up.

d Click the **Enable Automatic Failover** check box.

e Click **Execute** to register your backup server. The **Operation Status** window indicates whether or not the operation request was sent successfully.

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



5 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 258.

Example

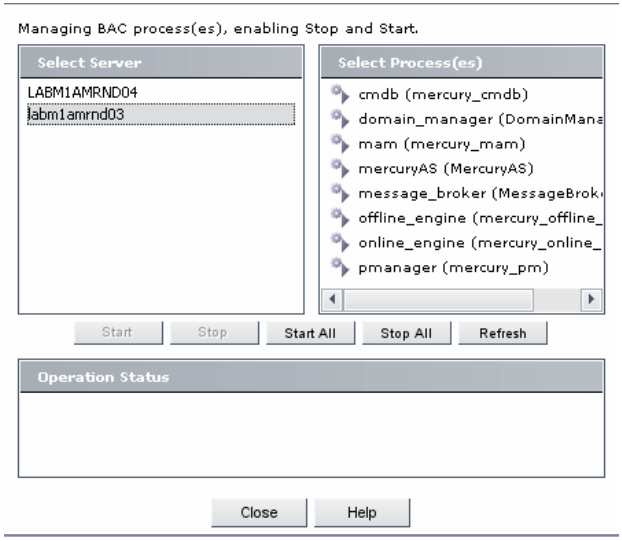
a On the Toolbar on either the System Health Dashboard or the Inventory Tab, click the **Process Manager** button .

b In the **Select Server** window, select the server you want to start or stop processes on.

c In the **Select Process(es)** window, select the process you want to start or stop. 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.

d 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** window indicates whether or not the operation request was sent successfully.



6 Display a Quick Report

Click the Quick Report button to display a Quick Report with information on monitors deployed on HP Business Availability Center components. For details, see "Quick Report Screen" on page 260.

Example

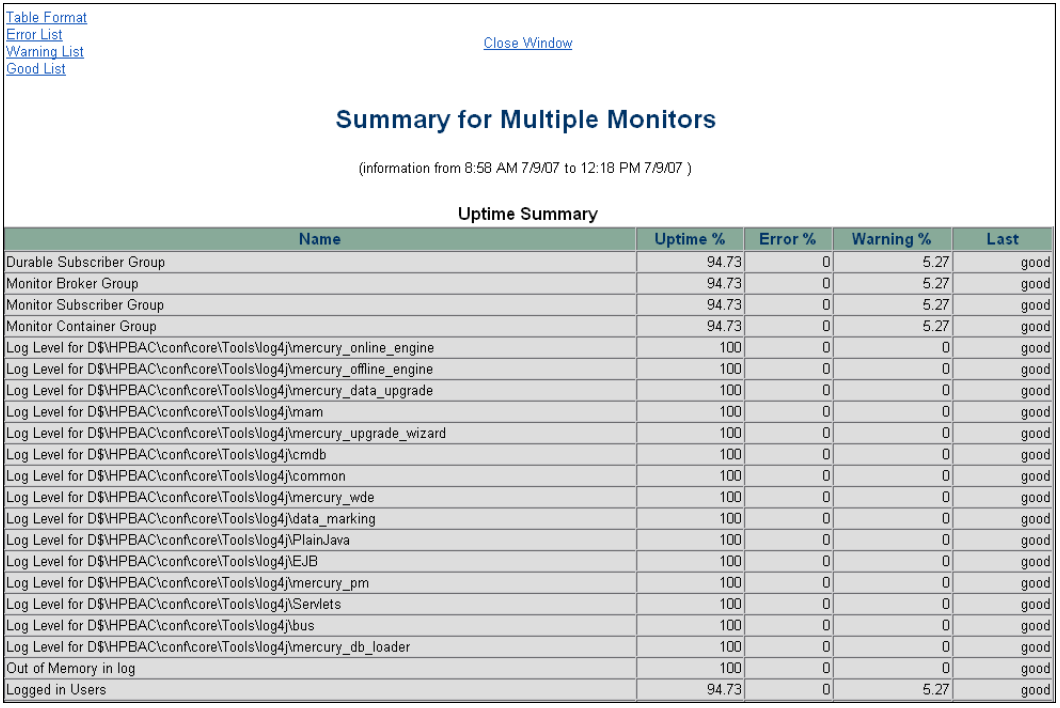


Table Format
Error List
Warning List
Good List

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 %	Warning %	Last
Durable Subscriber Group	94.73	0	5.27	good
Monitor Broker Group	94.73	0	5.27	good
Monitor Subscriber Group	94.73	0	5.27	good
Monitor Container Group	94.73	0	5.27	good
Log Level for D$\HPBAC\conf\core\Tools\log4j\mercury_online_engine	100	0	0	good
Log Level for D$\HPBAC\conf\core\Tools\log4j\mercury_offline_engine	100	0	0	good
Log Level for D$\HPBAC\conf\core\Tools\log4j\mercury_data_upgrade	100	0	0	good
Log Level for D$\HPBAC\conf\core\Tools\log4j\mam	100	0	0	good
Log Level for D$\HPBAC\conf\core\Tools\log4j\mercury_upgrade_wizard	100	0	0	good
Log Level for D$\HPBAC\conf\core\Tools\log4j\cmdb	100	0	0	good
Log Level for D$\HPBAC\conf\core\Tools\log4j\common	100	0	0	good
Log Level for D$\HPBAC\conf\core\Tools\log4j\mercury_wde	100	0	0	good
Log Level for D$\HPBAC\conf\core\Tools\log4j\data_marking	100	0	0	good
Log Level for D$\HPBAC\conf\core\Tools\log4j\PlainJava	100	0	0	good
Log Level for D$\HPBAC\conf\core\Tools\log4j\EJB	100	0	0	good
Log Level for D$\HPBAC\conf\core\Tools\log4j\mercury_pm	100	0	0	good
Log Level for D$\HPBAC\conf\core\Tools\log4j\Servlets	100	0	0	good
Log Level for D$\HPBAC\conf\core\Tools\log4j\bus	100	0	0	good
Log Level for D$\HPBAC\conf\core\Tools\log4j\mercury_db_loader	100	0	0	good
Out of Memory in log	100	0	0	good
Logged in Users	94.73	0	5.27	good

System Health User Interface

This section describes:

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:** Select **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. ➤ The user whose remote connection information you enter into the System Health Setup Wizard can perform only those actions for which they have permissions.
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 215, "Deploy and Access System Health" on page 222, "System Health Monitors" on page 271.
Wizard Map	The System Health Setup Wizard contains: Servers Remote Setup Page > Databases Remote Setup Page > Recipients Setup Dialog Box

Sample Status and Description

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

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 there was no attempt to establish remote connectivity between System Health and the component 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.

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 215
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 again to hide descriptions.
	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 connecting 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 215
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 again to hide descriptions.
	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:** Select **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 222 "System Health Setup Wizard" on page 235 "System Health Displays" on page 217

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 217

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 217

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 double click a monitor in the **Monitors** table to open the parent component in the System Health Dashboard. 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 268

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.

GUI Element	Description
	Click to reactivate the selected monitor's schedule.
	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. For details on the colored ball icons, see "Monitor Status and Description" on page 300.

General Table

Description	Contains information about the properties associated with 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.
Useful Links	"System Health Monitors" on page 271

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 217 "HP Business Availability Center Components" on page 268 "System Health Monitors" on page 271

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	"System Health Displays" on page 217 "HP Business Availability Center Components" on page 268

<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	"System Health Monitors" on page 271 "Monitors Table" on page 244

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 256 "Backup Server Setup Window" on page 257 "Process Manager Dialog Box" on page 258 "Quick Report Screen" on page 260

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.
	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 222. **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 219

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 230

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 232 "HP Business Availability Center Processes" on page 269

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.

GUI Element	Description
Operation Status	Displays the status of the operation performed.
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.

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 you 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 233 "Quick Report" 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.
<Warning List>	Lists the monitor runs that retrieved a **warning** status based on the thresholds configured for the monitor.

GUI Element	Description
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. **Note:** You may also see obsolete hosts that are no longer running HP Business Availability Center. To disable these obsolete hosts, browse to the URL **http://<Gateway Server machine name>.<domain_name>/topaz/systemConsole/displayBACHosts.do** and disable all obsolete hosts.
Useful Links	"System Health Displays" on page 217 "Monitor Status and Description" on page 300 "Monitors Table" on page 244

Component Status and Description

The following table displays a sample icon and a description of its outlined color and status, as it appears on the System Health Dashboard:

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.

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.

Status	Description
	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.

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. **Important:** You must select the cursor button  on the System Health Dashboard Toolbar to operate the expand button.
	Click to hide the subcomponents contained within the selected component. **Important:** You must select the cursor button  on the System Health Dashboard Toolbar to operate the expand button.
	Icon indicating a Database Server.
	Icon indicating a Database.
	Icon indicating a Gateway Server.
	Icon indicating a Processing Server.

GUI Element	Description
	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.
	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 251.

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 and Dependency Mapping Probes

- modeling
- Portal application (My BAC)
- Processes (for details, see "HP Business Availability Center Processes" on page 269)
- 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.

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 Probe.** Discovers the components of your IT infrastructure, creates CIs for them, and sends the data to the CMDB.
- **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.

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
Apache Web Server	Apache Web server process. Runs if the server is running on Apache. **Process name:** httpd
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
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

GUI Element	Description
IIS Web Server	IIS Web server process. Runs if the server is running on IIS. **Process name:** inetinfo
IPlanet Web Server	IPlanet Web server process. Runs if the server is running on IPlanet. **Process name:** webservd
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 be run only 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

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 272
- "Database Monitors" on page 273
- "HP Business Availability Center Server Monitors" on page 274
- "Gateway Server Monitors" on page 277
- "Processing Server Monitors" on page 285
- "Data Collectors" on page 296

Machine Hardware Monitors

The following group of monitors monitor the hardware and databases (where indicated) on which the Business Availability Center applications run:

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, if not otherwise indicated, on both:

General Monitors

Monitor Name	Description
Out of Memory in Log	Searches for unexpected behavior due to the server being 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 does not travel 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 258.

The two JVM monitors listed in the table below 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 the both the Java and non-Java processes. For details on the processes, see "HP Business Availability Center Processes" on page 269.

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 ➤**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 the 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. **Note:** This monitor is displayed as red for two hours after being connected.
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 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 the 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

Following are the data collectors that run as part of HP Business Availability Center:

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.

Monitor Status and Description

The following table displays a colored icon and a description of its status, as appears on both the Inventory Tab and the Monitors table in the Right Pane of the System Health Dashboard:

Status	Description
	The component and all subcomponents are working properly (status is **good**).
	The component or a subcomponent has a critical problem (status is **error**). A red indicator is accompanied by an **x** symbol.
	The component or a subcomponent 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 available for the monitors, as the 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.

Troubleshooting and Limitations

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	

12

Legacy System Health

Note to HP Software-as-a-Service 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.

This chapter includes:

Concepts

Tasks

Reference

➤ System Health Monitoring on page 324

Troubleshooting and Limitations on page 326

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 imbedded part of HP Business Availability Center. For details on deploying the new System Health interface, see “Deploy and Access System Health” on page 222.

Legacy System Health - Overview

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

Data Processing Server Resource Status

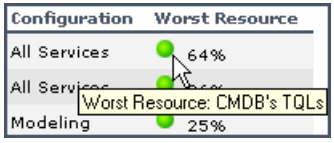
The resource status information that is displayed on the System Health page is based on capacity limit and threshold settings that are preconfigured by HP. These settings can be viewed in the Infrastructure Settings Manager (select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure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



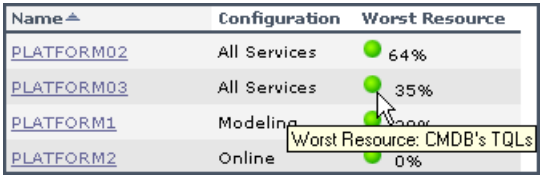
- **threshold representation of the percentage of capacity limit**. Uses a color-coded icon to express the percentage of the capacity limit, based on the following ranges:

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:

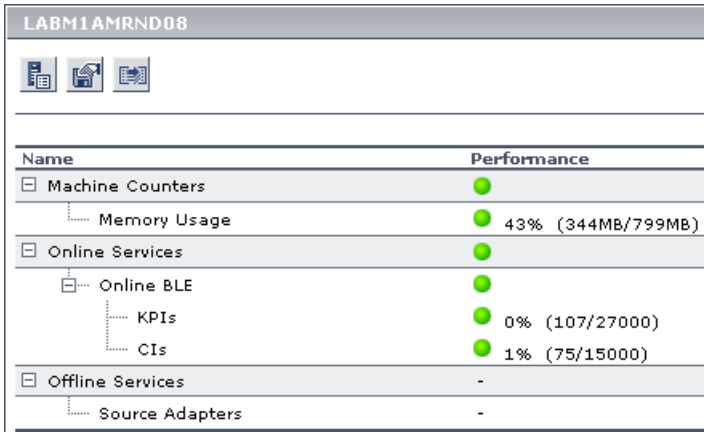
- for each active server in the list, the percentage of capacity limit and its threshold representation, in the Worst Resource column, indicating the status of the worst-performing resource among all the resources being monitored on that server.
- a tooltip with resource details. Place your mouse pointer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



- 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).

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 "Configure Automatic Failover for the Data Processing Server" on page 313.
- manually reassign services to accommodate the need for server machine maintenance. For details, see "Manually Reassign Services" on page 317.

Monitor System Resources on the System Health Page

This task describes how 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.

1 View 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).

2 View 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 "Data Processing Server Resource Status" on page 308.

3 View 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.

Configure Automatic Failover for the Data Processing Server

The process of automatically moving services from a primary server to another server is called **Automatic Failover**. Automatic Failover for a Data Processing Server to a backup server must be configured. It is not enabled by default.

This task describes how to configure automatic failover for the Data Processing Server:

1 Enable Automatic Failover of Primary Servers

To enable automatic Failover of Primary Servers, perform the following steps:

a 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.

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

c 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.

---

2 Configure the Backup Server for Primary Servers

To configure the backup server for primary servers, perform the following steps:

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

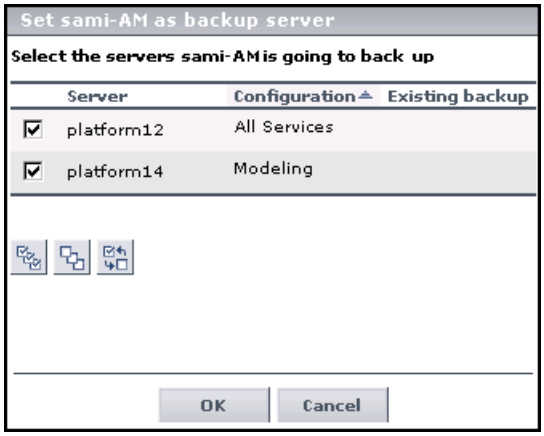
b In the Servers pane, choose the **Data Processing** tab. Click the server to be the backup server. Information about the selected server is displayed in the Services pane.

c 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.

d 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 “Manually Reassign Services” on page 317.

Remove Automatic Failover

This procedure describes how 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.

Manually Reassign 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 manually 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.

Legacy System Health User Interface

This section describes:

➤ System Health Page on page 318

System Health Page

Description	Displays the status of the servers, resource groups, services, and monitored resources running HP Business Availability Center. **To Access:** Select **Admin** > **Platform** > **Setup and Maintenance** > **System Health.**
Important Information	The System Health page consists of the following panes: ➤ Servers ➤ Services ➤ Management
Useful Links	"Legacy System Health - Overview" on page 305

Servers Pane

Description	Displays the status of the servers running HP Business Availability Center. **To Access:** Select **Admin** > **Platform** > **Setup and Maintenance** > **System Health**
Important Information	The Servers Pane is located on the left side of the page. It contains the following tabs: ➤ **All.** Lists the name and type of all servers running HP Business Availability Center. ➤ **Data Processing.** Lists information on the Data Processing Servers running Services HP Business Availability Center. Servers Pane elements described below appear on either the All tab, the Data Processing tab, or both. If the server is configured as a backup server, the names of the severs the server is backing up are displayed. This information is displayed even if Automatic Failover has been disabled.
Useful Links	"Legacy System Health - Overview" on page 305 "Data Processing Server Resource Status" on page 308

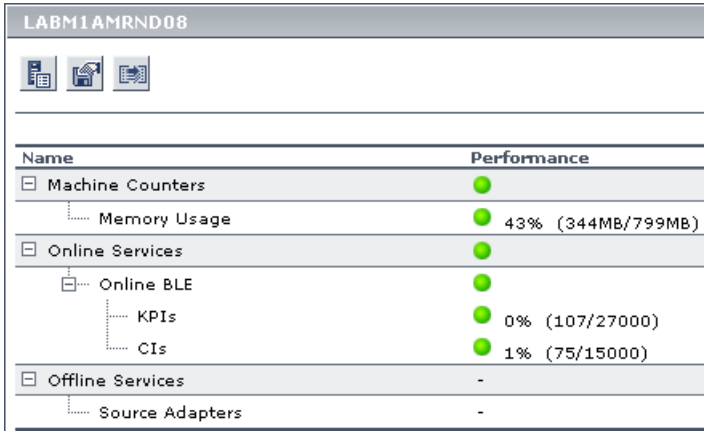
The Servers Pane includes the following elements (listed alphabetically):

GUI Element	Description
	Click to refresh the list of servers.
Configuration	The services that the specified server is configured for.
Name	The name of the server.

GUI Element	Description
Server Type	The type of the server.
Worst Resource	The status of the worst-performing resource among all resources being monitored on the server. Performance is indicated as follows: ➤ **percentage of capacity limit.** Represents the actual usage of the resource relative to its configured capacity limit. ➤ **threshold representation of the percentage of capacity limit.** Uses a color-coded icon to express the percentage of the capacity limit. For details on the ranges of the color-coded icons, see "Types of Resource Status Information" on page 309. **Tooltip:** Resource details on the specific resource whose status is being reported.

Services Pane

Description	Displays the statuses of all the monitored resources for the server currently selected in the Servers pane. **To Access:** Select **Admin** > **Platform** > **Setup and Maintenance** > **System Health**
Important Information	The Services Pane is located on the right side of the page. Information is displayed only if you have selected a server in the Servers Pane. The capacity limits displayed in the Performance column 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).
Useful Links	"Legacy System Health - Overview" on page 305 "Data Processing Server Resource Status" on page 308 "System Health Monitoring" on page 324



The Services Pane includes the following elements (listed alphabetically):

GUI Element	Description
	Click to show properties of the selected server. The <server name> Properties page contains the following fields: ➤ **Name.** The name of the server. ➤ **IPs.** 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.
	Click to set the selected server as a backup server.
	Click to move services from the selected server to another server. You choose which services you want to move from the dropdown list that appears, and then enter the destination server in the resulting dialog box.

GUI Element	Description
Name	The services and their monitored resources, per resource group.
Performance	The performance level of the corresponding service, monitored resource, or resource group. Performance data is presented as follows: ➤ 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 For details on the ranges of the color-coded icons, see "Types of Resource Status Information" on page 309.

Management Pane

Description	Displays the status of tasks that are running or were run during the course of the current Web session. **To Access:** Select **Admin** > **Platform** > **Setup and Maintenance** > **System Health**
Important Information	The Management Pane is located on the bottom of the page.
Useful Links	"Legacy System Health - Overview" on page 305

System Health Monitoring

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.
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

Resource Group	Service	Monitored Resource	Description
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

Troubleshooting and Limitations

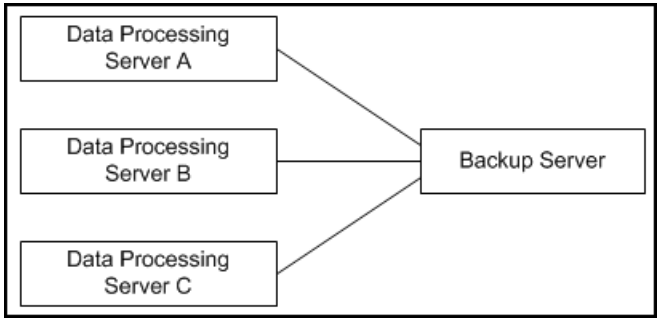
Use the following information to troubleshoot issues, as required.

Service Reassignment

Following are notes and limitations relating to Service Reassignment. For details on Service Reassignment, see “Understanding Service Reassignment” on page 306.

- 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.
- When manually reassigning services, if a task does not complete (that is, the reassigned services do not start successfully), the Status tab continues 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 329.
- 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.

  Use the following information to troubleshoot issues, as required.

Legacy 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.

Legacy 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*.

13

Audit Log

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

This chapter includes:

Concepts

Tasks

Reference

Audit Log - Overview

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:

- **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 Software-as-a-Service 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 Software-as-a-Service 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 "Use the Audit Log" on page 334.
- **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 Software-as-a-Service 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.

Use 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 to open the Auditing Filters pane 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.

Audit Log User Interface

This section describes:

- Audit Log Page on page 335

Audit Log Page

Description	Enables you to keep track of different actions performed by users in the system. **To Access:** Select **Admin** > **Platform** > **Setup and Maintenance** > **Audit Log**.
Important Information	You can optionally click the Auditing Filters link and specify filter criteria. For details, see "Auditing Filters Pane" on page 336.
Useful Links	"Audit Log - Overview" on page 331

The Audit Log page includes the following elements (listed alphabetically):

GUI Element	Description
	Click to move to the previous page or next page in the audit log.
Actions	Displays the actions performed by the specified user.
Additional Information	Displays additional information, where relevant.
Context	Select a context to view.
For user	Displays the user whose actions are displayed in the audit log, as specified in the Auditing Filters pane. **Default Value:** All
Modification Date	Displays the date and time that the specified actions were performed.
Modified By	Displays the user who performed the specified actions.
Profile	Select a profile for which you want to view the actions performed. **Note:** This field is not visible for all contexts.
RUM Engine	Select a RUM Engine for which you want to view the actions performed. **Note:** This field is displayed only if you have chosen the Monitor Administration (RUM) context.

GUI Element	Description
SiteScope	Select a SiteScope for which you want to view the actions performed. **Note:** This field is displayed only if you have chosen the Monitor Administration (SiteScope) context.
Time Period	Displays the time period whose actions are displayed in the audit log, as specified in the Auditing Filters pane. **Default Value:** All

Auditing Filters Pane

The Auditing Filters pane includes the following elements (listed alphabetically):

GUI Element	Description
	Click to open the calendar dialog box and select a date.
	Click to expand the Auditing Filters pane.
	Click to collapse the Auditing Filters pane.
Apply	Click to apply the selected filters.
Cancel	Click to cancel filtering and close the Auditing Filters pane.
Clear All	Click to clear the filters and display all log items.
Containing text	Specify a text string that the action must contain to be displayed.
End before	Specify an ending time period to view actions for.
Start after	Specify a starting time period to view actions for.
User	Specify a user in the system to view actions performed by only that user.

14

Report Schedule Manager

This chapter provides information on the Report Schedule Manager.

This chapter includes:

Concepts

Reference

Report Schedule Manager - Overview

A user with Administrator permissions can edit, delete, resume, or pause scheduled reports in the Report Schedule Manager. You schedule user reports (custom reports, trend reports, service reports, and favorite filters) in the Report Manager to enable specific recipients to automatically receive the specified report, via e-mail, at regularly defined intervals. For details on scheduling user reports, see “Create a Schedule” in *Reports*.

Report Schedule Manager User Interface

This section describes:

Report Schedule Manager Main Page

Description	Enables you to manage schedules configured on reports and report objects in the Report Manager. **To access:** Select **Admin** > **Platform** > **Report Schedule Manager**.
Important Information	You must have Administrator permissions to access the Report Schedule Manager. You cannot create a new schedule from the schedule list page. For details on creating schedules, see "Create a Schedule" in *Reports*.
Included in Tasks	"Create a Schedule" on page 103

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
	Click to open the Edit Schedule for <Report Name> dialog box and edit the selected schedule. For details, see "Create New Schedule Dialog Box" in *Reports*. **Note:** This dialog box enables you only to edit an existing schedule - you create a new schedule from the Report Manager interface. For details, see "Create a Schedule" in *Reports*.
	Click to delete the selected schedule.
	Click to resume the selected schedule.
	Click to pause the selected schedule.
	Click to refresh the Report Schedule Manager page.
	Click to reset the width of the columns to the default setting.

GUI Element (A–Z)	Description
	Click to select columns to be visible in the table. For details, see "Working with Tables" in *Reference Information*.
Generation Time	The time (in the indicated time zone) that the schedule is to be generated.
Recipients	The individuals configured in the Report Manager to receive the report or report item at scheduled intervals. For details on configuring Schedules, see "Create New Schedule Dialog Box" in *Reports*.
Recurrence	The recurrence pattern for the selected schedule.
Report Name	The name of the report that the schedule is configured for.
Report Type	The type of report that the schedule is configured for.
Status	The status of the schedule. Possible values are: ➤ Active ➤ Paused

Part III

Data Collection

15

Data Collector Maintenance

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

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

This chapter includes:

Concepts

Tasks

Reference

Data Collector Maintenance - Overview

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.

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 by clicking the link on the right column of the Data Collector Maintenance page.

Note: Data collectors can be installed from the Downloads page in Platform Administration. For details on downloading, see "Downloads Overview" on page 155.

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

Removing a Business Process Monitor

If a specific Business Process Monitor data collector becomes obsolete, you can use the Data Collector Maintenance page to remove it from the management database.

Removing a Business Process Monitor 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 Page" in *Using End User Management*.

Remove a Business Process Monitor Remotely

You can use HP Business Availability Center to remove 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 "Data Collector Information Dialog Box" on page 349.

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.

Data Collector Maintenance User Interface

This section describes:

➤ Data Collector Maintenance Page on page 347

Data Collector Maintenance Page

Description	Enables you to: ➤ View a list of your data collectors ➤ View data collector properties ➤ Remove a Business Process Monitor instance **To access:** Select **Admin** > **Platform** > **Data Collection** > **Data Collector Maintenance.**
Important Information	➤ The Data Collector Maintenance page contains the following tabs: ➤➤ SiteScope ➤➤ Business Process Monitor ➤➤ Real User Monitor ➤ Elements described in the following table appear on all tabs, unless otherwise noted. **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. ➤ To receive information on a data collector, click the **Information Button**  next to the selected data collector. For details, see "Data Collector Information Dialog Box" on page 349.
Useful Links	"Data Collector Maintenance - Overview" on page 344

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
	Click to refresh the list of services.
	Click to view the information window for the specific data collector. For details, see “Data Collector Information Dialog Box” on page 349.
<link to data collector's administration site>	Enables you to perform administrative tasks on the data collector directly from this page.
Export BPM Information Button	Click to export information from the selected Business Process Monitors to a text file. **Note:** This button is visible only on the Business Process Monitor tab.
Host Name	The name of the host machine on which the selected data collector is installed.
IP Address	The IP address of the host machine on which the data collector is installed.
Last Ping TIme	The last time the service pinged the management database.
Location	The location of the host machine on which the data collector is installed.
Location drop down list	Select to filter the list of data collectors by host location.
Removable	An indication of whether or not the data collector instance is removable. **Note:** This column is visible only on the Business Process Monitor tab.

GUI Element (A–Z)	Description
Remove Button	Click to remove selected Business Process Monitors. **Note:** This button is visible only on the Business Process Monitor tab.
Version	The version number, including build number, of the data collector software.

Data Collector Information Dialog Box

Description	Displays information on a data collector, including an explanation of why a non-removable instance cannot be removed. **To access:** Select **Admin** > **Platform** > **Data Collection** > **Data Collector Maintenance**; click the **Information Button**  next to the selected data collector.
Important Information	The Data Collector Information Dialog Box displays the same fields that appear on the tables in the Data Collector Maintenance page tabs, in addition to the fields described in the following table.
Useful Links	"Data Collector Maintenance - Overview" on page 344

The following elements are included:

GUI Element (A–Z)	Description
Associated Profiles	The profiles currently associated with the data collector.
Build Number	The build number of the data collector software.
Installed Updates	A list of the updates that have been installed on the data collector software.
Last Error	The last reported error message, if one exists.
Last Error Time	The time of the last reported error message, if one exists.

16

Downtime/Event Scheduling

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

This chapter includes the main concepts and reference information for scheduling Downtime and Events.

This chapter includes:

Concepts

Reference

Downtime and Event Scheduling - Overview

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

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.

For details on defining downtime and events, see “Downtime/Event Schedule Page” on page 353.

Downtime Events User Interface

This section describes:

Downtime/Event Schedule Page

Description	Displays the list of scheduled events in which HP Business Availability Center is marked as being in downtime. **To access:** Select **Admin** > **Platform** > **Data Collection** > **Downtime/Event Schedule.**
Important Information	➤ You can place the pointer over the entries in the Associated Profiles column to view a tooltip of all the profiles associated with a specific event. ➤ You can edit and delete only those events for which you have full permissions on all the profiles associated with the event. For details on permissions, see "Permissions Overview" on page 415.
Useful Links	"Downtime and Event Scheduling - Overview" on page 352

The following elements are included:

GUI Element (A–Z)	Description
Associated Profiles	The profiles associated with the event.
Event Description	A description of the downtime or scheduled event.
Event Name	The name of the downtime or scheduled event.
New Event	Click to create a new downtime or scheduled event.

New Downtime/Event Schedule Dialog Box

Description	Enables you to schedule downtime or an event when HP Business Availability Center excludes data collected during this time interval from its reports. **To access:** Select **Admin** > **Platform** > **Data Collection** > **Downtime/Event Schedule** > **New Event.**
Important Information	The New Downtime/Event Dialog Box consists of the following panes: ➤ **Event Schedule General Properties.** Enter the name and description of the event. ➤ **Event Frequency.** Schedule the frequency with which the event is to occur. **Important:** The time period that you define here must 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). ➤ **Event Schedule Action.** Specify the events to be performed during the event, and the profiles for which they apply. **Notes:** ➤ These settings do not affect the generation of alerts defined in SiteScope and cannot stop SiteScope from running during downtime or scheduled events. ➤ 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.
Useful Links	"Downtime and Event Scheduling - Overview" on page 352

Event Schedule Properties Pane

The following elements are included:

GUI Element (A–Z)	Description
Event Description	Enter a description of the event being configured.
Event Name	Enter a descriptive name for the event being configured.

Event Frequency Pane

The following elements are included:

GUI Element (A–Z)	Description
End On...	Click to configure the date and time for the event to end.
Event Duration	Select the duration of the event you are configuring. Select the relevant number of days, hours, and minutes that the event is to take place for.
Event Duration	Configure the duration of the event, in hours and minutes.
Every	Select to configure an event that is to occur more than once. You then select the appropriate day(s) of the week that the event is to occur on.
Every <date> of each month	Select to configure an event that is to occur once per month. Select the date of the month from the corresponding drop-down box.
Limit event recurrence to the following time range	Select to limit the event recurrence to occur only during the specified time range.
Once	Select to configure an event that is to occur one time.
Recurring Event Start Time	Configure the time of day that the recurring event is to start on.

GUI Element (A–Z)	Description
Single Event Start On	Click to configure the start date for the event you are configuring.
Start On...	Click to configure the date and time for the event to start.

Event Schedule Action Pane

The following elements are included:

GUI Element (A–Z)	Description
	Click to remove the highlighted profiles from the Selected Profile list.
	Click to move the highlighted profiles to the Selected Profiles list.
Available Profiles	Highlight a profile to move it to the Selected Profiles list. Hold the Ctrl key while selecting to choose multiple profiles.
Selected Profiles	The list of profiles associated with the event.
Stop Running the Profile during the event occurrence	Select to stop running the selected Business Process profile and data collection during the time the event is scheduled to occur.
Stop sending Event Based alerts during the event occurrence	Select to prevent alerts from being generated during the time the event is scheduled to occur.

17

Profile Entity Maintenance

This chapter includes the main concepts and reference information for Profile Entity Maintenance.

This chapter includes:

Concepts

Reference

Profile Entity Maintenance Overview

The Profile Entity Maintenance page enables you to exclude unwanted entities from your profiles by performing the following actions:

- Configure report filters globally. For details, see “Configure Report Filters Globally” on page 357.
- Delete entities from the database. For details, see “Delete Entities From the Database” on page 358.

Configure 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. This is useful if you want information only from specific entities in your profile.

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 Page" in *Using End User Management*.

Delete 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 Overview" 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.

Profile Entity Maintenance User Interface

This section describes:

➤ Profile Entity Maintenance Page on page 359

Profile Entity Maintenance Page

Description	Enables administrators to exclude - per profile - specific transactions, locations, and groups from all HP Business Availability Center reports for the current and future profile sessions. **To access:** Select **Admin** > **Platform** > **Data Collection** > **Profile Entity Maintenance.**
Important Information	➤ The Profile Entity Maintenance page consists of the following tabs: ➤ Transactions ➤ Locations ➤ Groups Choose the relevant tab for the type of entity you want to filter from all reports. ➤ 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.
Useful Links	"Profile Entity Maintenance Overview" on page 357

The following elements are included:

GUI Element (A–Z)	Description
Apply	Click to activate the selected filter(s).
Associated Hosts	The machine that hosts the location machine, if applicable. **Note:** This field appears only on the Locations tab.

GUI Element (A–Z)	Description
Associated Scripts	The scripts associated with the specified transaction, if applicable. **Note:** This field appears only on the Transactions tab.
Associated Locations	The locations where the specified group is located, if applicable. **Note:** This field appears only on the Groups tab.
Delete	Select the check box next to the transaction(s), location(s), or group(s) you want to delete. **Important:** 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 Delete check box is disabled for that entity.
Filter from Reports	Select the check box next to the transaction(s), location(s), or group(s) you want to exclude from reports for all users in the system.
Group Name	The name of the group you can exclude from reports for all users in the system. **Note:** This field appears only on the Groups tab.
Groups tab	Displays a table of the groups associated with the selected profile.
Location Name	The name of the location you can exclude from reports for all users in the system. **Note:** This field appears only on the Locations tab.
Locations tab	Displays a table of the locations associated with the selected profile.
Select Profile	Choose the profile from which you want to select transactions, locations, or groups to exclude from reports.

GUI Element (A–Z)	Description
Transaction Name	The name of the transaction you can exclude from reports for all users in the system. **Note:** This field appears only on the Transactions tab.
Transactions tab	Displays a table of the transactions that are running on the selected profile.

18

Working with Measurement Filters

Note to HP Software-as-a-Service customers: HP Operations administers these pages and the interface is hidden from view.

This chapter includes the main concepts and tasks for Measurement Filters.

This chapter includes:

Concepts

Tasks

Reference

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 display only 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.

Define Measurement Filters

This task describes how to define a measurement filter.

You define measurement filters from the Measurement Filters page, which you access from the **Admin** > **Platform** > **Data Collection** tab. For details, see "Measurement Filters Page" on page 366.

For details on the data types listed on the Measurement Filters page, see "Data Samples" in *Reference Information*.

1 Prerequisites

You must access the Measurement Filters page to define a measurement filter. Select **Admin** > **Platform** > **Data Collection** tab, and click the **New Filter** button.

2 Create a New Filter

You create measurement filters to display only the most relevant data entering HP Business Availability Center. For details on creating a measurement filter, see "New Filter Page" on page 368.

3 Create a Category

Optionally, you define categories that help to organize your filters in a meaningful manner. For details on defining categories, see "Measurement Filters Page" on page 366.

4 Assign a Category to a Measurement Filter

Optionally, you can assign one or more categories to a filter. For details on assigning categories to a filter, see "Measurement Filters Page" on page 366.

Measurement Filters User Interface

This section describes:

➤ New Filter Page on page 368

Measurement Filters Page

Description	Displays the measurement filters configured for the data received by HP Business Availability Center, to display only the most relevant data. **To access:** Select **Admin** > **Platform** > **Data Collection** > **Measurement Filter.**
Important Information	To edit a filter, click the filter's name in the list of filters.
Included in Tasks	"Define Measurement Filters" on page 365
Useful Links	"Measurement Filters Overview" on page 364 "Data Samples" in *Reference Information*.

The following elements are included:

GUI Element (A–Z)	Description
	Click to collapse and hide the filter list.
	Click to expand and view the filter list.
Category	Select to display the filters by category.
Category button	Click to view the category that the filter is associated with.

GUI Element (A–Z)	Description
Category Manager	Click to open the Category Manager dialog box and view the list of filter categories. For details on the Category Manager dialog box, see "Category Manager Dialog Box" on page 368. **Note:** This button is visible only if you have chosen to view filters by category. The Category Manager page contains of the following elements: ➤ **Category Name.** Lists the available categories. ➤ **New Category.** Click to create a new category.
Data Type	The data type for which you want to define a filter.
Duplicate button	Click to copy settings of the specific filter to a new filter.
Filter	The name of the specific filter.
Name	Select to display the filters by name.
New Filter	Click to create a new filter.
Search	Enter the complete or partial filter name in the Search box and click **Go** to locate a specific filter. **Note:** You can type an asterisk to replace characters. For example, to search for the filter **probe on cats machine**, enter ***cat***.

Category Manager Dialog Box

Description	Enables you to view the list of filter categories, and to add a new filter category. **To access:** Select **Admin** > **Platform** > **Data Collection** > **Measurement Filter,** select the **Category** option and click **Category Manager**.
Important Information	The Category Manager page contains of the following elements: ➤ **Category Name.** Lists the available categories. ➤ **New Category button.** Click to open the New Category dialog box and create a new category. Enter the name of the category in the **Name** field of the New Category dialog box.
Included in Tasks	"Define Measurement Filters" on page 365

New Filter Page

Description	Enables you to configure a new filter for filtering data from HP Business Availability Center. **To access:** Select **Admin** > **Platform** > **Data Collection** > **Measurement Filters**, click the **New Filter** button.
Important Information	➤ You build an expression by working in the following order: Field, Operator, Value. ➤ You should not use a field and operator combination twice in the same **And** phrase. ➤ The values you enter in the Value box are case sensitive and you must enter them precisely as they are used in the samples. ➤ 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). For details on the applicable data types, see "Data Samples" in *Reference Information*.

Included in Tasks	"Define Measurement Filters" on page 365
Useful Links	"Measurement Filters Overview" on page 364

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
Add 'OR' Expression	Click to define alternate parameters for the filter.
Add Values	Click to add specified values to the Value field. **Note:** This button is enabled only for select RUM data types fields. For details, see "Add Predefined Values to Fields" on page 370.
And	Click to define additional parameters for the filter.
Boolean Expression	Displays the result of the configured filter as a boolean expression.
Field	Choose the field by which to filter the sample. For a list of fields associated with each sample, see "Data Samples" in *Reference Information*.
Name	Enter a descriptive name for the filter.

GUI Element (A–Z)	Description
Operator	Choose an operator for which you want to filter the sample. **Notes:** ➤ The list of operators displayed depends on the selected field. ➤ 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".
Value	Enter a value that the expression compares with the value in the data sample.

Add Predefined Values to Fields

When configuring a new measurement filter, you enter a value that the boolean expression compares with the value in the data sample. However, 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 **Value** 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

19

Central Repository Service

Note to HP Software-as-a-Service customers: The repository for HP Software-as-a-Service scripts functions differently from the repository described here. For details on working with scripts, see "HP Software-as-a-Service Script Repository" on page 392.

This chapter includes the main concepts, tasks, and reference information for the Central Repository Service.

This chapter includes:

Concepts

Tasks

Reference

Central Repository Service - Overview

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.
- 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 Monitors Overview" and "Managing Business Process Profiles Overview" 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.

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 501 in *Solutions and Integrations*.

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 how to create file sets, see "Upload Scripts" on page 374.

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 and Monitors Overview" in *Using End User Management*.

Upload Scripts

This task describes how to upload scripts in the Central Repository Service.

This task includes the following steps:

- "Prerequisites" on page 374
- "Upload Scripts to the Central Repository Service" on page 374

1 Prerequisites

You must create folders to store scripts in. For details on creating and managing folders, see "Panel Tree Pane" on page 377.

2 Upload Scripts to the Central Repository Service

You upload scripts to the Central Repository Service folders.

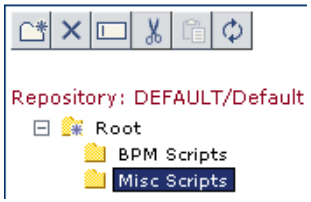
a In the folder tree in the left pane, highlight the folder into which you want to upload the script.

b In the right pane, click the **New** button on the bottom right corner of the Folder Content area, and fill in the relevant cells in the Create File Set dialog box.

For details on uploading scripts, see "File Set Table Pane" on page 379.

3 Results

Folders are created under the Root folder.



The folders contain the various scripts you upload to the Central Repository Service.

Work With Scripts

This task describes how to work with scripts in the Central Repository Service.

1 Prerequisites

You must upload a script in the Central Repository Service. For details on uploading scripts, see “Upload Scripts” on page 374.

2 Check out a Version

You can check out a version of a file set to ensure that no other user makes changes to this version of the script while you are editing it. For details on checking out a version, see “Action Buttons” on page 380.

3 Download File Set Content

You download file set content to open and edit the downloaded script. 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. For details on downloading a file set, see “Action Buttons” on page 380.

4 Upload File Set Content

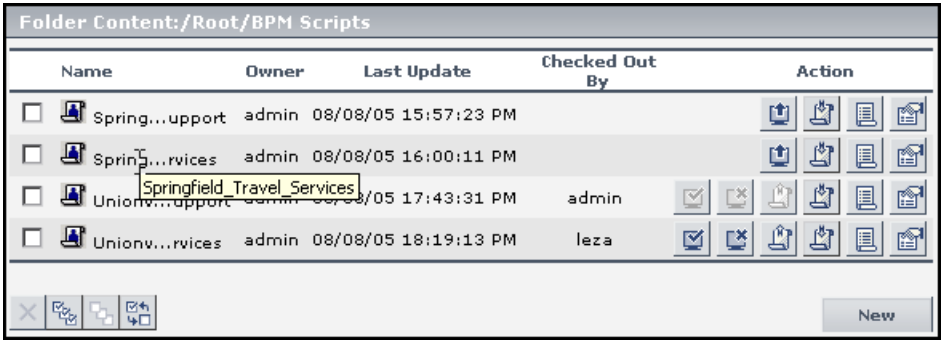
Optionally, you can upload a script without creating a new file set version. For details on uploading a script, see “Action Buttons” on page 380.

5 Checking In a File Set

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. Alternatively, you can cancel the check out to prevent the Central Repository Service from creating a new version number and leave the file checked in with its current version number. For details on checking in a file set and cancelling check out, see “Action Buttons” on page 380.

6 Results

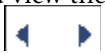
Your scripts appear in the File Set Table Pane on the right side of the page.



Central Repository Service User Interface

This section describes:

Central Repository Service Main Page

Description	Displays the Business Process Monitor scripts stored in the Central Repository Service, and the folders that contain the scripts. **To access: Admin** > **Platform** > **Data Collection** > **Central Repository Service**.
Important Information	The Central Repository Service Main Page consists of the following sections: ➤ **Panel Tree Pane.** Displays a tree hierarchy of the folders in the Central Repository Service, and the buttons used to manage them. For details, see "Panel Tree Pane" on page 377. ➤ **File Set Table Pane.** Displays a table with the content of the selected folder. For details, see "File Set Table Pane" on page 379. You can hide and view the Panel Tree by clicking the appropriate icon  between the Panel Tree and File Set Table panes.
Useful Links	"Central Repository Service - Overview" on page 372

Panel Tree Pane

Description	Displays a tree hierarchy of the folders in the Central Repository Service, and the buttons used to manage them. **To access:** Select **Admin** > **Platform** > **Data Collection** > **Central Repository Service.**
Important Information	You create folders below the **Root** level folder.
Useful Links	"Central Repository Service - Overview" on page 372

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
	Click to create a new folder.
	Click to delete the selected folder.
	Click to rename the selected folder.
	Click to cut the selected folder from its place in the tree hierarchy.
	Click to paste the previously cut folder to a new location in the tree hierarchy. **Note:** You cannot paste a folder into the same folder from which it was cut.
	Click to refresh the navigation tree. **Tip:** You refresh the tree to load the folder data that may have been modified by other users. **Note:** The tree refreshes automatically when you perform any of the folder operations, so it is not necessary to refresh it manually.
	Denotes the Root folder in the tree hierarchy.
	Denotes a Central Repository Service folder.

File Set Table Pane

Description	Displays, in table format, the file sets that have been created within the folder that is highlighted in the folder tree. The table also contains: ➤ Information relating to the file sets ➤ Action buttons for managing the file sets. **To access:** Select **Admin** > **Platform** > **Data Collection** > **Central Repository Service.**
Important Information	For details on viewing version properties, see "Version Properties Dialog Box" on page 386.
Useful Links	"Central Repository Service - Overview" on page 372

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
	Denotes a Virtual User Generator (VUGen) script.
	Denotes a QuickTest Professional script.
	Click to activate the search for the string entered in the **Search By Name** box.
Action	Icons denoting the available options you can perform on the fileset.
Checked Out By	The user who has the file set currently checked out. **Note:** If the file set is not checked out, this column is blank.
Last Update	The date when the file set was last checked into the repository. **Note:** This could be the date the file set was first created.

GUI Element (A–Z)	Description
Name	The name given to the file set when it was created and the script was uploaded. **Tooltip:** Displays the full name of the fileset, in case the name was long and therefore truncated in the table.
New	Click to open the Create File Set dialog box and create a new file set. For details, see "Create File Set Dialog Box" on page 383.
Owner	The user who created the file set by uploading the script.
Search By Name	Enter a string you want to search for appearing in the Name field of the File Set Table.

Action Buttons

The following elements are included in the Action column:

GUI Element (A–Z)	Description
	Click to open the Version History page and view version history for the file set. For details, see "Version History Dialog Box" on page 384.
	Click to open the File Set Properties page and view properties of the file set. **Notes:** ➤ 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** field can be edited only by the user who checked out the file set. ➤ You can click **Show Additional Properties** to view the properties related to the script itself.

GUI Element (A–Z)	Description
	Click to check out the selected file set for editing. **Notes:** ➤ Checking out a file set ensures 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.
	Click to open a check-in version of the Version properties dialog box and check in the file set version. For details on the Version properties dialog box, see "Version Properties Dialog Box" on page 386. **Important:** ➤ This button is displayed only for those file sets that have been checked out. ➤ When you check in a file set, the Central Repository Service automatically creates a new version number 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.

GUI Element (A–Z)	Description
	Click to cancel checkout of the file set. **Notes:** ➤ This button is displayed only for those file sets that have been checked 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.
	Click to upload a script to save your recent script modifications to the Central Repository Servicewithout creating a new file set version. **Notes:** ➤ This action serves 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.
	Click to download file set contents for editing. **Note:** 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.

Create File Set Dialog Box

The following elements are included:

GUI Element (A–Z)	Description
Content	Enter the path of the .zip file containing the script. You can also click **Browse** to locate the .zip file in your file system.
Description	Optionally, add a description for the new file set. The description appears in the file set properties.
Name	The name of the content or .zip file specified in the **Content** field. You cannot fill this field in manually.
Type	Choose the type of file set you want to add to the Central Repository Service from the Type list. **Notes:** ➤ If you select AUTO-DETECT, the script type is determined during the upload. ➤ Currently, the following types are supported in HP Business Availability Center: AUTO-DETECT, VUGEN SCRIPT, and QTP SCRIPT.

Version History Dialog Box

Description	Displays a listing of all the versions of a file set and the actions that can be performed on that file set version. **To access:** Click the **Show Versions** button  in the **Action** column of the File Set table.
Important Information	➤ 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 table, the following fields are visible 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 a variety of actions on the version checked-out version. For details on the available actions, see "Action Buttons" on page 380. ➤ You may want to access a previous version of a file set, to view information relevant to a specific date or activity. You can make this the current version of the file set by clicking the restore button  .
Included in Tasks	"Upload Scripts" on page 374

GUI Element (A–Z)	Description
	Select to view version properties. ➤ You can optionally modify the **Version Comment** field. All other fields are uneditable. ➤ Click the Show Additional Properties to view properties of the script itself.
	Click to restore a previous version of a file set and make it the current version.
	Click to download the specific version of the file set for editing. **Notes:** ➤ 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. ➤ You cannot download the version of a file set version that is checked out.
Action	Buttons enabling you to perform actions on the specified version, as follows:
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.
Modified By	The user who last checked in the version of the file set.
Version	The number given to the file set when it was last checked into the Central Repository Service.

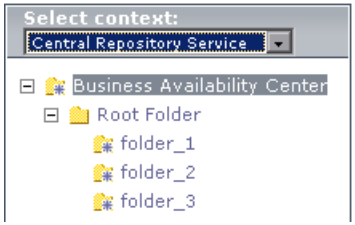
Version Properties Dialog Box

Description	Displays properties and property values of the file set version you are checking in. **To access:** Click the **Version Properties** button  next to the file you want to view properties and property values for.
Important Information	The Version Properties dialog box lists the properties and values of the specified file set version. The properties displayed in this dialog box are: ➤ **Last Modification Date** ➤ **Version Label** ➤ **Modified By** ➤ **Version Comment.** Optionally, you can 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. ➤ **Content.** Optionally, click **Browse** to locate and select the .zip file of the latest version of the script.
Included in Tasks	"Upload Scripts" on page 374

Central Repository Service Permissions

This section includes the following topics:

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 "Permissions Overview" on page 415.

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.

20

Data Collection Administration for HP Software-as-a-Service

Note: The Location IP Ranges, Script Repository, and Package Information pages are available to HP Software-as-a-Service customers only.

This chapter provides information on Data Collection Administration for HP Software-as-a-Service.

This chapter includes:

Concepts

Tasks

Reference

Data Collection Administration for HP Software-as-a-Service - Overview

Data Collection Administration for HP Software-as-a-Service enables you to do the following:

- View the customer's list of locations and related information. For details, see "Location IP Ranges Page" on page 395.
- Maintain your scripts and view their verification information. For details, see "HP Software-as-a-Service Script Repository" on page 392.
- View information on the package the customer agreed to when the HP Software-as-a-Service contract is signed. For details, see "Package Information Page" on page 396.

HP Software-as-a-Service Script Repository

The HP Software-as-a-Service 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. For details, see "Managing Business Process Profiles Overview" in *Using End User Management*.

Once you have created and recorded the scripts, you upload them using the Script Repository page. For details, see "Create and Upload Scripts to the Script Repository – Workflow" on page 393.

Create and Upload Scripts to the Script Repository – Workflow

This task describes how to create and upload scripts to the Script Repository.

This task includes the following steps:

- "Create and Record Business Process Monitor Scripts" on page 393
- "Zip Script Files" on page 393
- "Upload Scripts" on page 393
- "Edit Scripts" on page 394
- "Re-upload the Script" on page 394

1 Create and Record Business Process Monitor Scripts

You record Business Process Monitor scripts using the HP Virtual User Generator recording tool. For details, see "VuGen Recording Tips" in *Using End User Management*..

2 Zip Script Files

You zip only the Business Process Monitor scripts' run-time files for upload. Zipping all files may cause script verification to fail due to a limit in the file size allowed by the repository.

3 Upload Scripts

You upload scripts by clicking the **Upload** button on the Script Repository page. For details on uploading scripts, see "Upload Script Dialog Box" on page 406.

4 Edit Scripts

Click the script name link and save 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.

5 Re-upload the Script

After editing a script, you must upload it again to the repository. You must zip the script before uploading. After you upload the edited script, HP Business Availability Center reruns the verification process on the script.

HP Software-as-a-Service Data Collection User Interface

This section describes:

- Location IP Ranges Page on page 395
- Package Information Page on page 396
- Script Repository Page on page 401

Location IP Ranges Page

Description	Displays a list of locations defined in your package, including the detailed IP address ranges. **To access:** Select **Admin** > **Platform** > **Data Collection** > **Location IP Ranges.**
Important Information	The Location Info page displays 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.

Package Information Page

Description	Displays information about the customer package, as agreed upon and entered in the HP Business Availability Center application when the HP SaaS contract is signed. **To access:** Select **Admin** > **Platform** > **Data Collection** > **Package Information.**
Important Information	You can use the Package Information page for: ➤ Viewing Package Information. ➤ Selecting Locations for Business Process Monitors. For details, see "Package Locations Page" on page 397. ➤ Viewing and Modifying Package Properties Information. For details, see "Package Properties Page" on page 398. The abbreviation **POP** refers to **Point of Presence** - a place where the package is located. It is used in the following contexts: ➤ **Global POPs.** Any customer can access the locations. ➤ **Private POPs.** Only the associated customer can access the package.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
	Click to view the available Business Process Monitor locations on which to run the packages. For details, see "Package Locations Page" on page 397.
	Click to open the Package Properties page to view and modify package properties information. For details, see "Package Properties Page" on page 398.
Business Process Monitor Transactions	The total number of Business Process Monitor transactions that can be run as part of the package.

GUI Element (A–Z)	Description
Expiration	The expiration date of the package. 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.
Global POPs	The total number of Global Points Of Presence that can be run as part of the package.
Name	The name of the package.
Private POPs	The total number of Private Points Of Presence that can be run as part of the package.
URLs	The total number of single URL monitors that can be accessed as part of the package.

Package Locations Page

Description	Displays the available Business Process Monitor locations on which to run the package. **To access:** Select **Admin** > **Platform** > **Data Collection** > **Package Information**, and click the **Package Location** button  .
Important Information	The Package Locations Page contains the following fields: ➤ **Package name.** Indicates the name of the selected package. ➤ **Location name.** Indicates the locations that the package is available to run on. Select the check box to run the package; de-select the check box to disable the package from running.

Package Properties Page

Description	Displays information about the customer package for specific applications (Business Process Monitor and SiteScope). **To access:** Select **Admin** > **Platform** > **Data Collection** > **Package Information**, and click the **Edit** button  .
Important Information	This information is entered in HP Business Availability Center when the contract is signed with HP. You can modify only the subscribed recipients. The Package Properties page contains the following tabs: ➤ **General.** For details, see "General Tab" on page 398. ➤ **End User Management.** For details, see "End User Management Tab" on page 400. ➤ **System Availability Management.** For details, see "System Availability Management Tab" on page 401. You select the individual who approved the package properties in each tab via the **Approved by** dropdown.

General Tab

Description	Displays general information about the selected package. **To access:** Admin > Platform > Data Collection > Package Information, click the **Edit** button  .
Important Information	The General Tab is the default selection on the Package Properties screen.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
Customer Name	The name of the customer.
Customer UDX Name	The customer name to be used when reporting data into the system.
Package Name	The name of the selected 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.
Subscribed Recipients	The names of the recipients configured to receive package expiration notices via e-mail. Click **Change** to open the Select Recipients dialog box. For details on the Select Recipients dialog box, see ➤ 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.
Payment Policy	The policy for package payment that the customer has chosen. Available options are: ➤ Eval (Evaluation) ➤ Paying

End User Management Tab

Description	Displays package information related to End User Management. **To access:** Select **Admin** > **Platform** > **Data Collection** > **Package Information**, click the **Edit** button  and select the **End User Management** tab.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
Number of Private POPs	The number of private POPs allowed for the 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.
Location set	The set of Business Process Monitor locations for the package. Options include: ➤ WW (World Wide) ➤ Europe ➤ North America
Number of URLs	The number of single URL 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.

System Availability Management Tab

Description	Displays package information related to SiteScopes. **To access:** Select **Admin** > **Platform** > **Data Collection** > **Package Information**, click the **Edit** button  and select the **System Availability Management** tab.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
Monitor Frequency (min.)	Indicates how often (in minutes) the SiteScopes refresh themselves.
Number of SiteScope measurements	The number of SiteScope measurements that have been approved as part of the package.
Number of SiteScope 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.

Script Repository Page

Description	Displays the Business Process Monitor scripts that have been uploaded. **To access:** Select **Admin** > **Platform** > **Data Collection** > **Script Repository.**
Important Information	The Script Repository Page consists of the following tabs: ➤ **Business Process Monitor.** Used to manage your Business Process Monitor scripts. ➤ **Verification Subscription.** Used to configure recipients to receive email notification when Business Process Monitor script verification is complete. For details, see “Verification Subscription Tab” on page 406.

Included in Tasks	"Create and Upload Scripts to the Script Repository – Workflow" on page 393
Useful Links	"HP Software-as-a-Service Script Repository" on page 392

The following elements are included:

GUI Element (A–Z)	Description
	Click to open the Manual Script Verification dialog box and manually verify the script. For details, see "Manual Script Verification Dialog Box" on page 403.
	Click to open the **.usz** file directly in the Virtual User Generator (if you have installed it).
Last Update	The date the script was most recently updated.
Owner	The name of the most recent user to update the script.
Script Name	The name of the script. Click to open the **.zip** or **.obs** files that comprise the transaction. You click the script name link and save 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 or .obs formats.
Starts with	Filter your view of the Script Repository content according to the first character in the Script Name.
Status	The status of the verification process for the script. You double-click the status to open the Script Verification Results dialog box and modify it. For details, see "Script Verification Results Dialog Box" on page 404.

GUI Element (A–Z)	Description
Upload	Click to upload Business Process Monitor scripts to the Script Repository. For details, see "Upload Script Dialog Box" on page 406.
Version	The current version of the script. 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. For details on accessing older versions of a script, see "<Script Name> Versions Dialog Box" on page 405.

Manual Script Verification Dialog Box

Description	Enables you to change the verification status of a script and to remove a script from use. **To access:** Select **Admin** > **Platform** > **Data Collection** > **Script Repository**, click the **Manual Verification** button  .
Important Information	You can choose from the following options in the Script Status field: ➤ **Verified for HP SaaS.** Select to enforce script to be verified for HP SaaS (for operators and superusers only). ➤ **Verified for private POP.** Select for scripts that you want to verify for use on your private Business Process Monitor. ➤ **Verification failed.** Select to disable a transaction before running your profile.
Included in Tasks	"Create and Upload Scripts to the Script Repository – Workflow" on page 393
Useful Links	"Script Repository Page" on page 401 "HP Software-as-a-Service Script Repository" on page 392

Script Verification Results Dialog Box

Description	Displays the status of the verification process for the script. **To access:** Select **Admin** > **Platform** > **Data Collection** > **Script Repository**, select the **Business Process Monitor** tab and click the value in the **Status** field.
Included in Tasks	"Create and Upload Scripts to the Script Repository – Workflow" on page 393
Useful Links	"Script Repository Page" on page 401

The following elements are included:

GUI Element (A–Z)	Description
Expected/Allowed Value Verifications	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 ➤ Failed

<Script Name> Versions Dialog Box

Description	Enables you to track changes made to scripts and to access them to perform changes. **To access:** Select **Admin** > **Platform** > **Data Collection** > **Script Repository**, select the **Business Process Monitor** tab and click the script version number.
Important Information	The <script-name> versions dialog box 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.
Included in Tasks	"Create and Upload Scripts to the Script Repository – Workflow" on page 393
Useful Links	"Script Repository Page" on page 401

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
Description	The description of the script. This is useful for version control: you can describe why changes were made to this version of the script.
Last Update	The date the script was most recently updated.
Owner	The name of the most recent user to update the script.
Status	The status of the verification process for the script. You double-click the status to open the Script Verification Results dialog box and modify it. For details, see "Script Verification Results Dialog Box" on page 404.
Version	Click to open the scripts. Scripts are stored in **.zip** format

Upload Script Dialog Box

Description	Enables you to upload a Business Process Monitor script to the Script Repository. **To access:** Select **Admin** > **Platform** > **Data Collection** > **Script Repository**, select the **Business Process Monitor** tab and click **Upload**.
Included in Tasks	"Create and Upload Scripts to the Script Repository – Workflow" on page 393
Useful Links	"Script Repository Page" on page 401

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
Description	Enter a description of the script.
Script	The path of the Business Process Monitor script you are uploading.
Upload	Click to upload the script to the Script Repository.

Verification Subscription Tab

Description	Enables HP Business Availability Center to send email notification to specified recipients when Business Process Monitor script verification is complete. **To access:** Select **Admin** > **Platform** > **Data Collection** > **Script Repository**, select the **Verification Subscription** tab.
Important Information	To send email notification when verification is complete: ➤ Click the **Notify the following recipients when script verification is complete** check box. ➤ Specify one or more e-mail addresses of the recipients in the **E-mail address(es)** box. Multiple recipients addresses must be separated by a semi-colon.
Included in Tasks	"Create and Upload Scripts to the Script Repository – Workflow" on page 393

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.

Running Verifications	Rule	Actual Result
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).
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 Software-as-a-Service Support.

Part IV

User Management

21

User Management

This chapter includes the main concepts, tasks, and reference information for User Management.

This chapter includes:

Concepts

Tasks

Reference

User Management – Overview

You use the User Management interface to configure HP Business Availability Center 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.

The User Management interface is available only to users with appropriate permissions. A user's permissions are either inherited from their assigned role, or granted individually when their parameters are configured. For details on permissions, see "Permissions Overview" on page 415.

You can change a user's parameters, including their username and password, in the General Tab. For details, see "General Tab" on page 455.

For a suggested workflow to configure groups and users in your HP Business Availability Center system, see "Configure User Management - Workflow" on page 423.

Managing Groups

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 "An Example of Nested Groups" on page 421.

Permissions Overview

You can enable sophisticated and detailed permissions scenarios for the groups and users defined in your HP Business Availability Center platform, to assign permissions access to specific areas of HP Business Availability Center. Permissions are based on both the user who is granted the permission and the resource on which the permission is granted.

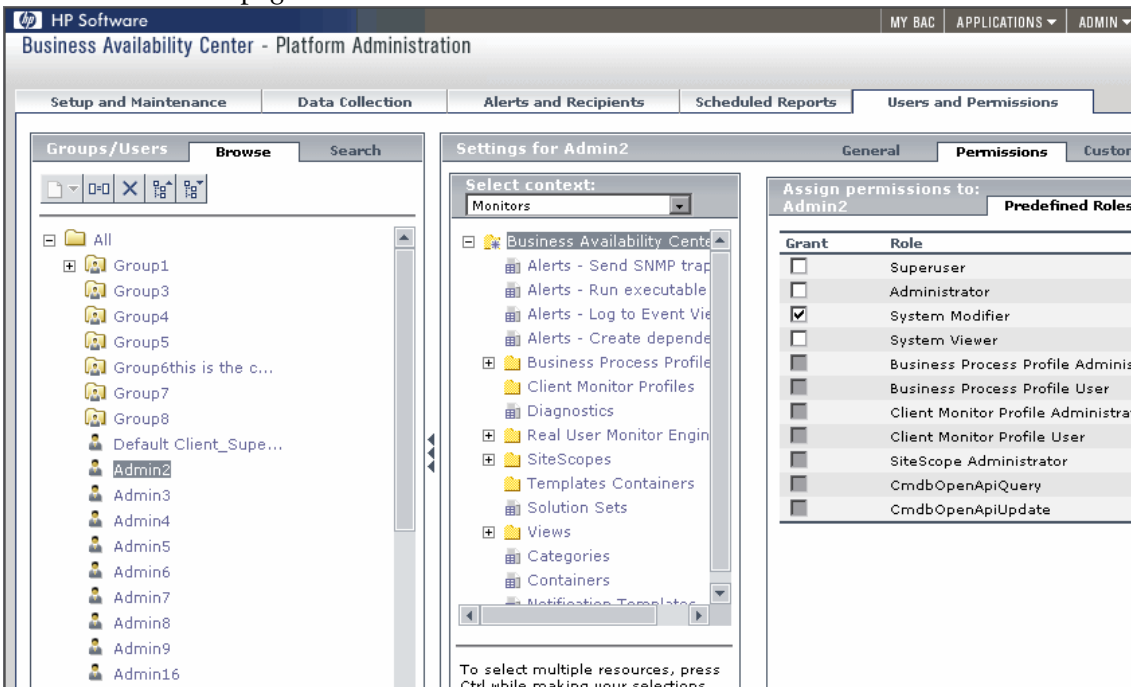
Granting permissions has three components:

- 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.



For details on assigning permissions, see “Assign Permissions” on page 435.

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 the Permissions tab. For details, see “Roles” on page 419.

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.

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.

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.

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.

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.

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.

For a description of each role, including details of the resources on which roles can be applied, see "User Management User Interface" on page 445.

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.

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.

  For details on the available operations in HP Business Availability Center, see "User Management Operations" on page 486.

Group and User Hierarchy

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.

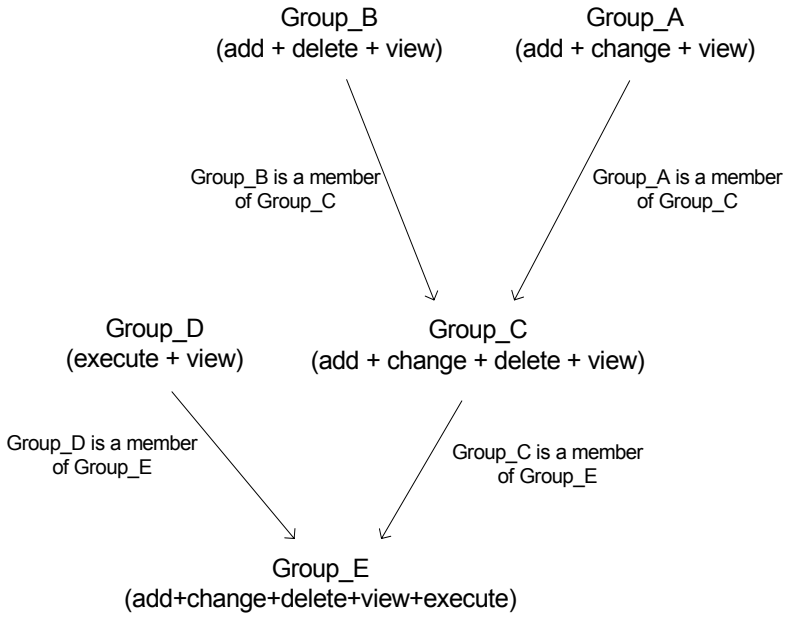
When nesting groups, please note the following:

- A group can be a member of several groups.
- 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.

  For details on setting up nested groups, see "Configure Group and User Hierarchy" on page 437.

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.

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 cannot be a member of Group_A.

Note: All permissions in the above example refer to the same resource.

For notes and limitations on nesting groups and users, see “Hierarchy Tab” on page 464.

Customizing User Menus

The Customization tab enables you to:

- Select 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 the interface to display only the areas of HP Business Availability Center that are relevant to specific users.

Configure User Management - Workflow

This task describes a suggested working order for the User Management application.

This is a suggested workflow. However, you can configure your User Management settings in any other logical order you choose.

For a scenario of this task, see "User Management Configuration- Scenario" on page 425.

This task includes the following steps:

1 Prerequisites

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 email address (contact information is required for HP Software-as-a-Service 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 417.

2 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 the user interface for creating groups, see "Groups/Users Pane" on page 447.

3 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 on assigning permissions, see "Assign Permissions" on page 435.

4 Create Users

You create users and then place them into the appropriate groups. For details on the user interface for creating users, see "Groups/Users Pane" on page 447.

5 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 on configuring user and group hierarchy, see "Configure Group and User Hierarchy" on page 437.

6 Customize User Settings

In the Customization tab, you customize the menu items that are displayed in different contexts for users. For details on customizing menu items, see "Customizing User Menus" on page 413.

User Management Configuration- Scenario

This scenario describes how to configure users and user groups in the User Management portal.

For a task of this scenario, see "Configure User Management - Workflow" on page 423.

1 Mapping Out Users and Groups

Jane Smith is the System Administrator at NewSoft Company, and wants to configure users and user groups to be authorized to use HP Business Availability Center, as well as end users who will be accessing Dashboard and reports. Before doing so, she requests the following preliminary information from relevant staff members:

- User names
- Login names
- Initial Passwords
- User Time Zones
- Contact Information (for example, telephone number, pager, email address)

Note: Contact information is mandatory only for HP Software-as-a-Service customers.

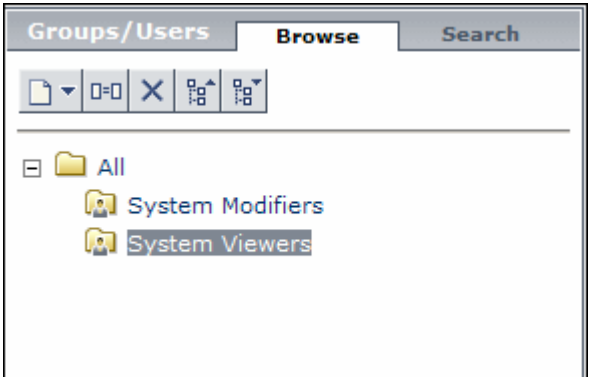
With this information, she then decides to create one group of users with the permission level of System Modifiers, and another with the permission level of System Viewers. Furthermore, one of the users is to have an additional role of SiteScope Administrator.

2 Creating Groups

Jane creates groups to group users together, according to the level of permissions they are to be granted. She clicks the **New Group/User** button in the Groups/Users pane and creates the following groups:

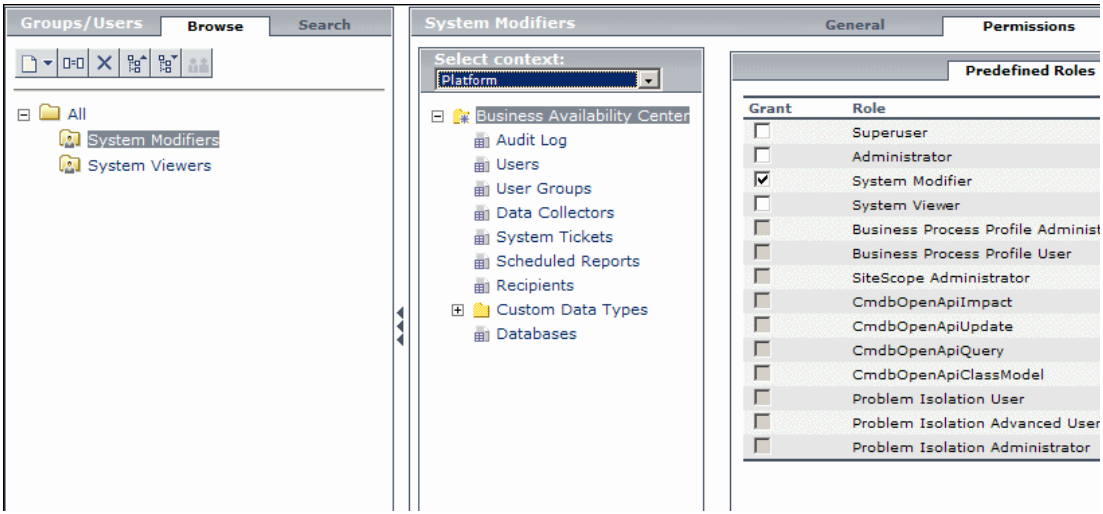
- System Viewers
- System Modifiers

The Groups/Users pane appears as follows:



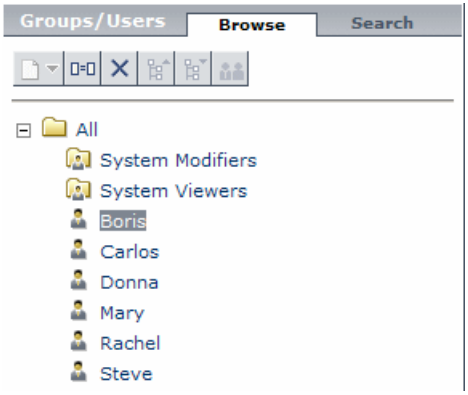
3 Assigning Permissions to Groups

Once the groups have been created, Jane assigns the relevant permission levels to the groups. After selecting **System Modifiers** in the Groups/Users pane, she navigates to the Permissions tab in the Information Pane on the right side of the page, and chooses the Root instance (Business Availability Center) from any context. In the Predefined Roles tab, she selects **System Modifier** and then clicks **Apply Permissions**. She then selects **System Viewers** in the Groups/Users pane and chooses the **System Viewer** role in the Predefined Roles tab, clicking **Apply Permissions** to assign the role.



4 Creating Users

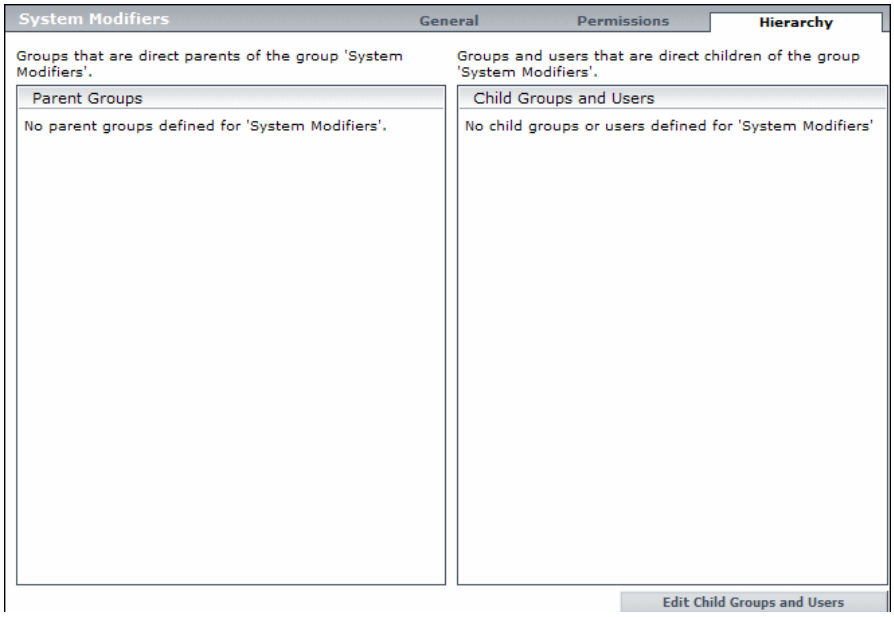
Jane must now create users to nest within the groups, in accordance with the desired permission levels of the individual users. She clicks the **New Group/User** button in the Groups/Users pane and while on the Root group, (**All**), she selects **Create User** and configures settings for each new user. The Groups/Users pane appears as follows:



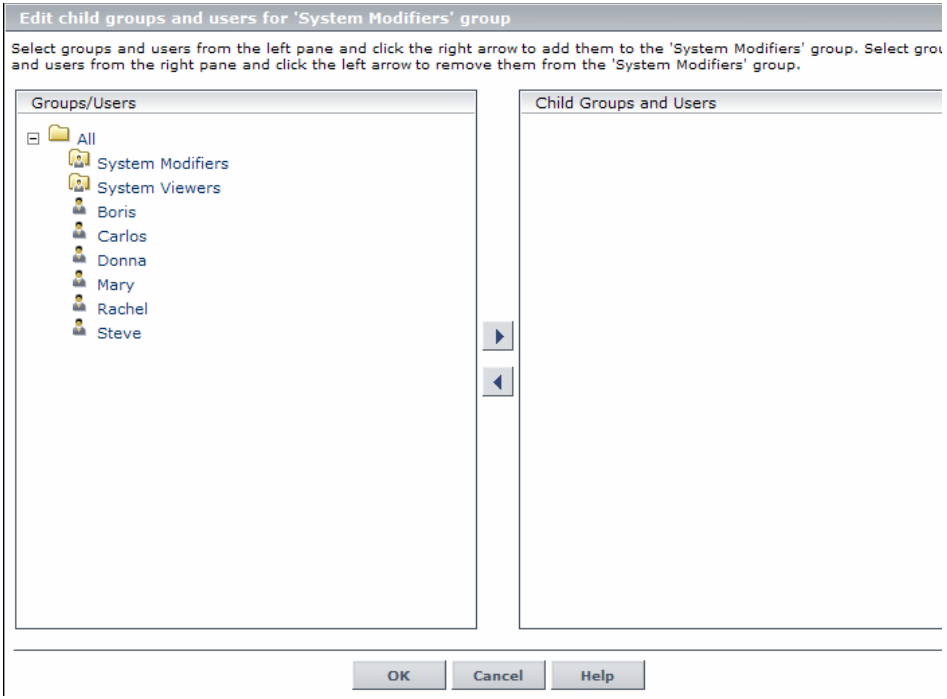
5 Configuring User and Group Hierarchy

Now that Jane has created users authorized to access HP Business Availability Center, she assigns their permission level by nesting them within the appropriate group.

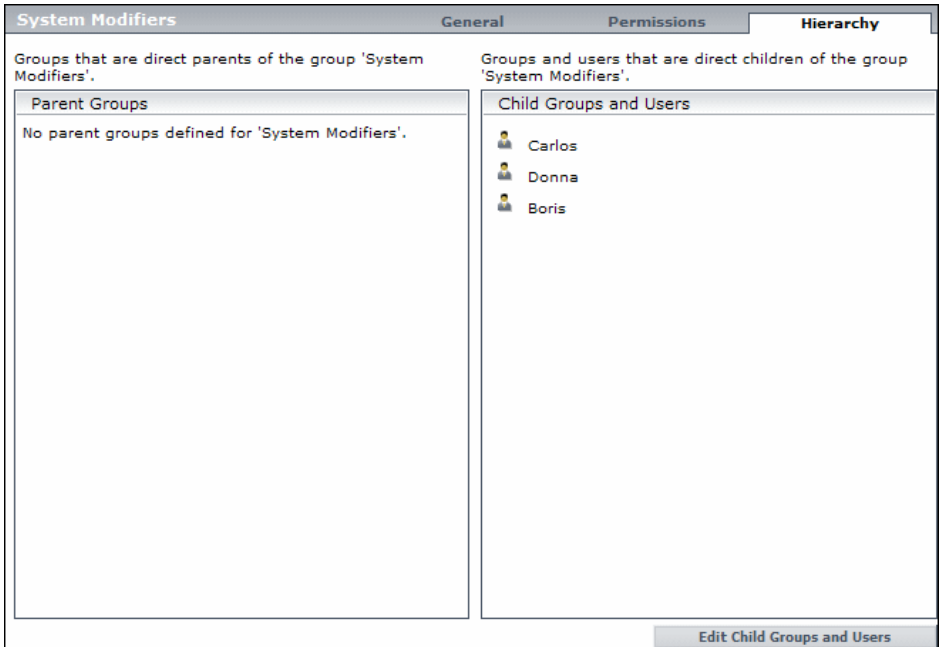
She selects the System Modifiers group from the Groups/Users pane to nest the appropriate users in this group. Jane then selects the **Hierarchy** tab from the Information Pane on the right side of the page. The hierarchy tab indicates that the System Modifiers group has no child groups, as follows:



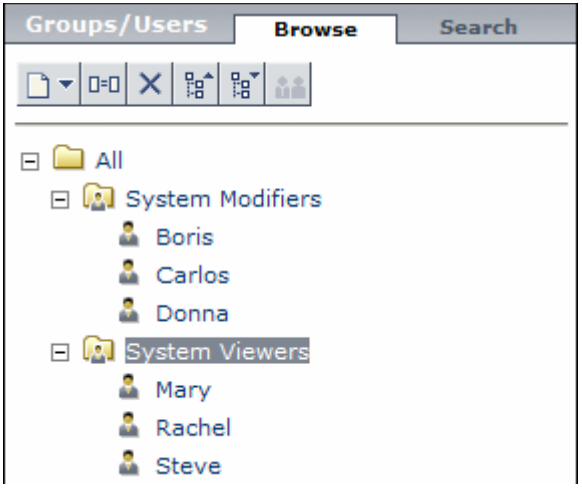
Jane clicks the **Edit Child Groups and Users** button to open the Edit Child Groups and Users dialog box, as follows:



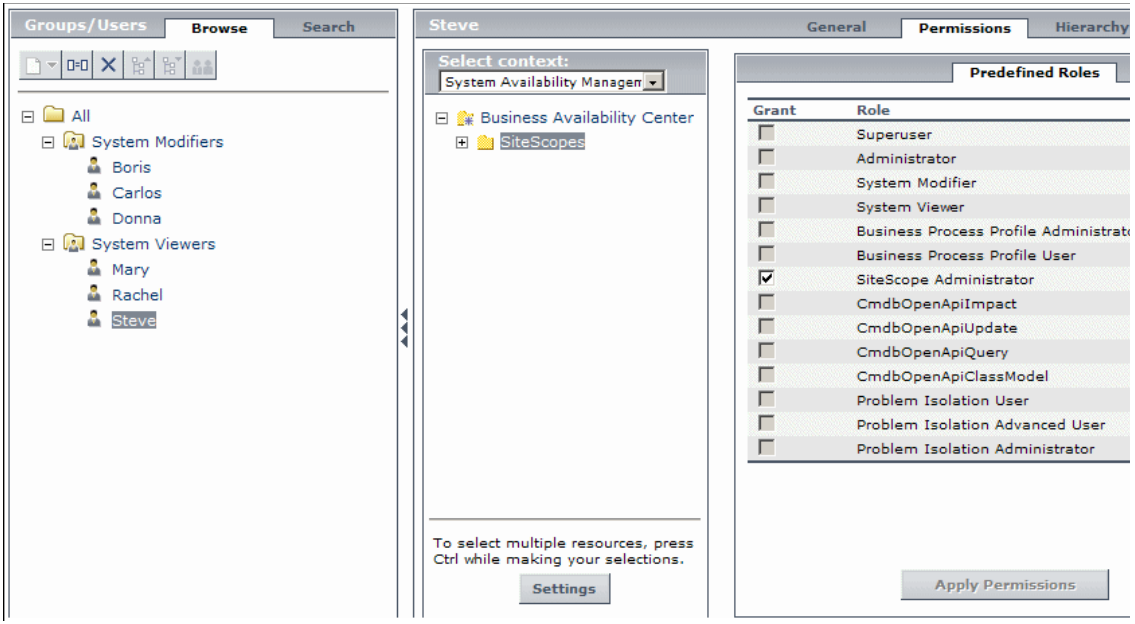
She then selects the relevant users from the Groups/Users Pane and clicks the right arrow to move them to the Child Groups and Users pane. The Hierarchy tab indicates that these users are nested within the System Modifiers group, as follows:



After following the same procedure to nest the relevant users in the System Viewers group, the Groups/Users pane is displayed as follows:



Since Steve has the added permission level of SiteScope Administrator, Jane selects the username of the user in the Groups/Users pane whom she wants to give the added permission level of SiteScope Administrator, and in the Permissions tab, selects the **System Availability Management** context. After selecting a resource, she then selects **SiteScope Administrator** from the Predefined Roles tab, and clicks **Apply Permissions**. The resulting screen appears as follows:



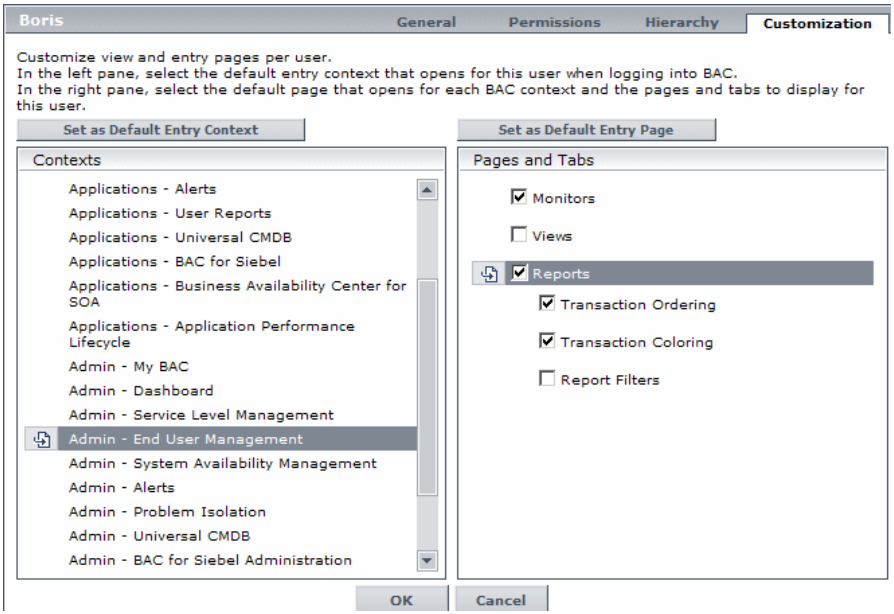
6 Customizing User Settings

Jane must now set the page each user sees when entering HP Business Availability Center, and the menu items available to them on pages throughout HP Business Availability Center. After selecting each user, she clicks the Customization tab and sets the following parameters:

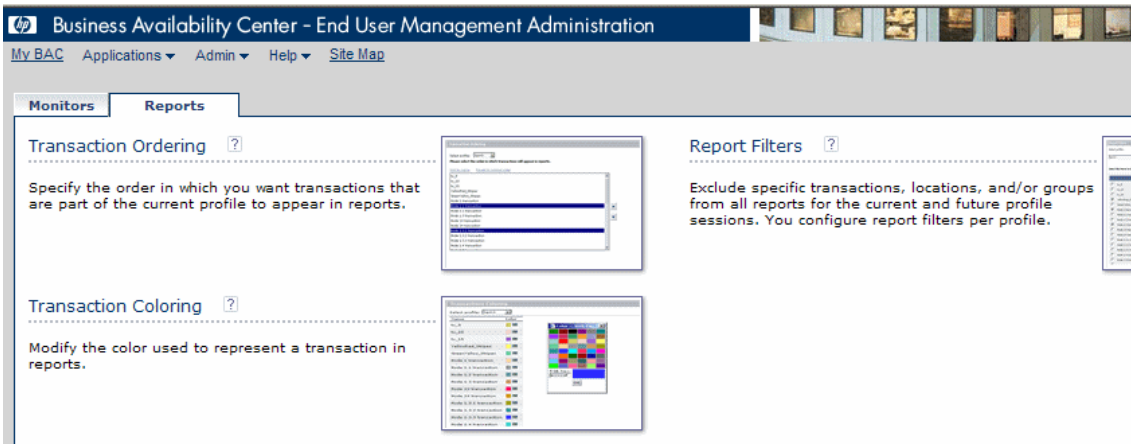
- The entry context that the user sees when logging into HP Business Availability Center. For example, **Admin - End User Management**.
- The page within the entry context that the user sees on the selected context. For example, **Reports**.

➤ The pages and tabs that are to be visible on each HP Business Availability Center page by selecting or clearing the relevant check boxes. For example, the **Views** page and the **Report Filters** tab are cleared to ensure that they are not visible on the **Admin - End User Management** context when the user logs in.

The configured settings are displayed on the customization tab as follows:



The login page that the user sees according to their customized configurations is as follows:



Assign Permissions

This task describes how to configure group and user permissions in User Management.

This task includes the following steps:

- "Task Prerequisites" on page 436
- "Select a Group or User" on page 436
- "Select a Context" on page 436
- "Assign a Role" on page 436
- "Assign Operations" on page 436
- "Configure Permissions Settings" on page 436

1 Task Prerequisites

Ensure that groups and users are configured in your system. For details on the user interface for creating groups, see "Groups/Users Pane" on page 447.

2 Select a Group or User

Select a group or user from the Groups/Users Pane on the left side of the page.

3 Select a Context

Select a context from the context list box above the resource tree in the center of the page. For details on the available contexts, see "User Management User Interface" on page 445.

4 Assign a Role

You assign a role for the selected group or user in the Roles tab on the right side of the page. For details on the available roles, see "User Management Roles" on page 467.

5 Assign Operations

You assign operations in the Operations tab that the group or user can perform in HP Business Availability Center. For details on the available operations, see "User Management Operations" on page 486.

6 Configure Permissions Settings

Optionally, click **Settings** at the bottom of the resource tree. The Apply Permissions Settings dialog box opens and you can configure the settings for the current session of applying permissions. For details, see "Settings" on page 459.

Configure Group and User Hierarchy

This task describes how to configure user and group hierarchy. For details on the Hierarchy tab user interface, see “Hierarchy Tab” on page 464.

This task includes the following steps:

1 Prerequisites

Ensure that you have configured at least one group and one user in the Groups/Users pane. For details on the Groups/Users pane, see “Groups/Users Pane” on page 447.

2 View Group and User Hierarchy

Select a group or user in the Groups/Users pane, and select the Hierarchy tab from the Information pane to view the parent and child groups of the group or user, if applicable.

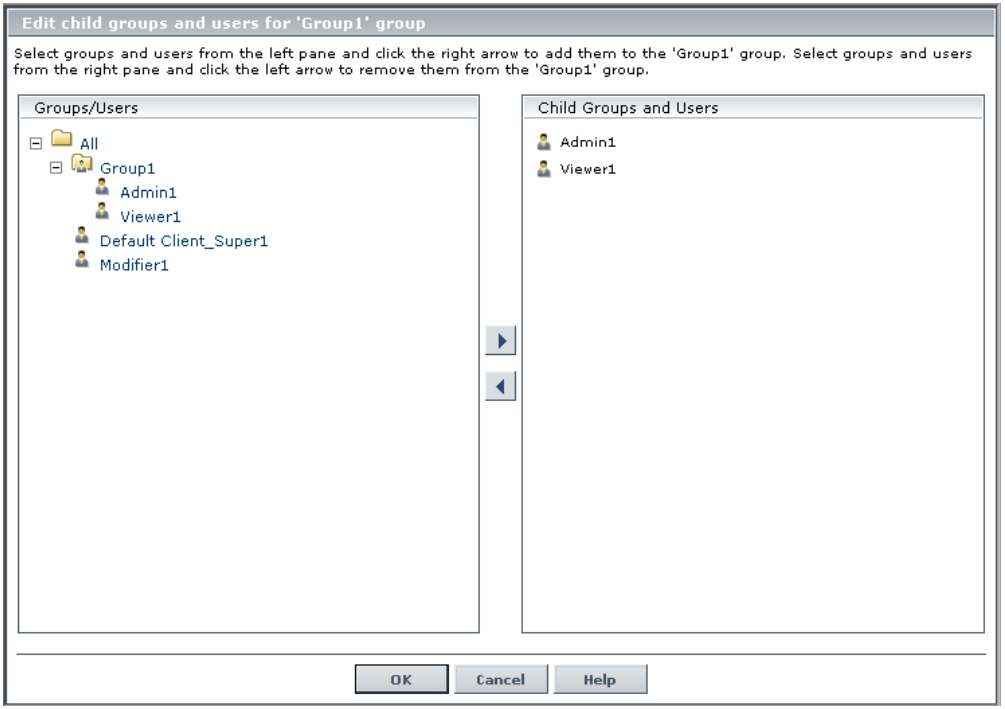
3 Nest Groups and Users

You choose a group in the Groups/Users pane, and choose groups and users to nest beneath it. Click the **Edit Child Groups and Users** button to open the Edit Child Groups and Users window. Choose a group or user from the left pane and click the right arrow button to move the group or user to the Child Groups and Users pane and nest it under the current group.

Example

1. Click a group or user in the **Browse** tab of the Groups/Users pane on the left side of the screen.
2. Click the **Hierarchy** tab on the right side of the screen.

3 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.



4 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.

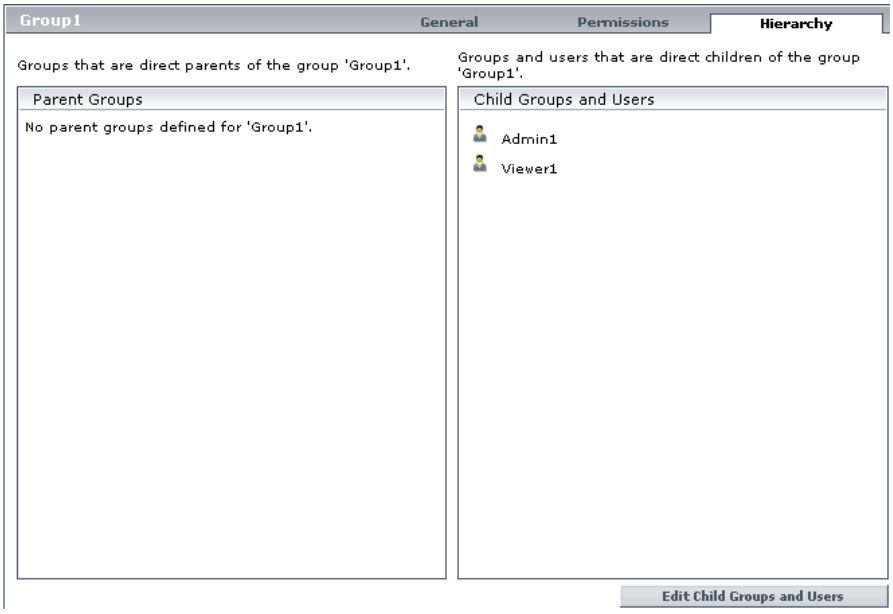
Unassign users and remove nested groups by selecting the group or user in the Child Groups and Users pane, and clicking on the right-to-left arrow.

To choose more than one group or user for nesting, press CTRL while making your selections.

4 Results

The nested groups and users appear in the right pane on the hierarchy tab.

Example



Customize User Menus

This task describes how to customize the page users see when entering HP Business Availability Center, and choose the menu items available on pages throughout HP Business Availability Center.

For a scenario of this task, see "Customize User Menus - Scenario" on page 441.

This task includes the following steps:

- "Prerequisites" on page 440
- "Choose a User" on page 440
- "Assign a Default Context" on page 440
- "Select Context Pages and Tabs" on page 440

1 Prerequisites

Ensure that you have configured at least one user in the Groups/Users pane. For details on the Groups/Users pane, see "Groups/Users Pane" on page 447.

2 Choose a User

Choose a user from the Browse tab in the Groups/Users pane whose pages and menu items you want to customize, and select the Customization tab.

3 Assign a Default Context

Select a context from the Contexts pane that you want to be the default entry context this user sees when logging into HP Business Availability Center, and click **Set as Default Entry Context**. For details on the Contexts pane, see "Customization Tab" on page 466.

4 Select Context Pages and Tabs

In the Pages and Tabs pane, select the check boxes of the pages and tabs that you want to be visible on the selected context for the user. Clear the check boxes of the pages and tabs that you want hidden from the user.

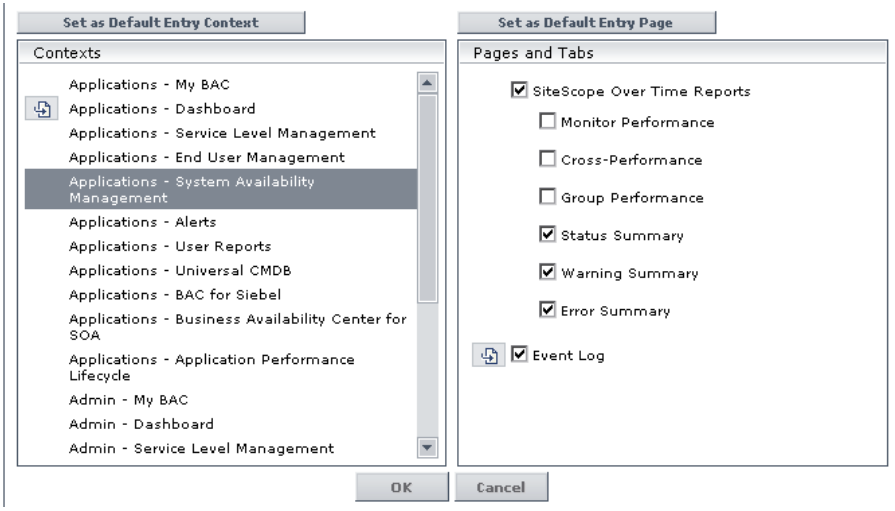
5 Assign a Default Entry Page

Select a page or tab to be the default entry page for the selected context, and click **Set as Default Entry Page**.

6 Results

The default entry icon appears next to the default entry context and page. Pages and tabs visible to the user are selected in the Pages and Tabs pane. Pages and tabs hidden from the user are cleared in the Pages and Tabs pane.

Example



Customize User Menus - Scenario

This scenario describes how to customize user menus for individual users.

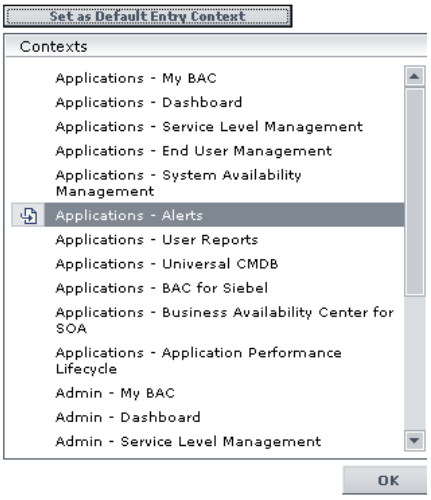
For a task of this scenario, see "Customize User Menus" on page 439.

1 Choosing a User

The administrator of ABC Insurance Company is creating several users in the User Management section of HP Business Availability Center. She decides that the user John Smith should be able to view only certain pages and tabs in HP Business Availability Center, and that a specific page should appear on his screen when he logs into HP Business Availability Center.

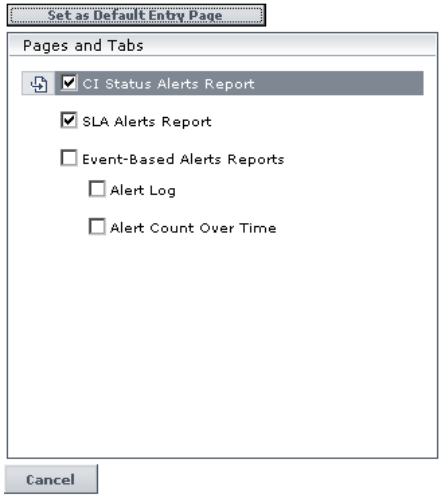
2 Assigning a Default Context

Since John's chief responsibility at ABC is to monitor alerts, the administrator designates the Applications - Alerts page as their default entry context. She selects **Applications-Alerts** in the Contexts pane, and clicks **Set as Default Entry Context**. The **Applications - Alerts** context is indicated as the default entry context with the default entry icon, as appears in the following image:



3 Selecting Context Pages and Tabs

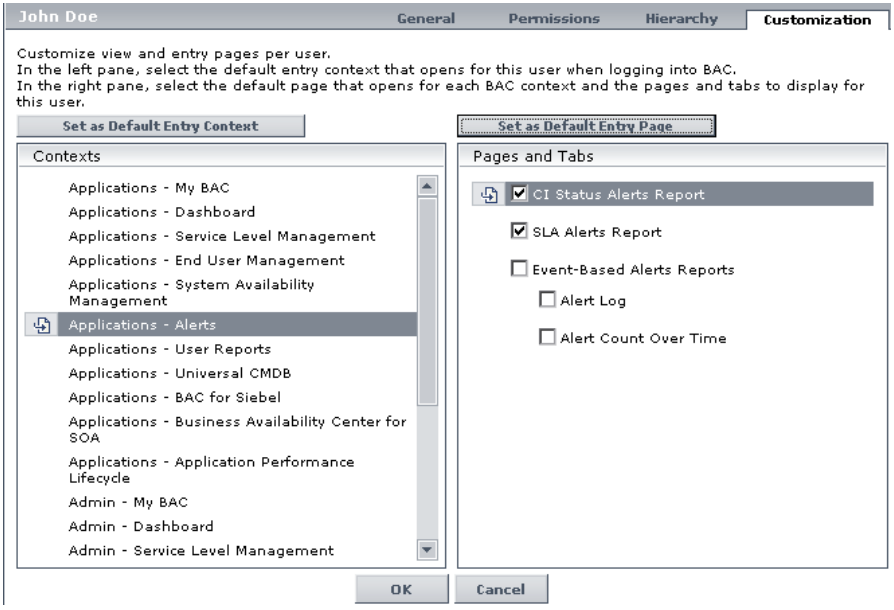
Since John is not authorized to view Event-Based Alert Reports, that option is cleared in the Pages and Tabs pane, leaving the remaining tabs, CI Status Alerts Report and SLA Alerts Report, checked to be visible when John logs into HP Business Availability Center. As Configuration Items Alerts are of the highest priority for ABC Insurance, the administrator designates this as the first page for John to see upon logging in. She selects **CI Status Alerts Report** in the Pages and Tabs pane, and then clicks **Set as Default Entry Page**. The **CI Status Alerts Report** is indicated as the default entry page with the default entry icon, as appears in the following image:



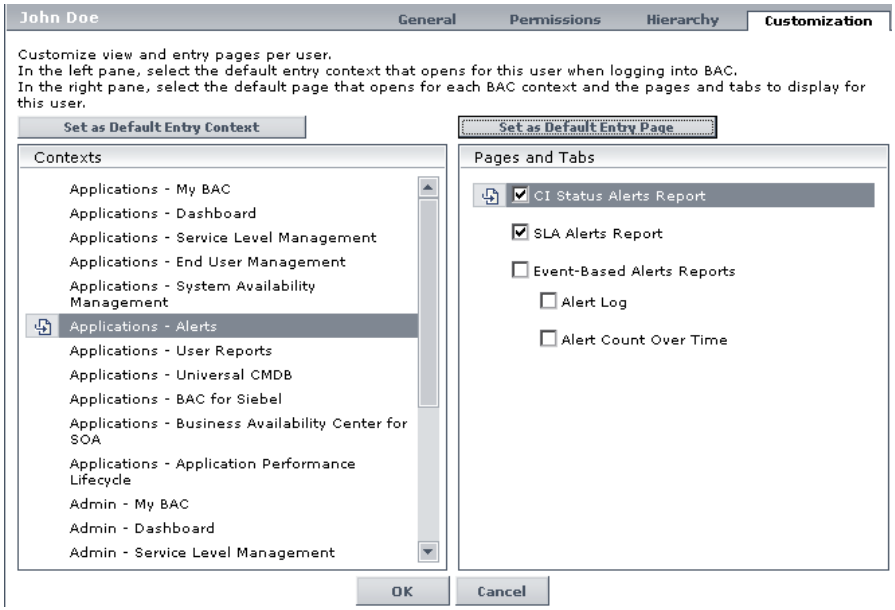
4 Results

The context that opens when John Doe logs into HP Business Availability Center is the **Alerts** context on the Applications menu. The **CI Status Alerts Report** page opens, and the SLA Alerts Report page is also available to him.

The configured Customization tab in User Management appears as follows:



The screen that John sees when logging into HP Business Availability Center appears as follows:



User Management User Interface

This section describes:

User Management Entry Page

Description	Displays an overview and suggested workflow of User Management, and the groups and users configured enabled to access HP Business Availability Center. **To access:** Select **Admin** > **Platform** > **Users and Permissions.**
Important Information	The User Management Entry Page consists of the following panes: ➤ **Groups/Users Pane.** Located on the left side of the page; displays the groups and users configured to access HP Business Availability Center. ➤ **Workflow Pane.** Displays introductory information about the User Management application, and a suggested workflow for configuring groups and users. **Note.** The Workflow Pane is visible when you enter the User Management application, or when you have chosen the Root group in the Groups/Users pane.
Included in Tasks	“Configure User Management - Workflow” on page 423
Useful Links	“User Management Main Page” on page 453

Groups/Users Pane

Description	Displays the list of users and groups of users configured to access HP Business Availability Center. **To access:** Select **Admin** > **Platform** > **Users and Permissions** > **Groups/Users.**
Important Information	The **Groups/Users Pane** is located on the left side of the User Management Main Page, and is visible on all views of the User Management application. The **Groups/Users Pane** contains the following tabs: ➤ **Browse.** Displays a list of configured users and groups, and enables you to create or delete users and groups. ➤ **Search.** Displays a table view of users and groups, and enables you to search for a user or group by any of the following criteria: ➤ Group name ➤ Login name ➤ User name ➤ User last login You can sort the columns by clicking on the column headers above the boxes. You can include wildcards (*) in your search. **Notes.** ➤ When selecting more than one user or group and modifying parameters, the changes take effect only for the first selected user. The exception is the Delete option, which deletes multiple users at once. ➤ When creating a group, the access permissions are automatically inherited by the group's users. ➤ When creating users while resting on a group, the users are automatically nested within that group.
Included in Tasks	"Configure User Management - Workflow" on page 423
Useful Links	"User Management Main Page" on page 453

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
	Click to create a user or group. Depending on whether you choose to create a user or group, the Create User or Create Group window opens.
	Click to copy the settings of an existing user or group to a new user or group.
	A configured user.
	A configured group of users.
	The root directory.
	Click to collapse or expand the hierarchy tree.
	Click and select **Group Mappings** to map local groups to groups configured on the LDAP server, or **Delete Obsolete Users** to delete HP Business Availability Center users no longer configured on the LDAP server. After selecting **Delete Obsolete Users,** you can remove mulitple users at once by holding the Ctrl button while selecting users. For details, see “Group Mappings Dialog Box” on page 451. **Note:** This button is enabled only if the appropriate settings are configured on the Infrastructure Settings page. For details on configuring these settings, see “Define an LDAP Authentication Strategy – Workflow” on page 86.

Create User Dialog Box

The following elements are included:

GUI Element (A–Z)	Description
Confirm Password	Re-enter the password specified in the **Password** field.
Email	Enter a valid email address. Note: The **Email** field is available for HP Software-as-a-Service customers only.
Login name	Enter a login name for the user, to be used when accessing HP Business Availability Center. **Notes:** ➤ The maximum number of characters you can enter is 50. All special characters are allowed except the following: " \ / [ ] : | < > + = ; , ? * ➤ The Login name appears as a tooltip when hovering over the user name in the Browse tab of the Groups/Users pane.
Password	Enter a password to be used when accessing HP Business Availability Center.
Time zone	Select the appropriate time zone, according to the user's location.

GUI Element (A–Z)	Description
User mode	Select the user mode for the user, 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.
User name	Enter a user name for the user. **Note:** The maximum number of characters you can enter is 50. All special characters are allowed except the following: " \ / [ ] : | < > + = ; , ? *

Create Group Dialog Box

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
Group Description	Enter a description for the group. **Note:** The group description is displayed as a tooltip when hovering on the group name in the Browse tab of the Groups/Users pane.
Group Name	Enter a name for the group.

Group Mappings Dialog Box

Description	Enables you to map groups configured in HP Business Availability Center to groups configured on the LDAP server. **To access:** Select **Admin** > **Platform** > **Users and Permissions**; in the Groups/Users pane, click the **LDAP Configuration** button  and select **Group Mappings**.
Important Information	➤ If you are switching from one LDAP server to another, ensure that you remove all existing group mappings from the original LDAP server before mapping to the new one. ➤ The Group Mappings dialog box consists of the following panes: ➤ **Corporate Directory Pane.** For details, see "Corporate Directory Pane" on page 452. ➤ **BAC Local Repository For Remote Group Pane: <group name>.** For details, see "BAC Local Repository for Remote Group: <group name> Pane" on page 453. ➤ **Local Groups to Remote Group Mappings.** Displays a table of the LDAP groups and the BAC groups that they are assigned to. The LDAP groups are displayed in the **Remote Group Name** column, and the BAC Groups are listed in the **Local Group Name** column.

Corporate Directory Pane

Description	Enables you to assign HP Business Availability Center groups to LDAP groups, and to list the users in the LDAP groups. **To access:** Select **Admin** > **Platform** > **Users and Permissions**; in the Groups/Users pane, click the **LDAP Configuration** button  and select **Group Mappings**.
Important Information	➤ To synchronize LDAP groups with HP Business Availability Center groups, click **Assign Groups** to open the Select Local Groups for Remote Group dialog box. ➤ To view the list of users associated with the respective LDAP groups, click **List Users**. You can also select either of these options by right clicking on the group. ➤ Once the LDAP groups have been mapped to the HP Business Availability Center groups, the HP Business Availability Center groups are managed only from the LDAP interface. This means that the following are fields are affected on the Users and Permissions interface: ➤ The **Create User** field is disabled. ➤ The **User Name** field is disabled. ➤ The **Password** field is invisible. ➤ The **Hierarchy** tab is enabled only for groups and not for users.

BAC Local Repository for Remote Group: <group name> Pane

Description	Displays the HP Business Availability Center mapped to the LDAP group selected in the Corporate Directory Pane, and enables you to remove the mapped HP Business Availability Center groups. **To access:** Select **Admin** > **Platform** > **Users and Permissions**; in the Groups/Users pane, click the **LDAP Configuration** button  and select **Group Mappings**.
Important Information	➤ To remove groups, select the group you want to remove and click **Remove Groups**. ➤ You can remove mulitple groups at once by holding the Ctrl button while selecting groups.

User Management Main Page

Description	Displays information on the groups and users configured to access HP Business Availability Center, including their respective permission levels. **To access:** Select **Admin** > **Platform** > **Users and Permissions.**
Important Information	The User Management Main Page consists of the following panes: ➤ **Groups/Users Pane.** Located on the left side of the page. ➤ **Information Pane.** Located on the right side of the page. For details, see “Information Pane” on page 454. **Note:** The Information Pane is visible only if you have selected a specific group or user in the Groups/Users Pane.
Included in Tasks	“Configure User Management - Workflow” on page 423
Useful Links	“User Management – Overview” on page 414 “Groups/Users Pane” on page 447 “Information Pane” on page 454

Information Pane

Description	Displays information on the specific user or group selected in the Groups/Users pane. **To access:** Select **Admin** > **Platform** > **Users and Permissions.**
Important Information	The Information pane is located on the right side of the User Management Main Page, and contains the following tabs: ➤ **General.** Displays general information about the user or group selected in the Groups/Users pane. **Note:** The fields on the General tab are identical to those in the Create User Dialog Box (for users), and the Create Group Dialog Box (for groups). For details, see "Groups/Users Pane" on page 447. ➤ **Permissions.** Displays the permission level for the specific user or group selected in the Groups/Users pane, as well as the HP Business Availability Center contexts that the permission levels apply to. For details, see "Permissions Tab" on page 457. ➤ **Hierarchy.** Displays the parent and child groups, if applicable, for the user or group selected in the Groups/Users pane. ➤ **Customization.** Enables you to set the default entry page and context for the user specified in the Groups/Users pane. **Note:** The Customization tab is visible only if you have selected a user in the **Groups/Users** pane.
Included in Tasks	"Configure User Management - Workflow" on page 423

General Tab

Description	Displays the parameters of the selected user or group. **To access:** Select **Admin** > **Platform** > **Users and Permissions** > **General** tab.
Important Information	➤ You can edit the user or group's parameters by editing the relevant fields on the General tab. ➤ The Group Name and Group Description fields appear only when a group is selected in the Groups/Users pane. All other fields appear only when a user is selected in the Groups/Users pane.
Included in Tasks	"Configure User Management - Workflow" on page 423
Useful Links	"User Management – Overview" on page 414 "Groups/Users Pane" on page 447 "Information Pane" on page 454

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Confirm Password	Re-enter the edited password that you entered in the Password field.
Group Description	The description of the group, as configured on the Create Group dialog box. **Note:** This field is optional.
Group Name	The name of the group, as configured on the Create Group dialog box.
Login name	The name that the user logs into HP Business Availability Center with. **Note:** The Login name cannot be changed.

GUI Element (A-Z)	Description
Password	The password of the selected user. **Note:** As a security precaution, this field appears blank on the General tab. To change the password, enter the new password and re-enter it in the Confirm Password field.
Time Zone	The time zone configured on the Create User dialog box, according to the user's location.
User Mode	The user mode, as configured on the Create User dialog box. Available options are: ➤ **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.
User name	The name of the user, as configured on the Create User dialog box.

Permissions Tab

Description	Enables you to apply permissions to groups and users for specific resources and instances of those resources that are defined in the system. **To access:** Select **Admin** > **Platform** > **Users and Permissions** > **Permissions** tab.
Important Information	➤ The Permissions tab is divided into the following areas: ➤ Resource tree pane in the center of the page ➤ Roles and operations pane on the right side of the page ➤ 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 “Hierarchy Tab” on page 464.
Included in Tasks	“Configure User Management - Workflow” on page 423 “Assign Permissions” on page 435
Useful Links	“Permissions Overview” on page 415

Resource Tree Pane

Description	Displays the instances and resources available within each HP Business Availability Center context that you set permissions for. **To access:** Select **Admin** > **Platform** > **Users and Permissions** > **Permissions** tab.
Important Information	The **Business Availability Center** resource refers to all contexts in HP Business Availability Center and can have only roles applied to it. 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. Following are the types of resources displayed in the Resource Tree pane: ➤ Resource with instances  ➤ Instances of a resource  ➤ Resource without instances  You can only select multiple resources when selecting instances. For information on instances, see "Resources and Resource Instances" on page 417.
Included in Tasks	"Assign Permissions" on page 435
Useful Links	"Understanding Permissions Resources" on page 417 "Resource Contexts" on page 459

The following elements are included:

GUI Element (A–Z)	Description
	An instance of a resource.
	A resource without instances.
	A resource that has instances (a resource collection).

GUI Element (A–Z)	Description
Select Context	Select an HP Business Availability Center context for which to configure permissions.
Settings	Click to apply specific permissions settings for configurations in your User Management session. Select from the following options: ➤ **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. **Note:** When you select the settings for applying permissions, the options selected apply only to the current HP Business Availability Center session.

Resource Contexts

The following contexts are included:

GUI Element (A–Z)	Description
CMDB	Includes the view resources for the CMDB in IT Universe.
Central Repository Service	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.

GUI Element (A–Z)	Description
Platform	Includes all the resources for administering the platform.
Problem Isolation	Includes all the resources for working with and administering Problem Isolation.
Production Analysis	Includes all the resources relating to Application Performance Lifecycle (APL).
Service Level Management	Includes the SLA resource.
System Availability Management	Includes the various SiteScope groups.
UCMDB WS API	Includes the extraction of data from the CMDB for use with third-party or custom tools or to write data to the database.
User Defined Reports	Includes the custom report, trend report, custom link, and Excel report resources.

Roles and Operations Pane

Description	Displays the predefined roles and operations configurable for groups and users in HP Business Availability Center. **To access:** Select **Admin** > **Platform** > **Users and Permissions** > **Permissions** tab.
Important Information	The Roles and Operations pane contains the following tabs: ➤ **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 which resources, see "User Management Roles" on page 467. ➤ **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 "User Management Operations" on page 486 **Note:** 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.
Included in Tasks	"Assign Permissions" on page 435
Useful Links	"Understanding Permissions Resources" on page 417 "User Management Roles" on page 467 "User Management Operations" on page 486

The following elements are included:

GUI Element (A–Z)	Description
Apply Permissions	Click to apply the permissions configured for the role or resource.
Grant	Click the check box to assign the specified role or operation to the group or user.

GUI Element (A–Z)	Description
Granted from Group/Role/Parent	Displays those permissions that have been granted from either a group, a predefined role, or a parent resource. **Notes:** ➤ 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.
Inherit	Select the check box in the **Inherit** column for the operation to be inherited to all the child resources within the selected resource. **Notes:** ➤ The **Inherit** check box is enabled only for selected resources. ➤ By default, the **Inherit** check box is selected when you assign an operation to specific resource instances . You can remove the **Inherit** option to prevent the operation from being inherited to all the child resources within the selected resource.
Operation	The operations that can be assigned to a group or user for the selected resource or instances. For details on the available operations, see “Operations” on page 463.
Role	The roles that can be assigned to a group or user for the selected resource or instances. For a description of the available roles, see “User Management User Interface” on page 445.

Operations

The following operation permissions can be assigned to users and groups. For a detailed description of how each operation applies to each resource, see "User Management Operations" on page 486.

GUI Element (A–Z)	Description
Add	Enables adding users to the system. **Note.** You cannot grant **Add** permission on an instance of a resource, only on the resource itself.
Change	Enables editing the selected resource or resource instance.
Delete	Enables removing the selected resource or resource instance.
Execute	Enables performing actions on the specified resource or resource instance.
Full Control	Enables performing all available operations, including granting and removing permissions, on the selected resource or resource instance. **Note.** 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.
Remove	Enables removing components on the specified resource or resource instance. **Note.** This operation is available only for HP Software-as-a-Service customers.
View	Enables viewing the selected resource or instance details. **Note.** To manage the permissions on a subresource, you must provide the user with at least **View** permissions on the selected resource's parent.

Hierarchy Tab

Description	Enables you to assign users to a group, unassign users from a group, or nest one group within another. **To access:** Select **Admin** > **Platform** > **Users and Permissions**, select a group or user from the **Groups/Users** pane, and click the **Hierarchy** tab.
Important Information	➤ The Hierarchy tab lists the groups that the selected group is nested under (parent groups), and the groups and users that are nested directly beneath the selected group (child groups). ➤ 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. ➤ When removing a nested group from its parent, the group itself is not deleted. ➤ When removing a parent group, the child groups and users are not deleted. ➤ The Hierarchy tab is invisible if there are no groups and users nested directly beneath the group or user selected in the **Groups/Users** pane. ➤ If HP Business Availability Center groups have been synchronized with groups on an external LDAP server, HP Business Availability Center users cannot be moved between groups and only groups appear on the interface. For details on synchronizing groups, see "Mapping Groups with LDAP" on page 104.
Included in Tasks	"Configure User Management - Workflow" on page 423 "Configure Group and User Hierarchy" on page 437
Useful Links	"Group and User Hierarchy" on page 420

The following elements are included:

GUI Element (A–Z)	Description
	Denotes a group that the selected group or user is nested under.
	Denotes a user that is nested beneath the selected group.
Child Groups and Users	Displays the groups and users that are nested directly beneath the group selected in the **Groups/Users** pane.
Edit Child Groups and Users	Click to open the Edit Child Groups and Users window and nest or remove groups and users from the selected group. For details, see "Edit Child Groups and Users Dialog Box" on page 465. **Note:** This button is displayed only when selecting a group in the Groups/Users pane.
Parent Groups	Displays the groups that the group or user selected in the **Groups/Users** pane is directly nested under.

Edit Child Groups and Users Dialog Box

The following elements are included:

GUI Element (A–Z)	Description
	Click to move the group or user to the Child Groups and Users pane and nest the group or user under the specified group.
	Click to move the group or user to the Groups/Users pane and remove the group or user from being nested beneath the specified group.
Child Groups and Users	Select a group or user you want to remove from the specified group.
Groups/Users	Select a group or user you want to nest under the specified group.

Customization Tab

Description	Enables you to select the page users see when entering HP Business Availability Center, and choose the menu items available on pages throughout HP Business Availability Center. **To access:** Select **Admin** > **Platform** > **Users and Permissions**, select a user from the **Groups/Users** pane, and click the **Customization** tab.
Important Information	The Customization tab is enabled only when a user has been selected in the Groups/Users pane on the left side of the page.
Included in Tasks	"Configure User Management - Workflow" on page 423 "Customize User Menus" on page 439
Useful Links	"Customizing User Menus" on page 422

The following elements are included:

GUI Element (A–Z)	Description
Contexts	Select an HP Business Availability Center context. You can perform the following actions on the context: ➤ Select pages and tabs in the Pages and Tabs pane to be visible for the specified user. ➤ Click the **Set as Default Entry Context** button to make it the context that is displayed when the user logs into HP Business Availability Center.
Pages and Tabs	➤ Select the pages and tabs you want to be visible for the HP Business Availability Center context selected in the Contexts pane. ➤ Assign a page or tab as the default page that opens for the context selected in the Contexts pane.

GUI Element (A–Z)	Description
Set as Default Entry Context	Click to set the selected context in the Contexts pane as the entry context that is displayed when the specified user logs into HP Business Availability Center. Note: The **Default Entry Context** icon  appears next to the specified context.
Set as Default Entry Page	Click to assign the specified page or tab as the default page that opens for the context selected in the Contexts pane. **Note:** The **Default Entry Page** icon  appears next to the specified page or tab.

User Management Roles

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 Software-as-a-Service customers only and are listed as such.

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.

Important: The default superuser does not have permissions to write to Business Availability Center from the UCMDB WS API. Specific roles exist for that purpose. For details, see “CmdbOpenApiQuery” on page 478 and “CmdbOpenApiUpdate” on page 477.

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 468).

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

CmdbOpenApiImpact

This role enables users to impact operations on the CMDB.

Context	Resource	Allowed Operation
UCMDB WS 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.

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
UCMDB WS API	Cmdb Open API	View
		Change

CmdbOpenApiClassModel

This role enables users to perform operations on CITs.

Context	Resource	Allowed Operation
UCMDB WS API	Cmdb Open API	View
		Change

Customer Superuser

Note: This role can be applied to HP Software-as-a-Service 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 Software-as-a-Service 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 Software-as-a-Service 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 Software-as-a-Service 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

Problem Isolation User

The Problem Isolation User role can be applied only to the Problem Isolation Application resource.

A Problem Isolation User can only view resources within the Problem Isolation application, 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 Problem Isolation User has no access to those resources.

Context	Resource	Allowed Operation
Problem Isolation	Problem Isolation Application	View

Problem Isolation Advanced User

The Problem Isolation Advanced User role can be applied only to the Problem Isolation Application resource.

A Problem Isolation Advanced User can view and run on demand monitors and revalidate problems, as well as view, change, add, or delete entries in the Problem list.

Context	Resource	Allowed Operation
Problem Isolation	Problem Isolation Application	View
		Add
		Change
		Delete

Problem Isolation Administrator

The Problem Isolation Administrator role can be applied only to the Problem Isolation Application resource.

A Problem Isolation Administrator has full permissions on all areas of Problem Isolation, and has full control over all resources and resource instances.

Context	Resource	Allowed Operation
Problem Isolation	Problem Isolation Application	View
		Add
		Change
		Delete
		Execute
		Full Control

User Management Operations

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.

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.

Monitors

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 (HP Software-as-a-Service only) to Business Process profiles.
	Change	Enables editing transaction monitor, WebTrace monitor, and single URL monitor (HP Software-as-a-Service only) properties.
	View	Enables viewing transaction monitor, WebTrace monitor, and single URL monitor (HP Software-as-a-Service only) properties.
	Delete	Enables deleting transaction monitors, WebTrace monitors, and single URL monitors (HP Software-as-a-Service only) from the profile.
	Full Control	Enables performing all available operations on transaction monitors, WebTrace monitors, and single URL monitors (HP Software-as-a-Service 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 Software-as-a-Service 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 Software-as-a-Service 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 Types Measurement 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 Software-as-a-Service 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 Software-as-a-Service 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.

Resources	Operation	Description
System Tickets (HP Software-as-a-Service 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.

Problem Isolation

Use the Problem Isolation context to assign permissions for accessing the Problem Isolation application. Problem Isolation enables you to isolate and manage enterprise problems discovered in HP Business Availability Center, and to identify likely suspects, to help find the root cause of a problem.

Resources	Operation	Description
Problem Isolation Application	View	Enables viewing of all areas of Problem Isolation.
	Full Control	Enables performing all available operations in Problem Isolation.
Problem Isolation Administration	Change	Enables modifying of On-demand monitors Monitor Profiles.
	View	Enables viewing of On-demand Monitors and Monitor Profiles.
	Full Control	Enables performing all available operations for On-demand Monitors and Monitor Profiles.

Resources	Operation	Description
Problem List	Add	Enables adding a problem to the Problem list.
	Change	Enables modifying an existing problem on the Problem list.
	Delete	Enables deleting an existing problem from the Problem list.
	Full Control	Enables performing all available operations on the Problem list.
Problem Isolation On Demand Manual Run	Execute	Enables manually running On-demand Monitors to check the status of Suspect Configuration Items.
	Full Control	Enables performing all available operations on the manual running of On-demand Monitors which check the status of Suspect Configuration Items.
Problem Isolation Revalidation Transactions Manual Run	Execute	Revalidates the transactions affected by the Suspect Configuration Item, to ensure that the specified problems still exist.
	Full Control	Enables performing all available operations on the revalidation of transactions affected by the Suspect Configuration Item.

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> **Note:** Groups are listed individually, as you can configure different permission levels for each group.	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 reports contained within that group, and creating SiteScope Over Time reports.
	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 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.

Resources	Operation	Description
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.
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.

22

Personal Settings

This chapter provides information on Configuring Personal Settings within HP Business Availability Center.

This chapter includes:

Concepts

Tasks

Reference

Personal Settings Overview

Personal settings enable customization of the way HP Business Availability Center presents information to individual users.

Individual users can configure personal settings to customize their specific user-related behavior of HP Business Availability Center.

The Personal Settings tab contains the following options:

- **General Settings.** For details, see "General Settings" on page 518.
- **Menu Customization.** For details, see "Menu Customization" on page 518.

General Settings

On the General Settings tab, you can configure the following personal settings:

- User name
- User mode
- Time zone used when displaying reports
- Password
- Refresh rate of reports
- Customized menu items

For details on the updating these settings via the user interface for General Settings, see "General Settings Page" on page 521.

Menu Customization

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. For details on the Menu Customization User Interface, see "Menu Customization Page" on page 522.

Customize User Menus

This task describes how to customize the page you see when entering HP Business Availability Center, and choose the menu items available on pages throughout HP Business Availability Center.

This task includes the following steps:

1 Assign a Default Context

Select a context from the Contexts pane that you want to be the default entry context you see when logging into HP Business Availability Center, and click **Set as Default Entry Context**. For details on the Contexts pane, see "Menu Customization Page" on page 522.

2 Select Context Pages and Tabs

In the Pages and Tabs pane, select the context of the pages and tabs that you want to be visible on the selected context for the user. Clear the check boxes of the pages and tabs that you want hidden from the user.

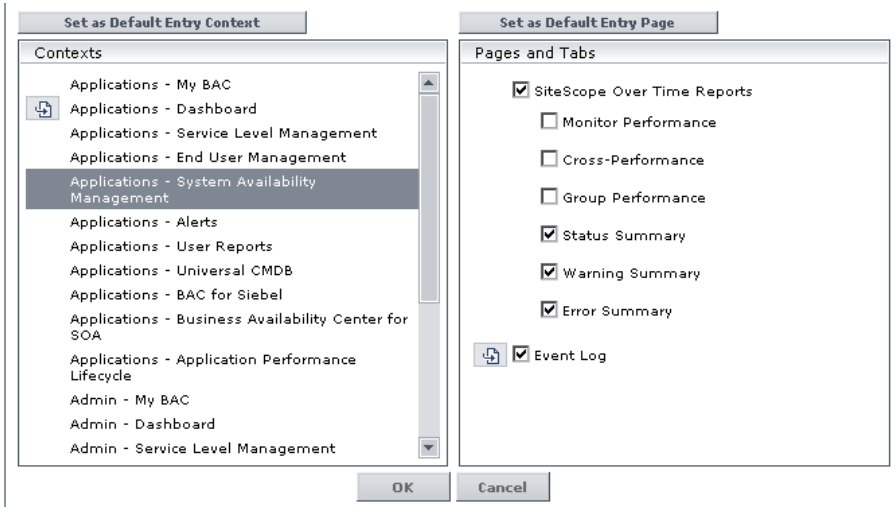
3 Assign a Default Entry Page

Select a page or tab to be the default entry page for the selected context, and click **Set as Default Entry Page**.

4 Results

The default entry icon appears next to the default entry context and page. Pages and tabs visible to the user are selected in the Pages and Tabs pane. Pages and tabs hidden from the user are cleared in the Pages and Tabs pane.

Example



Personal Settings User Interface

This section describes:

- General Settings Page on page 521
- Menu Customization Page on page 522

General Settings Page

Description	Enables you to configure the user name, user mode, time zone, password, and refresh rate settings. **To access:** Select **Admin** > **Personal Settings** > **General Settings**.
Important Information	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.
Useful Links	"General Settings" on page 518

The following elements are included:

GUI Element (A–Z)	Description
Confirm Password	Re-enter the password specified in the **Password** field.
Email	Enter a valid email address. Note: The **Email** field is available for HP Software-as-a-Service customers only.
Login name	The name used to login to HP Business Availability Center. **Note:** You cannot change the entry in this field.
Old Password	Enter the existing password.
Password	Enter a password to be used when accessing HP Business Availability Center.
Select auto-refresh rate	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. Note: This setting is active only when in the **Past day** or **Past hour** time resolution in reports.
Time zone	Select the appropriate time zone, according to the user's location.

GUI Element (A–Z)	Description
User mode	Select the user mode for the user, 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. For details on user types, see "KPIs for User Modes" in *Using Dashboard*. ➤ **Business User.** Enables the user to view the business version of KPIs. For details on user types, see "KPIs for User Modes" in *Using Dashboard*.
User name	Enter a user name for the user. **Notes:** ➤ The maximum number of characters you can enter is 50. ➤ All special characters are allowed except the following: " \ / [ ] : | < > + = ; , ? *

Menu Customization Page

Description	Enables you to: ➤ 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. **To access:** Select **Admin** > **Personal Settings** > **Menu Customization.**

Included in Tasks	"Customize User Menus" on page 519
Useful Links	"Personal Settings Overview" on page 517

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
Contexts	Select an HP Business Availability Center context. You can perform the following actions on the context: ➤ Select pages and tabs in the Pages and Tabs pane to be visible for the specified user. ➤ Click the **Set as Default Entry Context** button to make it the context that is displayed when the user logs into HP Business Availability Center.
Pages and Tabs	➤ Select the pages and tabs you want to be visible for the HP Business Availability Center context selected in the Contexts pane. ➤ Assign a page or tab as the default page that opens for the context selected in the Contexts pane.
Set as Default Entry Context	Click to set the selected context in the Contexts pane as the entry context that is displayed when the specified user logs into HP Business Availability Center. Note: The **Default Entry Context** icon  appears next to the specified context.
Set as Default Entry Page	Click to assign the specified page or tab as the default page that opens for the context selected in the Contexts pane. **Note:** The **Default Entry Page** icon  appears next to the specified page or tab.

Index

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V