HP Business Service Management

for the Windows operating system

Software Version: 9.00

Platform Administration

Document Release Date: July 2010

Software Release Date: July 2010

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.

Copyright Notices

Trademark Notices

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

AMD and the AMD Arrow symbol are trademarks of Advanced Micro Devices, Inc.

Google™ and Google Maps™ are trademarks of Google Inc.

Intel®, Itanium®, 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®, Windows® XP, and Windows Vista® are U.S. registered trademarks of Microsoft Corporation.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Acknowledgements

This product includes software developed by the Apache Software Foundation (**http://www.apache.org**).

This product includes software developed by the JDOM Project (**http://www.jdom.org**).

This product includes software developed by the MX4J project (**http://mx4j.sourceforge.net**).

Documentation Updates

The title page of this document 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

This site requires that you register for an HP Passport and sign-in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support web site at:

http://www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web 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 register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Table of Contents

PART I: ACCESSING AND NAVIGATING HP BUSINESS SERVICE MANAGEMENT

PART II: SETUP AND MAINTENANCE

PART III: DATA ENRICHMENT

PART IV: USERS, PERMISSIONS, AND RECIPIENTS

PART V: REPORT AND ALERT ADMIN

Welcome to This Guide

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

How This Guide Is Organized

The guide contains the following parts:

Part I Accessing and Navigating HP Business Service Management

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

Part II Setup and Maintenance

Describes how to download components, manage licenses and deployment, administrate the profile and management databases, enable data purging, configure the infrastructure settings, view the audit log, and troubleshoot working in a non-English language.

Part III Data Enrichment

Describes how to create location CIs; create, export and import content packs; and how to schedule downtime events.

Part IV Users, Permissions, and Recipients

Describes how to create and manage users and user groups, 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. Also describes how to configure HP Business Service Management to work with authentication strategies.

Part V Report and Alert Admin

Describes how to monitor report schedules, provides an introduction to reports, and describes how to create and manage notification templates for alerts.

Who Should Read This Guide

This guide is intended for the following users of HP Business Service Management:

- HP Business Service Management administrators
- HP Business Service Management platform administrators

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

How Do I Find the Information That I Need?

This guide is part of the HP Business Service Management Documentation Library. This Documentation Library provides a single point of access for all Business Service Management documentation.

You can access the Documentation Library by doing the following:

- In Business Service Management, select **Help** > **Documentation Library**.
- From a Business Service Management Gateway Server machine, select **Start** > **Programs** > **HP Business Service Management** > **Documentation**.

Topic Types

Within this guide, each subject area is organized into topics. A topic contains a distinct module of information for a subject. The topics are generally classified according to the type of information they contain.

This structure is designed to create easier access to specific information by dividing the documentation into the different types of information you may need at different times.

Three main topic types are in use: **Concepts**, **Tasks**, and **Reference**. The topic types are differentiated visually using icons.

Topic Type	Description	Usage
Concepts	Background, descriptive, or conceptual information.	Learn general information about what a feature does.
Tasks	**Instructional Tasks.** Step-by-step guidance to help you work with the application and accomplish your goals. Some task steps include examples, using sample data. Task steps can be with or without numbering: ➤ **Numbered steps.** Tasks that are performed by following each step in consecutive order. ➤ **Non-numbered steps.** A list of self-contained operations that you can perform in any order.	➤ Learn about the overall workflow of a task. ➤ Follow the steps listed in a numbered task to complete a task. ➤ Perform independent operations by completing steps in a non-numbered task.
	Use-case Scenario Tasks. Examples of how to perform a task for a specific situation.	Learn how a task could be performed in a realistic scenario.

Topic Type	Description	Usage
Reference 📌	**General Reference**. Detailed lists and explanations of reference-oriented material.	Look up a specific piece of reference information relevant to a particular context.
	User Interface Reference. Specialized reference topics that describe a particular user interface in detail. Selecting **Help on this page** from the Help menu in the product generally open the user interface topics.	Look up specific information about what to enter or how to use one or more specific user interface elements, such as a window, dialog box, or wizard.
Troubleshooting and Limitations 🔍	**Troubleshooting and Limitations**. Specialized reference topics that describe commonly encountered problems and their solutions, and list limitations of a feature or product area.	Increase your awareness of important issues before working with a feature, or if you encounter usability problems in the software.

Additional Online Resources

Troubleshooting & Knowledge Base accesses the Troubleshooting page on the HP Software Support Web site where you can search the Self-solve knowledge base. Choose **Help** > **Troubleshooting & Knowledge Base**. The URL for this Web site is http://h20230.www2.hp.com/troubleshooting.jsp.

HP Software Support accesses the HP Software Support Web site. This site enables you to browse the Self-solve knowledge base. You can also post to and search user discussion forums, submit support requests, download patches and updated documentation, and more. Choose **Help** > **HP Software Support**. The URL for this Web site is www.hp.com/go/hpsoftwaresupport.

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 user ID, go to:

http://h20229.www2.hp.com/passport-registration.html

HP Software Web site accesses the HP Software Web site. This site provides you with the most up-to-date information on HP Software products. This includes new software releases, seminars and trade shows, customer support, and more. Choose **Help** > **HP Software Web site**. The URL for this Web site is www.hp.com/go/software.

Documentation Updates

HP Software is continually updating its product documentation with new information.

To check for recent updates, or to verify that you are using the most recent edition of a document, go to the HP Software Product Manuals Web site (http://h20230.www2.hp.com/selfsolve/manuals).

Part I

Accessing and Navigating HP Business Service Management

1

Logging Into HP Business Service Management

This chapter includes:

Concepts

Tasks

Reference

Concepts

Logging In and Out - Overview

You access HP Business Service Management using a supported Web browser, from any computer with a network connection (intranet or Internet) to the HP Business Service Management servers. The level of access granted to a user depends on the user's permissions. For details on granting user permissions, see "How to Assign Permissions" on page 269.

HP Business Service Management is by default configured with Lightweight Single Sign-On (LW-SSO). LW-SSO enables you to login to HP Business Service Management 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 Service Management, see "Logging into BSM with Lightweight Single Sign-On" on page 22.

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

Logging into BSM with Lightweight Single Sign-On

When Lightweight Single Sign-On Authentication Support (LW-SSO) is enabled, you must ensure that the other applications in the Single Sign-On environment have LW-SSO enabled and are working with the same initString.

If you do not require Single Sign-On for HP Business Service Management, it is recommended that you disable LW-SSO. You can disable LW-SSO using one of the following utilities:

- **The Authentication Strategy Wizard.** For details on using the Authentication Strategy Wizard, see "Authentication Wizard" on page 400.

- **The JMX console.** For details on disabling LW-SSO through the JMX console, see "Resetting LDAP/SSO Settings via the JMX Console" on page 45.

Once LW-SSO is disabled, the default HP Business Service Management authentication service is automatically enabled. When either LW-SSO is disabled, or the Identity Management Single Sign-On (IDM-SSO) or Lightweight Directory Access Protocol (LDAP) authentication strategies are enabled, you do not need to enter the syntax **.<domain_name>** in the HP Business Service Management login URL (**http://<server_name>.<domain_name>/HPBSM**).

For details on implementing either an IDM-SSO or LDAP authentication strategy, see "Authentication Wizard" on page 400.

For details on the requirements for logging into HP Business Service Management, see "How to Log In and Out" on page 29.

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 Service Management.

Advanced login options include:

- **Automatic login.** You can configure HP Business Service Management so that after the initial login, you do not have to enter a login name and password, but 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 32.
- **Direct login capabilities.** You can guide another user to a specific target page in HP Business Service Management. For details, see "Use the Link to This Page Option to Open a Specific Page" on page 33.
- **Limiting login access.** You can limit the number of machines accessing HP Business Service Management using the same login name. For details, see "Limit Access by Different Machines Using the Same Login Name" on page 33.

- **Linking to specific pages.** You can guide another user to a specific target page in HP Business Service Management by creating a URL with a user name, password, and information about the target page. For details, see "Linking to a Specific Page" on page 24.

Linking to a Specific Page

You can guide another user to a specific target page in HP Business Service Management by creating a URL with a user name, password, and information about the target page.

Depending on how you use the **Link to this page** option, 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 Service Management 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 the **Link to this page** option selecting **Use Credentials** of a regular user (who is not authorized to view Infrastructure Settings). 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 Service Management 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.

For details on the user interface for the **Link to this page** option, see "Link to This Page Window" on page 38.

Creating a Direct Link in the ODB

You can create a link to a specific target page in the ODB using the Direct Links feature. For details on Direct Links, see "Create a URL for a Direct Link" in *Modeling Guide*.

Using the JMX Console

The JMX console comes embedded in HP Business Service Management, and enables you to:

- perform management operations
- view performance of processes
- troubleshoot problematic areas of HP Business Service Management

To access the JMX console, you must first enter the relevant URL (**http://<Gateway or Data Processing server name>:8080/jmx-console/**, where **Gateway or Data Processing server name** is the name of the machine on which HP Business Service Management is running), and enter the JMX console authentication credentials.

The credentials to access the JMX console are configured when installing BSM and running the Setup and Database Configuration utility. You can change the password but not the user name. For details on changing the JMX password, see "How to Change the JMX Password" on page 34.

Note: The login name cannot be changed.

You can monitor the availability of your HP Business Service Management system by accessing the following file, located on either the Gateway or Data Processing server:

<HPBSM root directory>\AppServer\webapps\myStatus.war\myStatus.html

On a Windows operating system, this file is also accessible through the following Start Menu path:

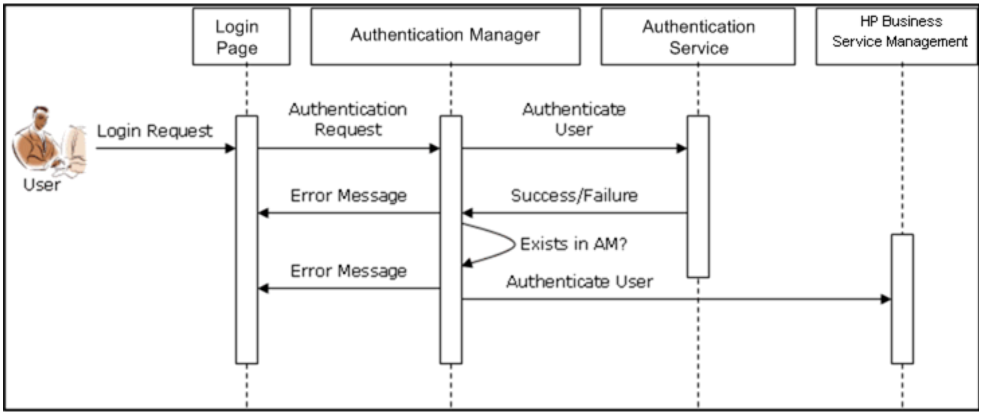
Start > **Programs** > **HP Business Service Management** > **Administration** > **HP Business Service Management Server Status**

You must enter your JMX username and password to access this page.

You can configure the JMX console to work with SSL, to encrypt JMX data for added security. For details, see "Configuring the Application Server JMX Console to Work With SSL" in the *HP Business Service Management Hardening Guide* PDF.

HP Business Service Management Login Flow

This section describes the general authentication flow in HP Business Service Management:



- 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 Service Management Authentication Manager together with the strategy name, principal, and credentials. You configure an authentication strategy in the Authentication Strategy wizard. For details, see "Authentication Wizard" on page 400.
- 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 Service Management verifies the user according to the selected strategy.

Note: When creating users in HP Business Service Management, make sure that user names match the user names in the relevant strategy database. A user can not login to HP Business Service Management if the name does not match.

➤ If the user passes the previous steps, they are considered an authenticated user. The HP Business Service Management 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 content and error message depend on which strategy you are implementing.

Tasks

How to Log In and Out

You log into HP Business Service Management from the login page.

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

To access the HP Business Service Management login page and log in:

1. In a Web browser, enter the URL **http://<server_name>.<domain_name>/HPBSM**, where **server_name** is the name or IP address of the HP Business Service Management Gateway 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 Service Management 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 Service Management 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**.

   Caution:

   ➤ It is recommended that the system superuser change this password immediately to prevent unauthorized entry. For details on the user interface for changing the password, see "General Tab (User Management)" on page 338.

   ➤ The login name cannot be changed.

For details on the user interface for creating users in the HP Business Service Management system, see "Create User Dialog Box" on page 335.

For details on login authentication strategies that can be used in HP Business Service Management, see "Set Up the Authentication Strategies" on page 393.

For login troubleshooting information, see "Troubleshooting and Limitations" on page 40.

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

To log out of HP Business Service Management:

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

Note: Clicking **Logout** 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.

How to Use Advanced Login Options

You can choose to enable advanced login options for HP Business Service Management. For details, see "Advanced Login Options" on page 23.

This section also includes:

➤ "Enable Automatic Login in the Login Page" on page 31

➤ "Modify Automatic Login Settings - Optional" on page 32

➤ "Use the Automatic Login URL Mechanism" on page 32

➤ "Use the Link to This Page Option to Open a Specific Page" on page 33

- "Limit Access by Different Machines Using the Same Login Name" on page 33
- "Open an Application Page Using a URL" on page 34

Enable Automatic Login in the Login Page

This task describes how to enable automatic login to HP Business Service Management.

1 On the HP Business Service Management login page, select the option to **Remember my login name and password for 14 days**.

Caution: This could be considered a security risk and should be used with caution.

2 When completing your session, close the browser window. Do not click **Logout** at the top of the page.

Clicking **Logout** disables the automatic login option and requires the login name and password to be entered when again accessing HP Business Service Management.

Note: When automatic login is enabled from the login page and the user enters the URL to access HP Business Service Management,

- 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.

Modify Automatic Login Settings - Optional

You can optionally modify the automatic login settings that you have configured.

1 Navigate to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings.**

2 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 the automatic login option from appearing on the login page by setting the **Enable automatic login** value to **false** (the default value is **true**).

   ➤ configure the number of machines that can simultaneously access HP Business Service Management using the same login name by configuring the **Maximum machines per login name** value (the default value is **0**). A value of 0 means that the number of logins is unlimited.

   For details on using the Infrastructure Settings page, see "Infrastructure Settings Manager Page" on page 130.

Use the Automatic Login URL Mechanism

You can use a special URL, containing several parameters (including login name and password), to access HP Business Service Management and automatically log in.

Caution: Though convenient, this method is not secure since the password is not encrypted in the URL.

In a Web browser, enter the URL **http://<server_name>.<domain_name>/<HPBSM root directory>/TopazSiteServlet?autologin=yes&strategy Name=Topaz&requestType=login&userlogin=<loginname>&userpassword=<password>&createSession=true**, where:

- **server_name** represents the name of the HP Business Service Management server
- **domain_name** represents the name of the user's domain according to his network configuration
- **loginname** and **userpassword** represent the login name and password of a user defined in HP Business Service Management

To enable direct entry to HP Business Service Management, bookmark this URL.

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 Service Management. **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 Service Management login page because the URL supplies the user name and password information. For details, see "Link to This Page Window" on page 38.

Limit Access by Different Machines Using the Same Login Name

HP Business Service Management can be accessed using the same login name from different machines. The number of machines accessing HP Business Service Management 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 you want to enable to access HP Business Service Management 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 Service Management, 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 45.

Open an Application Page Using a URL

You can open a specific HP Business Service Management page directly in your browser by using a URL. For details, see "Linking to a Specific Page" on page 24.

How to Change the JMX Password

This task describes how to change the JMX password.

1 Stop the HP Business Service Management Gateway or Data Processing server.

2 Run the appropriate file, depending on the operating system in use, on either the Gateway or Data Processing server:

Operating System	File Name
Windows	<HPBSM root directory>\tools\jmx\changeCredentials.bat
Solaris	<HPBSM root directory>\tools\jmx\changeCredentials.sh

The Change Password dialog box opens, where you enter and confirm your new password. The password change is registered and encrypted on either the Gateway or Data Processing server.

3 Restart HP Business Service Management.

Note: The login name cannot be changed.

How to Create a Keystore Certificate

This task describes how to create a keystore certificate if you do not already have one.

1 Open a **cmd.exe** window.

2 Run the following command to generate the keystore file:

```
keytool -genkey -dname
"CN=YourName,OU=yourDepartment,O=yourCompanyName,L=yourLocation
,S=yourState, C=yourCountryCode" -alias <youralias> -keypass changeit -
keystore "<keystore location>" -storepass changeit -keyalg "RSA" -validity
360
```

For example:

```
keytool -genkey -dname "CN=John Smith, OU=FND, O=HP, L=Los Angeles,
ST=Unknown, C=USA" -alias john -keypass mypassword -keystore
"D:\HPBSM\JRE\lib\security\cacerts" -storepass changeit -keyalg "RSA" -
validity 360
```

3 The keystore certificate is generated in the location you specified in the -keystore parameter.

4 Restart HP Business Service Management.

How to Track Login Attempts and Logged In Users

To track who has attempted to log in to the system:

See <**HPBSM root directory**>**\log\EJBContainer\UserActions.servlets.log**.

The appender for this file is located in <**HPBSM root directory**>**\conf\core\Tools\log4j\EJB\topaz.properties**

To display a list of users currently logged in to the system:

1 Open the JMX console on this machine. (For detailed instructions, see "Using the JMX Console" on page 25.)

2 Under the **Topaz** section, select **service=Active Topaz Sessions**.

3 Invoke the java.lang.String showActiveSessions() operation.

Reference

Security Notes and Precautions

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

- The user name and password in the URL are encrypted so that no login information is ever revealed.
- Sending encrypted information by email still entails a security risk, since the mail system can be breached. If the email is intercepted, access to HP Business Service Management 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 Service Management.

Logging Into HP Business Service Management User Interface

This section includes (in alphabetical order):

- HP Business Service Management Login Page on page 37
- Link to This Page Window on page 38

HP Business Service Management Login Page

This page enables you to log in to HP Business Service Management.

To access	In a Web browser, enter the URL **http://<server_name>.<domain_name>/<HPBSM root directory>**, where **server_name** is the name or IP address of the HP Business Service Management 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.
Relevant tasks	"How to Log In and Out" on page 29
See also	"Logging into BSM with Lightweight Single Sign-On" on page 22

User interface elements are described below:

UI Elements (A-Z)	Description
Login Name	Enter the relevant login name to access HP Business Service Management.

UI Elements (A-Z)	Description
Password	Enter the relevant password to access HP Business Service Management.
Remember my login name and password for 14 days	Select to enable HP Business Service Management 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

This window enables you to guide another user to a specific target page in HP Business Service Management.

To access	Select **Admin** > **Link to this page.**
Relevant tasks	"How to Use Advanced Login Options" on page 30
See also	"Advanced Login Options" on page 23 "Create a URL for a Direct Link" in *Modeling Guide*.

User interface elements are described below:

UI Elements (A-Z)	Description
Cancel	Cancels the Link to this page operation.
Create Link	Creates a URL for the user to enter into their browser and displays the specified HP Business Service Management page. **Note:** If you select this option after selecting **No Credentials**, and you want to invoke the login URL on the same local machine you created it on, you must log out of HP Business Service Management.
Confirm password	Re-enter the password entered in the **Password** field.

UI Elements (A-Z)	Description
Copy to Clipboard	Copies the content of the **Link** field to the clipboard. **Note:** If you use the Firefox browser, you must change your security settings for this option to work. Enter about:config in the browser's search window, locate the **signed.applets.codebase_principal_support** option, and set it to **true**.
Generate HTML	Generates an HTML page for the specified HP Business Service Management page. **Note:** If you select this option after selecting **No Credentials**, and you want to invoke the login URL on the same local machine you created it on, you must log out of HP Business Service Management.
Link	The URL that the receiver uses to access the specified HP Business Service Management 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.

Troubleshooting and Limitations

This section describes troubleshooting and limitations for logging into HP Business Service Management.

This section contains the following topics:

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 Service Management failed to connect to the jboss application server running on the Gateway server. This may be due to: ➤ the jboss server being down ➤ problems with the HP Business Service Management 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 Service Management application.
LI003	The management database is 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 Service Management 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 "Port Usage" in the *HP Business Service Management Deployment Guide* PDF.

Error No.	Problem/Possible Cause(s)	Solution(s)
LI005	The HP Business Service Management 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://<Gateway or Data Processing 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 Service Management login fails or hangs.	**Solution 3:** Ensure that the user has appropriate permissions to access HP Business Service Management. For details on user permissions, see "Permissions Overview" on page 246. **Solution 4:** Verify that an authentication strategy has been configured correctly. For details on authentication strategies, see "Set Up the Authentication Strategies" on page 393.
LI006	The HP Business Service Management 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 Service Management servers	**Solution 1:** Ensure that the client Web browser is set to accept cookies from HP Business Service Management servers. **Solution 2:** Ensure that there are no underscore characters (_) in the names of the machines running the HP Business Service Management servers. If there are, either rename the server or use the server's IP address when accessing the machine. For example, to access HP Business Service Management, use http://111.222.33.44/<HPBSM root directory> instead of http://my_server/<HPBSM root directory>

Error No.	Problem/Possible Cause(s)	Solution(s)
LI007	The HP Business Service Management login fails. This is because the maximum number has been reached of concurrent logins from different machines that access HP Business Service Management using the same login name.	**Solution 1:** Log out of the instances of HP Business Service Management 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.

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 Service Management is that of the Gateway or Proxy server and not the IP of the client. As a result, HP Business Service Management treats each client as coming from the same IP. Since the number of logins from the same machine (IP) is not limited, all of the clients can login to HP Business Service Management, even though they originate from different IPs.

Configuring the JMX Console to Work with SSL Limitations

After configuring the JMX console to work with SSL, it is not possible to access the \<**HPBSM root directory**>**AppServer****webapps****myStatus.war****myStatus.html** page to view the availability of HP Business Service Management.

Resetting LDAP/SSO Settings via the JMX Console

If your LDAP or SSO settings have not been configured properly, you may be prevented from accessing HP Business Service Management. 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 Service Management:

To reset LDAP/SSO settings via the JMX console:

1. Enter the URL of the JMX console (**http://<Gateway or Data Processing 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

Navigating and Using HP Business Service Management

This chapter includes:

Concepts

Tasks

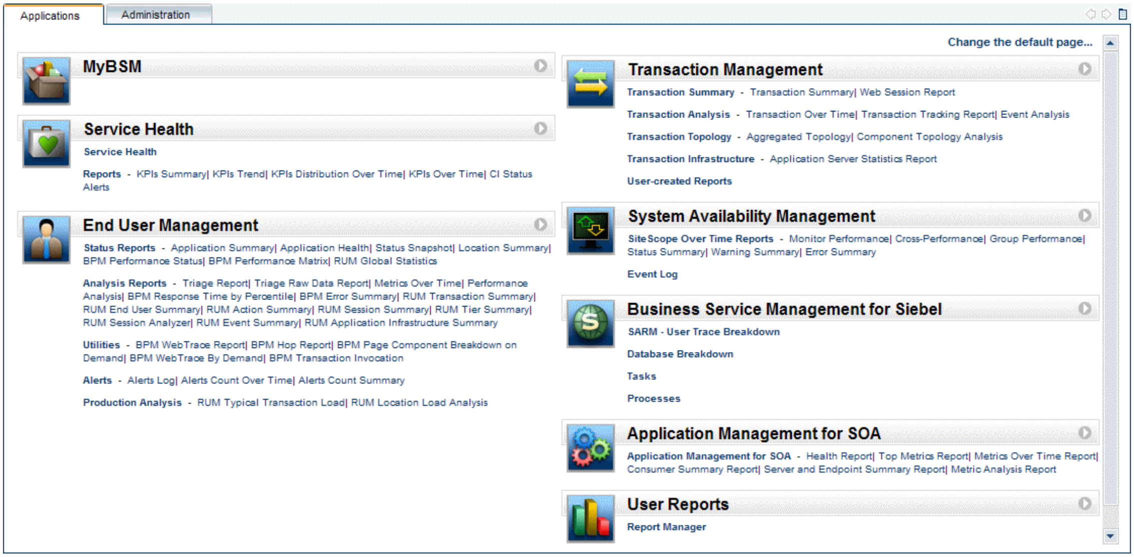
Reference

Concepts

Navigating HP Business Service Management

HP Business Service Management runs in a Web browser. You move around HP Business Service Management 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 Service Management. If the default page is changed after login, you can access the Site Map by clicking the **Site Map** link, either on the top menu or from the Help menu.



Applications | Administration

Change the default page...

MyBSM

Service Health

Service Health

Reports - KPIs Summary| KPIs Trend| KPIs Distribution Over Time| KPIs Over Time| CI Status Alerts

End User Management

Status Reports - Application Summary| Application Health| Status Snapshot| Location Summary| BPM Performance Status| BPM Performance Matrix| RUM Global Statistics

Analysis Reports - Triage Report| Triage Raw Data Report| Metrics Over Time| Performance Analysis| BPM Response Time by Percentile| BPM Error Summary| RUM Transaction Summary| RUM End User Summary| RUM Action Summary| RUM Session Summary| RUM Tier Summary| RUM Session Analyzer| RUM Event Summary| RUM Application Infrastructure Summary

Utilities - BPM WebTrace Report| BPM Hop Report| BPM Page Component Breakdown on Demand| BPM WebTrace By Demand| BPM Transaction Invocation

Alerts - Alerts Log| Alerts Count Over Time| Alerts Count Summary

Production Analysis - RUM Typical Transaction Load| RUM Location Load Analysis

Transaction Management

Transaction Summary - Transaction Summary| Web Session Report

Transaction Analysis - Transaction Over Time| Transaction Tracking Report| Event Analysis

Transaction Topology - Aggregated Topology| Component Topology Analysis

Transaction Infrastructure - Application Server Statistics Report

User-created Reports

System Availability Management

SiteScope Over Time Reports - Monitor Performance| Cross-Performance| Group Performance| Status Summary| Warning Summary| Error Summary

Event Log

Business Service Management for Siebel

SARM - User Trace Breakdown

Database Breakdown

Tasks

Processes

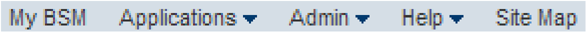
Application Management for SOA

Application Management for SOA - Health Report| Top Metrics Report| Metrics Over Time Report| Consumer Summary Report| Server and Endpoint Summary Report| Metric Analysis Report

User Reports

Report Manager

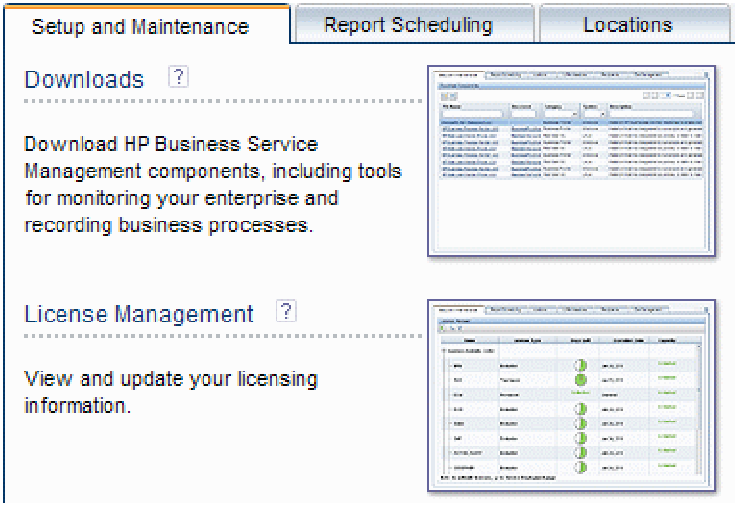
- **Menu Bar.** Enables navigation to the applications, Administration Console pages, help resources, and a link to the Site Map.



You can click the **Full Screen View** link to display the current page over the full screen. When selecting **Full Screen View**, the Task Assistant (if displayed), Menu Bar, Breadcrumbs, and Tabs are hidden. To return to the standard view of the page, click **Standard View** or press Esc on your keyboard.

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

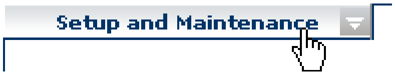
- ➤ **Tabs.** Enable navigation to various contexts within a particular area of HP Business Service Management, such as to different types of reports within an application, views within a report, or administrative functions within the Administration Console. In certain contexts, tabs are used to distinguish 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.



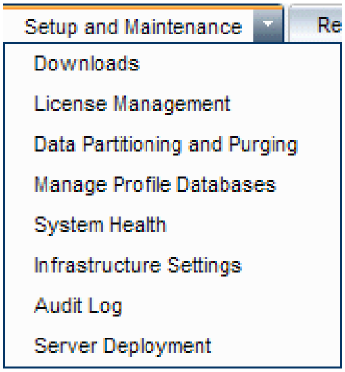
Download HP Business Service Management components, including tools for monitoring your enterprise and recording business processes.

View and update your licensing information.

- **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.



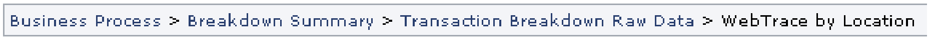
- **Navigation buttons.** Forward and back buttons, positioned in the upper left corner of the window, enable to you to navigate between viewed pages. You can go back to the most recently viewed page or forward to the previously viewed page before clicking the back button.
- **History**. You can select from a dropdown list of pages that are now stored in history. It is enabled by selecting the down arrow adjacent to the forward and back navigation buttons. This history is composed of the latest contexts you have viewed. You can view up to twenty viewed pages.

  The pages stored in history are those that HP Business Service Management has stored in its server. For all reports, if you return to a previously viewed page, the page opens exactly as you left it with the filters and conditions selected as previously.

There are several pages whose contexts and selections are not saved as previously viewed and when you return to that page, you may have to make your selections again. For example, if you were working in a specific context in Infrastructure Settings and return to the Infrastructure Settings page using the history option, your context has not been saved and you are returned to the default Infrastructure Settings page.

Note: You can change the number of pages stored in history (default is twenty) by accessing the file **<HPBSM root directory>\conf\settings\website.xml** and changing the value of the **history.max.saved.pages** field. This change is on the server and, therefore, affects all users.

- **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:



Business Process > Breakdown Summary > Transaction Breakdown Raw Data > WebTrace by Location

If the breadcrumb is longer than the width of the screen, only the tail of the breadcrumb is displayed. Click the **View** icon to the left of the breadcrumb to display the hidden portion of the breadcrumb in the current tab.

Note: The Web browser **Back** function is not supported in HP Business Service Management. Using the **Back** function does not always revert the current context to the previous context. To navigate to a previous context, use the navigation buttons within HP Business Service Management or the breadcrumb function.

User Interface Enhancements

The Business Service Management interface includes many features to enhance the user experience. These include:

- **Section 508 compliance.** BSM is compliant with the accessibility and usability standards for people with disabilities set by the US Federal Electronic and Information Technology Accessibility and Compliance Act ("Section 508"), and supports the JAWS® screen reader.

  JAWS users should change the **User Accessibility** setting from false to true. To do this:

  - Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**.
  - Select **Foundations**.
  - Select **Business Service Management Interface**.
  - In the **Business Service Management Interface - Display** area, locate **User Accessibility**. Change the value to **true**.

- **Personalization.** BSM remembers from one session to the next adjustments to tables (such as column width and column visibility) that you can make in a variety of applications and features, such as recipient management, reports management, reports, and report scheduling.

  Note: If two or more users are logged in simultaneously with the same credentials, BSM may not remember their personalized settings.

- **Table functionality.** You can manipulate tables in HP Business Service Management in a number of ways. A variety of controls enable, for example:

  - **Filtering.** BSM tables include various filtering options. For advanced editing of filters, click ▽.

- **Sorting.** Click on a column heading to sort by that column. Sort order changes between ascending and descending each time you press the column heading.
- **Selecting columns.** Click ▥ to choose which columns to display.
- **Changing column width.** Drag a column heading border to the left or right to modify column width. Click ☰ to reset column width to its original state.
- **Changing column order.** Drag a column heading to the left or right to change column order.
- **Paging.** Use buttons on the page control |◀ ◀ 1-20 of 25 ▶ ▶| to move to a table's first, previous, next, or last page.
- **Exporting.** Click the appropriate button to export a table to another format, such as Excel ▦ , PDF ▤ or CSV CSV.

For details about table functionality in reports, see "Common Report and Page Elements" on page 330.

Note: Not all tables support all table functionality.

- **Customization of the masthead title and logo.** You can customize the header text of the application title and the masthead logo (HP logo by default) displayed in the upper left-hand corner of the HP Business Service Management window. This change is made on the server side and affects all users accessing Business Service Management. For details, see "How to Customize the Masthead Title and Logo" on page 55.
- **Session expiration.** By default, a ping-to-server mechanism, called **Session Keepalive**, prevents your BSM session from timing out when not in active use. You can enable automatic session expiration by disabling Session Keepalive.

  To disable Session Keepalive, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**:

  - Select **Foundations**.

- Select **Business Service Management Interface**.
- In the **Business Service Management Interface - Timing** area, locate **Enable Session Keepalive**. Change the value to **false**.

Tasks

How to Customize the Masthead Title and Logo

To change the header text and logo, select Admin > Platform > Setup and Maintenance > Infrastructure Settings:

1 Select the **Foundations** context.

2 Select **Business Service Management Interface** from the list.

3 In the **Business Service Management Interface - Customized Masthead** table, change the following:

- In the **Customized Masthead Application Title,** enter the text to use as the title for the application. Business Service Management appears by default if there is no value defined for this field. You can use html coding to enter the text but do not include any scripts. If you using html, verify its validity before saving.
- In the **Customized Masthead Logo URL**, enter the URL of the file containing the logo you want to appear at the top of the window. The HP logo appears by default if there is no value defined for this field. It is recommended to use an image with a height of 19 pixels. If the image is higher, it does not appear correctly in the masthead.

  Once you modify these settings, the changes appear as soon as the browser is refreshed.

Reference

Client Requirements for Viewing BSM

The following table describes minimum and recommended client system requirements for viewing BSM:

Display	➤ Minimum: color palette setting of at least 256 colors ➤ Recommended: color palette setting of 32,000 colors **Note:** This requirement is only necessary for the Gateway Server machine.
Resolution	1280x1024 or higher (recommended) 1024x768 1280x800
Supported Browsers	➤ Microsoft Internet Explorer (IE) 8.0 ➤ Microsoft Internet Explorer (IE) 7.0 **Note: T**he browser must be set to accept all cookies.
Flash Player	Acrobat Flash 10.0 or later

Java Plug-in (to view applets)	**Recommended**: 6u18 **Supported**: 6u18 and later **Note:** You may not be able to view all HP Business Service Management applets with an earlier version of Java and you will need to download the latest version from the Java download site (http://www.java.com/en/download/manual.jsp) and install it. You may also have to disable earlier versions after download. After installation, if you are using Internet Explorer, verify that the browser is using the correct Java version and disable earlier versions. To do so, choose **Tools** > **Internet Options** > **Advanced** tab, locate the **Java (Sun) item** and select the check box for the correct Java version, click **OK**, close the browser, and reopen it.
Viewing the Documentation Library	➤ The Documentation Library is best viewed in Internet Explorer. ➤ The Documentation Library is best viewed from a browser with Java support. If your browser does not have Java support, download the Sun Java plug-in from the Sun Java Web site (http://java.com/en/index.jsp). Note that if Java support is not available, the Documentation Library automatically opens using the JavaScript implementation. The JavaScript implementation provides the same basic functionality as the Java implementation, however does not allow use of the Favorites tab within the navigation pane. ➤ If you experience a JavaScript error when opening the Documentation Library, disable the **Show Exception Dialog Box** in the Java Console and open the Help again.

Note for users having trouble opening Java applets:

If you are having trouble opening Java applets in the user interface, try one or both of the following:

- If you are using Internet Explorer, select **Tools** > **Internet Options** > **Connections** > **Local Area Network (LAN) Settings**. Clear the following options: **Automatically detect settings** and **Use automatic configuration script**.
- Select **Control Panel** > **Java** > **General** tab > **Network Settings** > Select **Direct connection** option (instead of the default option to Use browser settings).

Menus and Options

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

This section includes:

- "MyBSM" on page 58
- "Business User Applications" on page 59
- "Administration Console" on page 60
- "Help Menu" on page 62

MyBSM

Opens the MyBSM application, a portal that individual users can customize to display key content relevant to them. For details, see *Using MyBSM*.

Business User Applications

HP Business Service Management features the business user applications listed below. You access all applications from the **Applications** menu, except for the MyBSM application which is accessed from the top menu bar.

Menu Option	Description
Service Health	Opens the Service Health application, a real-time dashboard for viewing performance and availability metrics from a business perspective. For details, see *Using Service Health*.
Service Level Management	Opens 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	Opens 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*.
Operations Management	Opens the Operations Management application, used to proactively manage events from a business perspective, in order to restore services and minimize service disruptions. For details, see *Operations Management*.
Transaction Management	Displays transaction topology and infrastructure for data collection and report viewing. For details, see *Using Transaction Management*.

Menu Option	Description
System Availability Management	Opens the System Availability Management application, used for complete system and infrastructure monitoring as well as event management. For details, see *Using System Availability Management*.
User Reports	Opens the Report Manager, used for creating and saving 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*.

Administration Console

Administrators use the Administration Console to administer the HP Business Service Management 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
Service Health	Opens the Service Health 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 Service Health*.
Service Level Management	Opens 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*.
Operations Management	Opens the Operations Management Administration pages. For details, see *Operations Management*.

Menu Option	Description
End User Management	Opens 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*.
System Availability Management	Opens the System Availability Management Administration pages, where you configure and administer the SiteScope data collector. For details, see *Using System Availability Management*.
ODB Administration	Opens the ODB Administration pages, where you build and manage a model of your IT universe in the ODB. From ODB 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 Service Management applications. You can also manually create CIs to add to the model. For details, see *Modeling Guide*.
Business Service Management for Siebel Administration	Opens the Application Management for Siebel Administration page. For details, see *Solutions and Integrations*.
Platform	Opens the Platform Administration pages, which provide complete platform administration and configuration functionality. For details, see *Platform Administration*.
Integrations	Opens the EMS Integrations application, where you access out-of-the-box integrations (HP ServiceCenter, HP OM, NetScout, and others) and customize the Integration Monitor configuration files to correctly map the data Integration Monitors collect to a format recognizable by HP Business Service Management. For details, see *Solutions and Integrations*.

Menu Option	Description
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 Service Management. For details, see "Link to This Page Window" on page 38.
Personal Settings	Select to access the Personal Settings tab, which enables personalization of various aspects of HP Business Service Management, including menus and passwords. Note that Personal Settings are available to all users. For details, see "Personal Settings" on page 379.

Help Menu

You access the following online resources from the HP Business Service Management Help menu:

Menu Option	Description
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 Service Management.
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

Menu Option	Description
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. **Note:** The Site Map is the default entry page when you log into HP Business Service Management. Click **Change the default page** on the Site Map to open the Personal Settings tab and select a different entry page. For details on configuring Personal Settings, see "Personal Settings" on page 379.
What's New?	Opens the What's New document, which describes the new features and enhancements of the version.
About HP Business Service Management	Opens the About HP Business Service Management dialog box, which provides version, license, patch, and third-party notice information.

Part II

Setup and Maintenance

3

Downloads

This chapter includes:

Concepts

Tasks

Reference

Concepts

Downloads Overview

Once the servers for HP Business Service Management 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 Service Management, you must install the data collector setup file. For details, see "Installing Component Setup Files" in *the HP Business Service Management Deployment Guide* PDF.

Tasks

How to Download Components

This task describes how to download components on the **Download Components** page:

1. Click the component you want to download.
2. Save the component's setup file to your computer.
3. Run the component's setup file to install the component.

Reference

Downloads User Interface

This section includes:

- Download Components Page on page 70

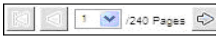
Download Components Page

This page lists the HP Business Service Management 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	➤ You can filter the downloadable components either by category or by system. ➤ Since some files run immediately when you click to download them, right click the file you want to download, select **Save Target As**, and choose the location in which you want to save the file.
See also	"Downloads Overview" on page 68

User interface elements are described below:

UI Elements (A-Z)	Description
☰	Resets the table columns' width to its default setting. You can adjust the width of the table's columns by dragging the borders of the column to the right or the left.
▥	Opens the Select Columns dialog box enabling you to select the columns you want to be displayed on the table.

UI Elements (A-Z)	Description
	Divides the table of data into pages. You move from page to page by clicking the relevant button: ➤ To view more reports, click the **Next page** or **Last page** buttons. ➤ To view previous reports in the list, click the **Previous page** or **First page** buttons.
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 Service Management. ➤ **Business Process Monitor.** Downloadable files that enable you to install and run Business Process Monitor components on HP Business Service Management. ➤ **Diagnostics.** Downloadable files that enable you to install and run Diagnostics components. ➤ **Data Flow Probe.** The Data Flow Probe downloadable file that enables you to install and run the Data Flow Probe component on HP Business Service Management. ➤ **Other**. Used for other applications for download. If you see no applications listed for this category, there are none available. ➤ **Real User Monitor.** Downloadable files that enable you to install and run Real User Monitor components. ➤ **SiteScope.** The SiteScope downloadable file that enables you to install and run SiteScope components. **Note:** Ensure that you have selected the file that corresponds to the Operating System with which you are working. ➤ **TransactionVision.** Downloadable files that enable you to install and run TransactionVision components. ➤ **TransactionVision or Diagnostics.** Downloadable files that enable you to install and run the HP Diagnostics/TransactionVision Agent for Java file.
Description	An explanation of the specific downloadable file.

UI Elements (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 Service Management components are to run.

4

Licenses

This chapter includes:

Concepts

Reference

Concepts

License Management Overview

You must have a valid license to run monitors and transactions, and to use various integral applications in HP Business Service Management.

The HP Business Service Management 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 expiration date, all depend on the license your organization has purchased from HP.

The initial license may be installed only in the configuration wizard, during the installation process.

HP Business Service Management posts a license expiration reminder after the login page of the Web site (for administrators only), ten days before license expiration.

A number of HP Business Service Management applications require additional licensing. To use these applications, you must obtain a license from HP and then upload the license file in HP Business Service Management. For more information, see "License Manager Page" on page 75.

Reference

Licenses User Interface

This section includes:

- License Manager Page on page 75

License Manager Page

This page displays information on general license properties and enables you to update your license key, as necessary.

To access	Select **Admin** > **Platform** > **Setup and Maintenance** > **License Management**
Important information	To review the status of your license, select **Admin** > **Platform** > **License Management**
Relevant tasks	"How to Update Your BSM Licenses, Applications, or Deployment Scope" on page 82
See also	"License Management Overview" on page 74 "Server Deployment Overview" on page 80

User interface elements are described below:

UI Elements	Description
⊞	**Add License.** Opens the Add License dialog box. Use the dialog box to upload a license file. You must determine the location of the license file. These files are data files and end in **.DAT**.
Name	This is the name of the licensed feature. It includes an association to the product resource with which it was bundled.

UI Elements	Description
License Type	There are three types of licenses: ➤ **Evaluation:** A license with a fixed trial period of up to 60 days. This type of license is available only until a Time Based or Permanent license is purchased. Once purchased, the trial period immediately terminates. **Note:** An Evaluation License cannot be renewed. ➤ **Time Based:** A license which has a time-based expiration date. ➤ **Permanent:** A license which does not expire.
Days Left	Displays a measure of the amount of days the license may continue to be used, in relation to the amount of days already used. This qualification is expressed as a pie chart graphic. When green, expiry time is pending; when red, the license is expired.
Expiration Date	Displays the license's fixed expiration date. This date is displayed only for time-based licenses.
Capacity	If the license is capacity based, the amount of capacity available and the amount of capacity used will be expressed by means of a status bar. **Available when:** This feature is available when the license is capacity based. If the license is not capacity based, the words Not Applicable will appear in the capacity column.

UI Elements	Description
Capacity Details	If the license is capacity based, the amount of capacity available and the amount of capacity used will be expressed by means of a ratio. **Available when:** This feature is available when the license is capacity based. If the license is not capacity based, the words Not Applicable will appear in the capacity column.
Service Deployment Link	When you add a license to BSM, you must enable the application in the Server Deployment page. This includes a check to see whether the physical resources of your deployment can handle the added application. For user interface details, see "Server Deployment User Interface" on page 85. For concept details, see "Server Deployment Overview" on page 80.

Troubleshooting and Limitations

This section describes troubleshooting and limitations for Activating licenses

Some licenses will not automatically activate upon installation. These licenses need to be activated for specific use and do not run at all times. To activate such a license, click on the Service Deployment link at the bottom of the License Manager pane.

5

Server Deployment

This chapter includes:

Concepts

Tasks

Reference

Concepts

Server Deployment Overview

HP Business Service Management is composed of many applications and subsystems that consume hardware and software resources. The available applications answer a variety of use cases, not all of which are required by every user. You can align the deployment of the BSM servers with your company’s business requirements.

BSM’s Server Deployment page provides a mechanism to deploy only the applications required by your company. You can determine the required hardware according to the required capacity for your specific deployment. The Server Deployment feature displays exactly how much hardware capacity you need for your deployment and enables you to free up unused resources.

The Server Deployment page is available both in the Setup and Database Configuration Utility that is run once BSM servers are installed, and in the Platform Admin area of the BSM interface. This enables you to update your deployment, enable or disable applications as needed, and adjust your deployment’s capacities even after installation is complete and any time you have adjustments to make to your BSM deployment. You can enable or disable applications as needed so as not to use any unnecessary resources in your deployment.

Capacity Calculator

You can use the capacity calculator Excel sheet to determine the scope and size of your BSM deployment. You input the information regarding the scope of your deployment in terms of numbers of applications running, users, and expected data. The capacity calculator then calculates the required memory, CPU cores, and determines the size of your deployment. If you are making any change to your deployment, for example adding a license for an application, you use the information in the capacity calculator to determine your hardware requirements and deployment configuration.

You can upload a file that has been saved with your data directly into the Server Deployment page. This enables you to automatically populate the fields in the page with the data as you entered it into the Excel sheet.

If you used the file when you first installed BSM, use your saved version whenever you need to make any changes to your deployment. If you do not have your own version, the file can be found in the **Documentation** folder in the main BSM installation DVD, or you can download the latest version from the HP Software Product Manuals Web site (http://h20230.www2.hp.com/selfsolve/manuals).

You enter the information regarding your deployment in the **Deployment Calculator** sheet of the file. In the **Capacity Questionnaire** columns, include information such as applications and size and the **Output** tables automatically calculate the hardware and software requirements. Make sure to save the file in a location from which you can upload it to the Server Deployment page. It is recommended that you make a copy of the file each time before updating it.

When you update the capacity calculator, you are not making any changes to your deployment. You use the capacity calculator to update the values in the Server Deployment page. Only changing values and clicking **Save** in the Server Deployment page actually updates your deployment.

Tasks

How to Update Your BSM Licenses, Applications, or Deployment Scope

This task describes how to make changes to your server deployment.

This task includes the following steps:

- "Use the capacity calculator to determine the required capacity of your deployment change" on page 82
- "Add a new license - optional" on page 83
- "Update the deployment in the Server Deployment page" on page 83
- "Restart BSM" on page 84
- "Results" on page 84

1 Use the capacity calculator to determine the required capacity of your deployment change

Before you make any changes to your BSM deployment, such as adding a license for an application, it is recommended that you use the capacity calculator Excel file to determine if your current servers meet the required capacity.

It is recommended that you modify the saved version of the capacity calculator that was used prior to installing BSM. If you did not save your own version of the capacity calculator before installation or thereafter, a version can be found in the **Documentation** folder in the main BSM installation DVD, or you can download the latest version from the HP Software Product Manuals Web site (http://h20230.www2.hp.com/selfsolve/manuals).

Make sure to save the file with your current requirements in a location from which you can upload it to the Server Deployment page.

For concept details, see "Capacity Calculator" on page 81.

2 Add a new license - optional

Perform this step if you are updating your deployment with a new license.

Select **Admin** > **Platform** > **Setup and Maintenance** > **License Management**.

Click **Add license from file** to open the Add license dialog box where you can search for the relevant .dat file. The file is uploaded from the client machine to the BSM server.

At the bottom of the License Management page, click the **Server Deployment** link.

3 Update the deployment in the Server Deployment page

Select **Admin** > **Platform** > **Setup and Maintenance** > **Server Deployment**.

➤ **Input table**. Click the **Browse** button to upload the saved version of your capacity calculator Excel file. When you select a file to upload, the values entered in the capacity calculator file automatically populate the Server Deployment page with the correct information for your deployment.

  You can also enter the required information in the upper table manually, but it is recommended to use the capacity calculator so that it calculates the capacity for you and determines the scope of your deployment based on the values you input.

➤ **Server status table**. In the lower table indicating the status of the servers, ensure that the required memory does not exceed the detected memory on the servers. If it does, you must either remove selected applications, change the capacity level, or increase the memory on the servers.

  For user interface details, see "Server Deployment Page" on page 85.

4 Restart BSM

After you click **Save** in the Sever Deployment page, you must disable and enable BSM.

Select **Start** > **Programs** > **HP Business Service Management** > **Administration** > **Disable HP Business Service Management/Enable HP Business Service Management**.

5 Results

If you added any applications to your deployment, they now appear in the BSM menus. For example, if you enabled the System Availability Management application, you can now find the menu option under both the **Admin** and **Applications** menu.

Conversely, if you removed any applications from your deployment, they are no longer available in the applicable menus.

Reference

Server Deployment User Interface

This section includes:

- Server Deployment Page on page 85

Server Deployment Page

This page enables you to update your deployment and determine if your hardware meets the memory requirements of any change you make.

To access	**Admin** > **Platform** > **Setup and Maintenance** > **Server Deployment**
Important information	➤ It is recommended to use this page in conjunction with the capacity calculator. For details, see "Capacity Calculator" on page 81. ➤ Once you save the changes to this page, BSM must be restarted for the changes to take effect.
Relevant tasks	"How to Update Your BSM Licenses, Applications, or Deployment Scope" on page 82
See also	"Server Deployment Overview" on page 80

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Elements	**Description**
<Capacity Calculator file name>	Use the **Browse** button to locate and upload your saved capacity calculator Excel file. If you have not yet entered your values into a capacity calculator, it is recommended that you do so prior to making any changes to this page. A capacity calculator file can be accessed from the **Documentation** folder in the main BSM installation DVD, or you can download the latest version from the HP Software Product Manuals Web site (http://h20230.www2.hp.com/selfsolve/manuals). For concept details, see "Capacity Calculator" on page 81 and for the task, see "Use the capacity calculator to determine the required capacity of your deployment change" on page 82.

UI Elements	Description
<**Capacity table**>	The upper table in the page displays the current information regarding deployment and applications. If you upload a capacity calculator file, this table is automatically updated with the information in the capacity calculator. You can change the capacity level of your deployment for: ➤ Users ➤ Model ➤ Metric data ➤ Applications You can also clear or select any of the applications listed. After you click **Save** and restart BSM: ➤ When you select an application that was previously not selected, the application is available in BSM and applicable menus. ➤ When you clear an application that was previously selected, the application is no longer accessible.

UI Elements	Description
<Server status table>	The lower table lists all the servers running BSM including: ➤ **Status**. Whether the machine is up and running. ➤ **Aligned**. Whether this machine is aligned with the current deployment configuration. It would be aligned only if BSM was restarted on this machine after any changes were made. If BSM was not yet restarted on this machine since any configuration changes were made in this page, the machine is not aligned. ➤ **Machine**. The name of the server. ➤ **Installed**. Which type of BSM server is installed on the machine, Gateway or Processing or both (Typical installation when Gateway and Data Processing are on the same machine). ➤ **Activated**. Which type of BSM server is currently activated on the machine, Gateway or DPS (data processing server). ➤ **Detected**. The free memory detected on the machine. ➤ **Required**. The required memory for each type of server based on the applications and capacity levels listed in the upper table. If the Required memory is higher than the memory in the Detected column, you must either: ➤ Change capacity levels for your deployment, for example: clear applications from the list of available applications. ➤ Add memory to the physical machines and try to update your deployment again.

Troubleshooting and Limitations

This section describes troubleshooting and limitations for Server Deployment.

- If an application is missing from the BSM interface, activate it using the Server Deployment page.
- If an application was activated but does not appear in the BSM interface, restart all BSM servers.
- If an application was selected in the capacity calculator but was not imported to the Server Deployment page, ensure that you have a valid license for this application.

6

Database Administration

This chapter includes:

Concepts

Tasks

Reference

Concepts

Database Management - Overview

HP Operations administers these pages and the interface is hidden from your view.

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

Before you configure your monitoring environment, you must configure the database into which you want monitoring data saved. A profile database can store data for different types of data sources (Business Process Monitor, SiteScope). You can either create one database for all data or create dedicated databases (for example, for each data 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 Service Management supports two database types:

- **Microsoft SQL server.** This database runs on Windows operating systems only. For details on how to configure a database on a Microsoft SQL server, see "How to Configure a Profile Database on a Microsoft SQL Server" on page 98.
- **Oracle server.** This database runs on any HP Business Service Management supported operating system. An Oracle server database is referred to as a user schema. For details on how to configure a database on an Oracle server user schema, see "How to Configure a User Schema on an Oracle Server" on page 99.

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 Service Management 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 Service Management to collect the following types of data:
  - Service Level Management data
  - SOA data
  - data from Real User Monitor and Business Process Monitor
  - data used in Service Health
  - HP Diagnostics data
  - persistent custom data

Note: The first database added on the Database Management page is automatically designated as the default profile database.

- **Add profile tables to an existing, empty database.** HP Business Service Management 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 Service Management 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 Service Management Database Guide* PDF. It is recommended that you review the relevant portions of *the HP Business Service Management Database Guide* PDF before performing profile database management tasks.

Partitioning and Purging Historical Data from Profile Databases

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.

HP Business Service Management'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 Service Management reports. After an additional defined amount of time, a partition is purged from the profile database.

The Partition and Purging Manager is activated for each profile database and handle partitioning and later purging of historical data according to the time period listed for the database table. The size of each partition is determined by the EPM (events per minute) value displayed on the Purging Manager page. The default EPM values are preset according to the appropriate level of the specified database table. 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.

Note: The partitioning method used by the Partition and Purging Manager is Database Native Partitioning. (Refer to database support matrix in the release notes for the SQL SERVER and Oracle Enterprise editions supported for this release). In an Oracle database, the Oracle Partitioning option should be enabled. If the Oracle Partitioning option is not available, the Partition and Purging Manager does not partition or purge data. Failure to partition or purge may result in major performance issues.

You can also use the Partition and Purging Manager to set a specific time period—per table—for removing historical data. For details on the user interface for performing this task, see "Purging Manager Page" on page 112.

The Partition and Purging Manager runs every hour to check if a new data partition needs to be created and to purge data older than the retention time defined per table.

Note: By default, the Partition and Purging Manager does not purge data. Make sure to configure purging policies for your data samples using the Partition and Purging Manager administration screen.

For guidelines and tips on using the Partition and Purging Manager, see "Guidelines and Tips for Using the Partition and Purging Manager" on page 96.

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 and 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 Service Management Database Guide* PDF.

Guidelines and Tips for Using the Partition and Purging Manager

This section contains 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 Service Management.

  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 on the Data Processing server at **<HPBSM server root directory>\log\pmanager.log**.
- Use the following principle when defining purging for your raw and aggregated data: 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.

Tasks

How to 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 98
- "Add a Database" on page 99

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 a Microsoft SQL server is installed. If you are connecting to a non-default Microsoft SQL server instance in dynamic mode, enter the server name in the following format:

```
<host_name>\<instance_name>
```

b **Database user name and password.** The user name and password of a user with administrative rights on a 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. You must change the port number in one of the following instances:

- The default Microsoft SQL server instance listens to a port other than 1433.
- You connect to a non-default Microsoft SQL server instance in static mode.

- You connect to a non-default Microsoft SQL server instance in dynamic mode. In this case, enter port number 1434.

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 user interface details, see "Profile Database Properties - MS SQL Server Page" on page 106.

How to Configure a User Schema on an Oracle Server

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

This task includes the following steps:

- "Prerequisites" on page 99
- "Gather Connection Parameters" on page 100
- "Add a User Schema" on page 100

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 Service Management 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 Service Management 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 - Oracle Server** page. For user interface details, see "Profile User Schema Properties - Oracle Server Page" on page 109.

If your Profile database is part of Oracle Real Application Cluster (RAC), see Appendix E, "Support for Oracle Real Application Cluster" in *the HP Business Service Management Database Guide* PDF.

How to Work with the Purging Manager

This task describes how to work with the Purging Manager.

This task includes the following topics:

- "Prerequisites" on page 101
- "Change the Database Template" on page 101
- "Change Settings for Multiple Databases" on page 102
- "Change Settings for Individual Databases" on page 103

1 Prerequisites

Ensure that you have at least one profile database configured in your HP Business Service Management system. For details on configuring a profile database on a Microsoft SQL server, see "How to Configure a Profile Database on a Microsoft SQL Server" on page 98.

For details on configuring a user schema on an Oracle server, see "How to Configure a User Schema on an Oracle Server" on page 99.

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**.

How to Determine the Events Per Minute for Data Arriving in BSM

You can determine the amount of data per minute that is arriving in HP Business Service Management. You enter this number in the **Change to EPM** box at the top of the **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\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.

To determine to which data table in the Partition Manager the sample belongs, follow the instructions for "Advanced Sample Retrieval" under "Generic Reporting Engine API – Overview" in *Reports*. The resulting list displays the data table in parentheses next to the name of the sample. You can then enter the EPM number for the correct table.

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

Reference

Database Administration User Interface

This section includes (in alphabetical order):

- Database Management Page on page 105
- Profile Database Properties - MS SQL Server Page on page 106
- Profile User Schema Properties - Oracle Server Page on page 109
- Purging Manager Page on page 112

Database Management Page

This page enables you to maintain and administer the databases HP Business Service Management uses to store monitoring data.

To access	Select **Admin** > **Platform** > **Setup and Maintenance** > **Manage Profile Databases**
Important information	The first database added on the Database Management page is automatically designated as the default profile database.

User interface elements are described below:

UI Elements (A-Z)	Description
❌	Disconnects the database or user schema. **Note:** You cannot delete the default profile database or a database which is in use.
Add	Adds a Microsoft SQL server database or Oracle server user schema, as specified in the dropdown database list.

UI Elements (A-Z)	Description
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 on which the database is running.

Profile Database Properties - MS SQL Server Page

This page 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 Service Management Database Guide* PDF. ➤ Database creation can take several minutes.
Relevant tasks	"How to Configure a Profile Database on a Microsoft SQL Server" on page 98
See also	"Database Management - Overview" on page 92

User interface elements are described below:

UI Elements (A-Z)	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.
Disconnect	Disconnects the database from HP Business Service Management. **Note:** This button appears only 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 Service Health, Real User Monitor, HP Diagnostics (if installed), Service Level Management, SOA, or persistent custom data. ➤ Selecting this check box overwrites the existing default profile database.
Password	➤ Should remain empty if you are using Windows authentication. Make sure HP Business Service Management service runs by a windows user configured in the database server as an authorized windows login. ➤ If you are using SQL server authentication, enter the password of a user with administrative rights on Microsoft SQL server.

UI Elements (A-Z)	Description
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). ➤ You use a non-default port in static mode. ➤ You use a non-default port in dynamic mode. In this case, enter port **1434**.
Server name	Enter the name of the machine on which the Microsoft SQL server is installed. If you are using a non-default instance in dynamic mode, enter the server name in the following format: <my_server\my_instance>
SQL server authentication	Select if the Microsoft SQL server is using SQL server authentication.
User name	➤ Should remain empty if you are using Windows authentication. ➤ 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

This page 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 Service Management 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, verify that the user schema name appears in the database list on the Database Management page to ensure that the user schema was successfully created.
Relevant tasks	"How to Configure a User Schema on an Oracle Server" on page 99
See also	"Database Management - Overview" on page 92

User interface elements are described below:

UI Elements (A-Z)	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 enabled only 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 enabled only 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	Disconnects the user schema from HP Business Service Management. **Note:** This button appears only 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.

UI Elements (A-Z)	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 Service Health, Real User Monitor, HP Diagnostics (if installed), Service Level Management, SOA, or persistent custom data. ➤ Selecting this check box overwrites the existing default profile 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 Service Management on the Oracle server.

If your Profile database is part of Oracle Real Application Cluster (RAC), refer to Database Guide/Support for Oracle Real Application Cluster appendix.

Purging Manager Page

This page enables or disables the Partition and Purging Manager which instructs BSM to begin or stop the process of partitioning the data.

To access	Select **Admin** > **Platform** > **Setup and Maintenance** > **Data Partitioning and Purging**
Important information	Partitioning and Purging manager partitioning method is native partitioning. In an Oracle database, the Oracle Partitioning option should be enabled. For details on purging data from an Oracle database, see "About Data Partitioning and Purging" in the *HP Business Service Management Database Guide* PDF.
See also	"Partitioning and Purging Historical Data from Profile Databases" on page 94

User interface elements are described below:

UI Elements (A-Z)	Description
Apply to	Used to select the databases and template to which you want the configurations on the Template and Multiple Databases tab to apply. You can clear all databases to make changes only to the selected template.
Change to EPM	The amount of data per minute configured to arrive in BSM. **Note:** Leave this field empty to retain the existing EPM value. For details on determining this value, see "How to Determine the Events Per Minute for Data Arriving in BSM" on page 103.
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.

UI Elements (A-Z)	Description
Epm Value	The amount of data per minute that is arriving in BSM. For details on determining this value, see "How to Determine the Events Per Minute for Data Arriving in BSM" on page 103.
Keep Data for	The time range for keeping data in the database tables whose check box is selected. This element appears as follows: ➤ **Selection fields.** At the top of the page, set the time period 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** selection fields at the top of the page. **Note:** The time period configured in the **Keep Data for** fields indicates that the data is stored for at least the specified amount of time - it does not indicate when the data is purged. By default, retention time is Infinite, meaning no purging is set.
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: ➤ Alerts ➤ BPI ➤ Business Logic Engine ➤ Business Process Monitor ➤ Diagnostics ➤ Real User Monitor ➤ SOA ➤ Service Level Management ➤ SiteScope ➤ TransactionVision ➤ UDX (custom data) ➤ WebTrace

UI Elements (A-Z)	Description
Select a profile database	Select a profile database for which you want to modify time range configurations for purging data. **Note:** This field is visible only on the Database Specific tab.
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.

7

Infrastructure Settings

HP Operations administers these pages and the interface is hidden from view, except for the user accessing with superuser permissions.

This chapter includes:

Concepts

Infrastructure Settings Manager - Overview

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

HP Business Service Management enables you to modify the value of many settings that determine how HP Business Service Management and its applications run.

Caution: Modifying certain settings can adversely affect the performance of HP Business Service Management. 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 the following groups:

- **Applications.** This list includes those contexts that determine how the various applications running within HP Business Service Management behave. Contexts such as Service Health Application, MyBSM, and Service Level Management are listed.
- **Foundations.** This list includes those contexts that determine how the different areas of the HP Business Service Management foundation run. Contexts such as ODB and LDAP Configuration are listed.

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

There are some infrastructure settings which are configured outside the Infrastructure Settings Manager. For details, see "How to Modify the Ping Time Interval" on page 118, and "How to Modify the Location and Expiration of Temporary Image Files" on page 118.

Tasks

How to 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 BSM 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. 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 BSM on the Gateway server machine.

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

How to Modify the Location and Expiration of Temporary Image Files

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

When you generate a report in BSM applications, or when BSM automatically generates a report to send through the scheduled report mechanism, images (for example, graphs) are created. BSM saves these images, for a limited period of time, in temporary directories on the Gateway server machines 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 120.

➤ **The length of time that BSM keeps temporary image files before removing them**

For details, see "Modify the Length of Time that BSM Keeps Temporary Image Files" on page 125.

➤ **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 129.

This section also includes:

➤ "Modify the Directory in Which Temporary Image Files Are Stored" on page 120

➤ "Access Temp Directory with Multiple Gateway Server Machines" on page 122

➤ "Modify the Length of Time that BSM Keeps Temporary Image Files" on page 125

➤ "Specify the Directories from Which Temporary Image Files Are Removed" on page 129

Modify the Directory in Which Temporary Image Files Are Stored

You can modify the path to the directory where HP Business Service Management 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 Service Management 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 Service Management 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 122.

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 Service Management 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 Service Management 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 Service Management 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 Service Management 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 BSM Keeps Temporary Image Files

You can modify settings that control how long HP Business Service Management 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 Service Management 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 Service Management 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 Service Management 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 Service Management to use only maximum size criteria (see below).

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

  Specifies the total size, in KB, to which the defined directory can grow before HP Business Service Management 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 Service Management first removes expired files. HP Business Service Management 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 Service Management removes files based only 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 Service Management 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 Service Management to use only the expiration time criterion.

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

  Specifies the additional amount by which HP Business Service Management 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 Service Management deletes the oldest files first.

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

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

  Specifies how often HP Business Service Management runs the mechanism that performs the defined work.

Example:

HP Business Service Management is instructed to perform the following work once every 30 minutes: HP Business Service Management first checks whether there are files older than 1 hour and, if so, deletes them. Then HP Business Service Management 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 Service Management reduces the total directory size by 50% by removing the oldest files. As a result, HP Business Service Management 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 Service Management 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 Service Management 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 Service Management to remove temporary image files from the subdirectories of the specified path.

To configure HP Business Service Management 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 Service Management on the Gateway server machine.

5 Repeat the above procedure on all Gateway server machines.

Reference

Infrastructure Settings User Interface

This section includes:

➤ Infrastructure Settings Manager Page on page 130

Infrastructure Settings Manager Page

This page enables you to define the value of many settings that determine how HP Business Service Management 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 Service Management. It is highly recommended not to modify any settings without first consulting HP Software Support or your HP Services representative.
See also	"Infrastructure Settings Manager - Overview" on page 116

User interface elements are described below:

UI Elements (A-Z)	Description
All	Select to view all the settings for both Applications and Foundations.
Applications	Select to edit one of the HP Business Service Management Applications.

UI Elements (A-Z)	Description
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 Service Management Foundations.
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	Restores 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.

8

Audit Log

This chapter includes:

Concepts

Tasks

Reference

Concepts

Audit Log - Overview

You use the audit log to keep track of different actions performed by users in the system, according to specific contexts:

- **Alert Administration.** Displays actions related to creating and managing alerts.
- **Assignment Administration.** Displays actions related to creating and managing assignments.
- **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 Service Health 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 (Business Process profiles, Real User Monitor engines, and SiteScope monitors) from End User Management Administration.
- **Downtime/Event Scheduling.** Displays actions related to creating and modifying downtime and scheduled events.
- **End User Management-Applications.** Displays actions related to adding, editing, updating, disabling and deleting event-based alerts, as well as registering and unregistering alert recipients. For additional details, see "**Audit Log**" in *Using End User Management.*

- **IT World Configuration.** Displays actions, including editing, updating, and removing CIs and relationships, performed in the IT Universe Manager application.
- **Locations Manager.** Displays actions related to adding, modifying, and deleting locations, performed in the Location Manager application.
- **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.
- **Operations Management.** Displays actions related operations management, such as the creating and modifying of content packs, event rules, and notifications.
- **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.
- **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 "How to Use the Audit Log" on page 137.
- **SLA Alert Administration.** Displays actions related to creating, modifying, or deleting SLA alerts.
- **System Availability Manager.** Displays actions related to system availability and SiteScope.
- **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.

For details about the user interface, see "Audit Log Page" on page 138.

Tasks

How to Use the Audit Log

This task describes how to access the Audit Log, which is available from the Audit Log page in the Setup and Maintenance menu in 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 Service Management 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.
5. Click **Apply**. HP Business Service Management updates the table with the relevant information.

If required, use the **Previous Page** arrow to navigate to the previous page of the Audit Log, or the **Next Page** arrow to navigate to the next page of the Audit Log.

Reference

Audit Log User Interface

This section includes:

Audit Log Page

This page enables you to keep track of different actions performed by users in the system.

To access	Select **Admin** > **Platform** > **Setup and Maintenance** > **Audit Log**
See also	"Audit Log - Overview" on page 134

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Elements (A-Z)	Description
▲ ▼	Moves to the previous page or next page in the Audit Log.
<Audit log table>	Displays the contents of the audit log. For details, see "Audit Log Table" on page 140.
<EUM applications>	Select an <EUM application> for which you want to view the actions performed. **Note:** This field is displayed only if you have chosen the End User Management-Applications context.
Auditing Filters	Click the Auditing Filters heading to specify filter criteria. For details, see "Auditing Filters Pane" on page 139.

UI Elements (A-Z)	Description
Context	Select a context to view. For a detailed list of the available contexts, see "Audit Log - Overview" on page 134.
For user	Displays the user whose actions are displayed in the Audit Log, as specified in the Auditing Filters pane. **Default Value:** All
SiteScope	Select a SiteScope for which you want to view the actions performed. **Note:** This field is displayed only if you have chosen the System Availability Manager 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

User interface elements are described below:

UI Elements (A-Z)	Description
...	Opens the Calendar dialog box enabling you to select a date.
⏬	Expands the Auditing Filters pane.
⏫	Collapses the Auditing Filters pane.
Apply	Applies the selected filters.
Cancel	Cancels filtering and closes the Auditing Filters pane.
Clear All	Clears the filters and displays all log items.
Containing text	Specify a text string to filter out all the actions that do not include this text string.
End before	Specify an ending time until which you want to view actions.

UI Elements (A-Z)	Description
Start after	Specify a starting time from which you want to view actions.
User	Select a user to view actions performed by only that user.

Audit Log Table

Important information	For details about the audit log for the EUM Alert Administration, see "Audit Log" in *Using End User Management*.

User interface elements are described below:

UI Elements (A-Z)	Description
Actions	Displays the actions performed by the specified user.
Additional Information	Displays additional information, where relevant.
Modification Date	Displays the date and time that the specified actions were performed.
Modified By	Displays the user who performed the specified actions.

9

Working in Non-English Locales

This chapter includes:

Reference

Reference

Installation and Deployment Issues

➤ If you use a CJK language in your browser, you must ensure that the Gateway server machine running HP Business Service Management has East Asian languages installed. On the machine on which the HP Business Service Management Gateway server is installed, you must select **Control Panel** > **Regional & Language Options** > **Languages** > **Install files for East Asian languages**.

➤ Business Process Monitors and the Gateway Server must be installed on an operating system that has the same locale as the data.

➤ During Business Process Monitor installation, non-Latin characters cannot be used for the host name and location. If necessary, after installation you can change the names to include non-Latin characters, in **Admin** > **End User Management** > **Settings**.

➤ The installation path for all HP Business Service Management components must not contain non-Latin characters.

Database Environment Issues

- To work in a non-English language HP Business Service Management environment, you can use either an Oracle Server database or a Microsoft SQL Server database. When using a Microsoft SQL Server database, it should use the same encoding as you use in your BSM servers. When using an Oracle Server database, the encoding of the database can also be UTF-8 or AL32UTF-8, which supports both non-English languages as well as multiple languages. For a list of supported and tested database servers refer to, "HP Business Service Management Databases" in the *HP Business Service Management Deployment Guide* PDF.
- When you create a new Oracle instance in an Oracle database, you must specify the character set for the instance. All character data, including data in the data dictionary, is stored in the instance's character set. For details on working with Oracle databases, refer to "Deploying and Maintaining the Oracle Server Database" in the *HP Business Service Management Database Guide* PDF. For supported and certified Oracle character sets, refer to "Oracle Summary Checklist" in
- The SiteScope Database Query Monitor can connect to an Oracle database but the Oracle user names and passwords must contain only Latin characters.

Administration Issues

- E-mail alerts sent with ISO-2022-JP encoding are supported only by an SMTP server running on a Windows platform. Use of this encoding affects all HP Business Service Management servers.
- When using the default authentication strategy, Lightweight SSO, to authenticate users logging in to HP Business Service Management, user names and passwords can be in non-Latin characters.
- To support non-Latin characters, the encoding for HP Business Service Management databases must be defined as UTF-8 or AL32UTF-8 (Oracle only), or set to the specific language.

Service Health Issues

You may have to perform several steps to enable displaying non-Latin languages in the Service Health Top View.

To display non-Latin languages in Service Health Top View:

1. Verify that you have followed the instructions on installing the JRE on a non-Western Windows system. The instructions are found at the http://java.sun.com/j2se/1.5.0/jre/install-windows.html.
2. Make sure that you:
   - ➤ have administrative permissions to install the J2SE Runtime Environment on Microsoft Windows 2000 and XP.
   - ➤ (For users installing the JRE on non-Western 32-bit machines) choose a **Custom** Setup Type. In Custom Setup under feature 2 (**Support for Additional Languages**), select **This feature is installed on local hard drive**.
3. Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, click **Applications**, select **Service Health Application**, and locate the **Top View Font Name** entry in the **Service Health Application – Top View Properties** table. Change the value to **Arial Unicode MS**.

   Caution: If the value of the **Top View Font Name** entry is **default**, you do not need to perform this step, as the Top View Font Name property automatically assumes the Arial Unicode MS value in that case.

4. Close all instances of the Web browser.
5. Log in to HP Business Service Management and access Service Health Top View. Verify that the Chinese or Japanese characters now appear correctly.

Service Level Management Issues

Service Level Management does not support service names that contain more than 50 multibyte characters.

Application Management for Siebel Issues

- Non-Latin characters may not appear or may be corrupted in the Topology View. If you encounter this problem, install the Arial Unicode Microsoft font from the Microsoft Web site.
- HP Business Service Management by default only supports English language Siebel. Do not deliver data from a non-English version of Siebel to HP Business Service Management. You should use special translation adapters to enable HP Business Service Management to work with a non-English version of the Siebel application. For details, contact HP Software Support.

Report Issues

- HP Business Service Management does not support Custom Report names that contain more than 50 multibyte characters.
- The Page Component Breakdown report does not support URLs that contain multibyte characters. When specifying a URL and a location from which to run the breakdown, you must enter Latin characters in the URL box.
- Excel reports must have Latin-character file names when uploading to HP Business Service Management running on a Chinese Simplified operating system. To view Excel reports, select **Applications** > **User Reports** > **Report Manager**.
- Reports downloaded from HP Business Service Management to Excel cannot be displayed properly on an operating system whose language differs from the data language.

To download Excel files with multibyte data when HP Business Service Management is installed on an English-language machine, set the **user.encoding** entry in the <**Business Service Management root directory**>**\AppServer\resources\strings.properties** file to the correct encoding.

Business Process Monitor Issues

- If the Business Process Monitor log files contain non-English data, you must open them in a viewer that supports UTF-8 format parsing, for example, Notepad, rather than from the View BPM Files window in the Business Process Monitor Admin.

  Log files that are saved in the default encoding of the server on which the Business Process Monitor Admin is installed are shown correctly in the View BPM Files window.
- HP Business Service Management does not support Business Process Monitor host names that contain more than 25 multibyte characters.
- All BPM instances (application, scripts, parameters, etc.) should be named with Latin chars or BPM Server locale characters only.

SiteScope Issues

- In SiteScopes running in I18N mode, the **Return to Group** link displayed during monitor set creation shows the indexed-based group name (for example, **group0**) instead of the user-defined group name.
- The Database Query Monitor can connect to an Oracle database only if the Oracle user names and passwords contain Latin-only characters.
- SiteScope does not support non-Latin characters in the username/password.
- Beginning with SiteScope version 8.5, the user interface can be displayed in several languages. For details, see "Using SiteScope in an Internationalization (I18N) Environment" in *Using System Availability Management*.

- For a list of monitors that are tested for internationalization, see "Monitors Tested for Internationalization" in *Using System Availability Management*.

Real User Monitor Issues

- Real User Monitor supports non-Latin characters in UTF-8 format. For details on configuring the HP Real User Monitor probe to support non-Unicode encodings, see "Configuring the HP Real User Monitor Probe for I18N" in the *Real User Monitor Administration* PDF.
- To support non-Latin characters from Real User Monitor, the encoding for HP Business Service Management databases must be defined as UTF-8, or set to the specific language. For further details, see "Database Environment Issues" on page 143.
- The Real User Monitor Probe Windows installation screens are not translated and are in English only. For details on installing the Real User Monitor Probe, see "Installing the HP Real User Monitor Probe" in the *Real User Monitor Administration* PDF.

End User Management Administration Issues

- Global replace does not support non-English languages.
- When accessing the Status Snapshot in End User Management (**Applications** > **End User Management** > **Status Snapshot**), certain characters appear unreadable. To resolve this, ensure that you have installed files for East Asian Languages on your local machine, as follows:

  Select **Start** > **Control Panel** > **Regional and Language Options** > select the **Languages** tab > select **Install Files for East Asian Languages**.

Data Flow Management Issues

- When exporting a CI instance to a PDF file, Japanese characters are not displayed in the PDF file. (**Data Flow Management** > **Discovery Control Panel** > **Basic Mode.** Run discovery. When finished, select a CIT in the **Statistics Results** pane. Click the **View Instances** button. In the Discovered by dialog box, select **Export Data to File** > **Export Displayed CIs to PDF.**)

Multilingual Issues

- The SNMP notification method does not support multilingual text, and can only send a notification in the character set of the Gateway Server machine. This is because HP Business Service Management uses SNMP version 1.0, which does not support multilingual data.
- Error messages in the Failed Transactions report do not display correctly when HP Business Service Management runs on an English operating system, and the Business Process Monitor runs on a Japanese operating system. To access the Failed Transactions report, select **Applications** > **End User Management** > **Business Processes** > **Error Summary**. Locate the General Errors table, and click a link to open the Failed Transactions window.
- HP Business Service Management can store multilingual data. However, a regular executable cannot usually accept multilingual data on the command line.

The following table describes the procedures that you must perform to add multilingual data to the command line when running an executable file upon alert:

Platform	Procedure
Windows	To prevent multilingual data from being lost, write the application with a **wmain** function instead of a **main** function. You can also use another **main**-type function that can take command line parameters of type **wchar** instead of type **char**. **Note:** When you use the SubAlerts command line option, the created XML file does not include an encoding attribute, and the encoding is different from the default UTF-8 encoding.
Solaris	Inform the writer of the application that the parameters passed to the application must be encoded in UTF-8.

For details on using a custom command line when running an executable file upon alert, see "Run Executable File Dialog Box" in *Using End User Management*.

- An executable file that was created for a previous version of HP Business Service Management is compatible with a multilingual version.

Multilingual User (MLU) Interface Support

The HP Business Service Management user interface can be viewed in the following languages in your Web browser:

Language	Language Preference in Web Browser
English	English
French	French (France) [fr]
Japanese	Japanese [ja]
Korean	Korean [ko]
Simplified Chinese	Chinese (China) [zh-cn]

The following are languages in which HP Business Service Management can operate but the user interface of only ODB-related pages are presented in the language.

Language	Language Preference in Web Browser
Dutch	Dutch (Netherlands) [nl]
German	German (Germany) [de]
Portuguese	Portuguese (Brazil) [pt-br]
Russian	Russian [ru]
Spanish	Spanish [es]
Italian	Italian (Italy) [it]

Use the language preference option in your browser to select how to view HP Business Service Management. The language preference chosen affects only your local machine (the client machine) and not the HP Business Service Management machine or any other user accessing the same HP Business Service Management machine.

To set up and view HP Business Service Management in a specific language:

1 Install the appropriate language's fonts on your local machine if they are not yet installed. If you choose a language in your Web browser whose fonts have not been installed, HP Business Service Management displays the characters as squares.

2 If you are logged in to HP Business Service Management, you must log out. Click **LOGOUT** at the top of the HP Business Service Management window.

Close every open browser window or alternatively clear the cache (if HP Business Service Management is running on Internet Explorer).

3 If HP Business Service Management is running on Internet Explorer, configure the Web browser on your local machine to select the language in which you want to view HP Business Service Management (**Tools** > **Internet Options**).

a Click the **Languages** button and in the Language Preference dialog box, highlight the language in which you want to view HP Business Service Management.

b If the language you want is not listed in the dialog box, click **Add** to display the list of languages. Select the language you want to add and click **OK**.

c Click **Move Up** to move the selected language to the first row.

d Click **OK** to save the settings.

e Display the HP Business Service Management login window.

f From the Internet Explorer menu, select **View** > **Refresh**. HP Business Service Management immediately refreshes and the user interface is displayed in the selected language.

Note: For details on viewing Web pages in Internet Explorer that are written in a different language, see http://support.microsoft.com/kb/306872/en-us.

---

4 If HP Business Service Management is being viewed on FireFox, configure the Web browser on your local machine as follows:

a Select **Tools** > **Options** > **Advanced**. Click **Edit Languages**. The Language dialog box opens.

b Highlight the language in which you want to view HP Business Service Management.

If the language you want is not listed in the dialog box, expand the **Select language to add...** list, select the language, and click **Add**.

c Click **Move Up** to move the selected language to the first row.

d Click **OK** to save the settings. Click **OK** to close the Language dialog box.

Notes and Limitations

- There is no language pack installation. All translated languages are integrated into the HP Business Service Management Multilingual User Interface (MLU).
- Data remains in the language it is entered in, even if the language of the Web browser changes. Changing the language of the Web browser on your local machine does not change the language of any data that was entered by a user.
- You cannot deploy a package if the server locale is different than the client locale and the package name contains non-Latin characters. For details, see "Package Manager" in the *ODB Administration Guide*.
- You cannot create a package that contains resources (for example, views and TQLs) having non-Latin characters in their names, if the server locale is different from the client locale. For details, see "Package Manager" in the *ODB Administration Guide*.
- In the Modeling Studio, you cannot create a new view if the view's name contains more than 18 Japanese characters. For details, see "Modeling Studio" in the *ODB Administration Guide*
- The HP Business Service Management server status HTML page appears only in English. It is not translated into any other language. For details, see "Post-Deployment" in the *HP Business Service Management Deployment Guide* PDF.

Part III

Data Enrichment

10

Location Manager

This chapter includes:

Concepts

Tasks

Reference

Concepts

Location Manager Overview

The Location Manager is used to define geographical and logical location CIs and assign them ranges of IP addresses. Location CIs can be attached to any other CI. They are used, for example, to attach a location to a Business Process Monitor (BPM) agent or a page discovered automatically by Real User Monitor (RUM).

You access the Location Manager from:

- **Admin** > **Platform** > **Locations**

You can also:

- Access Location Manager from End User Management Administration (**Admin** > **End User Management** > **Settings** > **Business Process Monitor Settings** > **BPM Agents**). Click to open the Change Agent Location dialog box.
- View location CIs in the IT Universe Manager (**Admin** > **ODB Administration** > **Modeling** > **IT Universe Manager**). To see location CIs, select **Locations** view.

Location Manager is accessible to users who have Administrator predefined permissions. Permissions are configured in **Admin** > **Platform** > **Users and Permissions**.

Location Details and Descriptions

- **Location Entity.** An entity that describes a place in the world. It may be a geographical location, such as a country or city, or a logical location, such as a building. The location entity may be connected to devices and logical CIs representing end-users or data center locations.
  - **Geographical Location**. An absolute location in the world, selected from a predefined list of cities/states/countries, and assigned specific geographical coordinates

  - **Logical Location.** A user-defined virtual location, which may or may not relate to a real location in physical space. If a user assigns geographical coordinates to a logical location, these coordinates can be changed or deleted.

- **Hierarchy.** Locations may be nested under other locations, creating a hierarchical tree with a maximum of seven levels under the root.

- **Geographical Coordinates.** Longitude/latitude values, in degrees (expressed as decimal fractions). Coordinates are assigned to individual locations.

- **Default Container.** The parent location for all locations discovered automatically by Real User Monitor (RUM). By default, the Default Container is **World** (the root of the Locations tree), but any location on the tree can be set as the Default Container.

- **IP Ranges.** Each location may be assigned a set of IP ranges. An IP range is a range of IP addresses that have been designated for use by devices in a certain geographical area.

Populating the Location Manager

Location Manager can be populated with locations in a number of ways:

- **Using the Location Manager in Platform Admin.** For details on the user interface, see "Location Manager Page" on page 167.

- **Mass upload from an XML file.** BSM enables you to create and define location CIs using an XML file external to the user interface. Mass upload is an alternative to using the user interface, and better suited for defining a large number of locations.

  For details, see "Creating and Working with the XML File" on page 159.

- **Using Real User Monitor (RUM).** When RUM encounters an IP address for which the location is unknown, that IP is propagated to the Location Manager for location discovery. The Location Manager then searches in the Hexasoft IP2Location repository for a geographical location that matches the given IP address. If a match is found, new locations are created in the Location Manager for the IP address. Depending on the information in the IP addresses repository, at most three locations (country, state, and city) may be created for each IP address.

Note: If End User Management (EUM) is enabled after being disabled, it may take a few hours until automatic discovery of locations starts to work. This is the time that it takes for the IP-to-location information to load into the database.

Creating and Working with the XML File

You can define your own hierarchy of locations by creating an XML file and loading it through a Java Management Extensions (JMX) console. (For details on accessing and using the JMX, see "Using the JMX Console".)

The XML can be generated and edited in any tool that supports text. You can create the file yourself, or base it on an XML file created by BSM in the JMX console, which already includes the tags, elements, and attributes necessary for the mass upload XML file.

XML File Details

For a reference detailing all the XML tags, elements, and attributes included in the mass upload file, see "XML Tag Reference" on page 177.

Each mass upload XML must begin with the following declarations:

- **<?xml version="1.0" encoding="UTF-8"?>** This states that this is an XML file with UTF-8 character encoding.
- **<!DOCTYPE locations_manager SYSTEM "./locations.dtd">** This is the document type declaration. The **locations.dtd** file is located in the **HPBSM/conf/locations** folder. The path to **locations.dtd** must be specified relative to the location of your XML file, and may need to be updated. If your XML file is saved in the same location as **locations.dtd**, no path is necessary.

  The XML file is validated using the **locations.dtd** file. If the XML structure is incorrect, you get a SAXParseException and the operation fails. If the DOCTYPE line does not correctly reference the path of the **locations.dtd** file, validation and the entire operation fails.

Note: Populating the location manager through XML results in deletion of all locations that were previously defined in the Location Manager.

XML File Example

In this example, customer 1 wants to upload an XML file to create a hierarchy of locations in Location Manager, as follows: The first location, a site in Los Angeles, includes geographical coordinates, ISP address ranges, and ISPs. Locations 2 and 3 are nested under the first location (Los Angeles), and 2a and 2b are under 2. Location 4 is parallel to Los Angeles in the hierarchy.

World

- Los Angeles; latitude 34.0396, longitude -118.2661; ISPv4 address range 4.38.41.136 to 4.38.80.152 (ISP = Level 3 Communications); ISPv6 address range 2002:0C19:8B00:0000:0000:0000:0000:0000 to 2002:0C19:B28F:0000:0000:0000:0000:0000 (ISP = AT_T WorldNet Services)
  - location_2
    - location_2a
    - location_2b
  - location_3
- location_4

Note: There is no need to add the World root location.

The XML file used to upload this hierarchy of locations is as follows:

```
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE locations_manager SYSTEM "conf/locations/locations.dtd">
<locations_manager>
    <customer_hierarchy customer_id="1">
        <locations_list>
            <location location_name="Los Angeles">
                <latitude>34.0396</latitude>
                <longitude>-118.2661</longitude>
                <ip_ranges>
                    <ip_range>
                        <start_ip>4.38.41.136</start_ip>
                        <end_ip>4.38.80.152</end_ip>
                        <isp>Level 3 Communications</isp>
                    </ip_range>
                    <ip_range ip_v6="true">
                        <start_ip>2002:0C19:8B00:0000:0000:0000:0000:0000</
start_ip>
                        <end_ip>2002:0C19:B28F:0000:0000:0000:0000:0000</
end_ip>
                        <isp>AT_T WorldNet Services</isp>
                    </ip_range>
                </ip_ranges>
                <locations_list>
                    <location location_name="location_2">
                        <locations_list>
                            <location location_name="location_2a" />
                            <location location_name="location_2b" />
                        </locations_list>
                    </location>
                    <location location_name="location_3" />
                </locations_list>
            </location>
            <location location_name="location_4" />
        </locations_list>
    </customer_hierarchy>
</locations_manager>
```

For information on each of the XML elements and attributes, see "XML Tag Reference" on page 177.

Tasks

How to Populate the Location Manager

The Location Manager can be populated with location CIs in a number of ways. You can:

- "Create locations with the user interface" on page 162
- "Populate the Location Manager using an XML file" on page 162

Create locations with the user interface

Use the Locations Manager user interface to create, edit, and manage locations and assign them IP ranges. For details about the user interface, see "Location Manager Page" on page 167.

Populate the Location Manager using an XML file

Upload location CIs to the Location Manager using an XML file external to the user interface. Mass upload is an alternative to using the user interface, and better suited for populating the Location Manager with a large number of locations.

For details on this task, see "How to Update Locations Using Mass Upload" on page 163.

How to Update Locations Using Mass Upload

This task describes how to load an XML file, change an existing location hierarchy using XML, and view the results.

To create and modify an XML file to upload locations:

1 Create an XML file with no IDs for the locations in the following ways:

- ➤ Create the file yourself in any tool that supports text. Save the XML file you created to a network location accessible to the BSM server. For details, see "Creating and Working with the XML File" on page 159. For details on the XML file elements and attributes, see "XML Tag Reference" on page 177.
- ➤ Export the current hierarchy as XML using the JMX console, as described in the steps below.

2 Open the JMX console on this machine. (For detailed instructions, see "Using the JMX Console" on page 25.)

3 Under the **BSM-Platform** section, select **service=Locations Manager**.

4 If you are creating an XML file from the current hierarchy, invoke the **convertLocationsHierarchyToXML** method entering the following values:

- ➤ **customerId**. By default, use 1 for **customerID**. If you are an HP SaaS customer, use your HP SaaS customer ID.
- ➤ **target path.** The location where you want to save the XML file.

5 Locate and edit the XML file just saved:

a Check that the list of existing locations looks accurate. The World root location is not included in this XML file.

b To add a new location, no ID should be defined.

c To modify a location, change the fields, but do not change the real ID.

d To delete a location, delete all its details from the XML file.

e To change a location’s position in the hierarchy, move the location with its real ID to another position in the XML file.

f Save the XML file you created to a network location accessible to the BSM server.

Tip: Save the XML file into the same directory as the **locations.dtd** file so you do not have to reference a different path in the document type declaration line of the XML file. The **locations.dtd** is located in the **<HPBSM root directory>\conf\locations** directory.

6 To upload your edited XML file, in the JMX **service=Locations Manager**, invoke the **buildLocationsHierarchyFromXML** method.

a In **xmlFilePath**, enter the path to the location where you saved the XML file.

b In the **saveInFile** parameter, choose **True** to save the existing locations hierarchy in the file **<HPBSM root directory>\conf\locations\current_locations_hierarchy.xml**.

Notes:

- The XML file must comply with the rules listed below. If any of the rules are violated, **buildLocationsHierarchyFromXML** will abort before any changes are made to the locations model:

  1. No two locations in the hierarchy may have the same name.

  2. A maximum of seven levels of hierarchy can be defined.

  3. No two locations may have the same ID.

  4. All location ID values in the XML must match an existing location with that ID.

  5. No two overlapping IP ranges are allowed.

- Saving the existing hierarchy in a file may lengthen the time required to load the new XML file.

7 The locations have now been uploaded to the Location Manager. They are visible on the Locations Tree of the user interface and through the JMX console.

To view through the JMX:

➤ Under **service=Locations Manager,** locate the **getAllLocations** method.

➤ Enter the relevant customer ID. By default, use 1 for **customerID**. If you are an HP SaaS customer, use your HP SaaS customer ID.

➤ Invoke the method and check that all your locations are there, including the World root location.

Reference

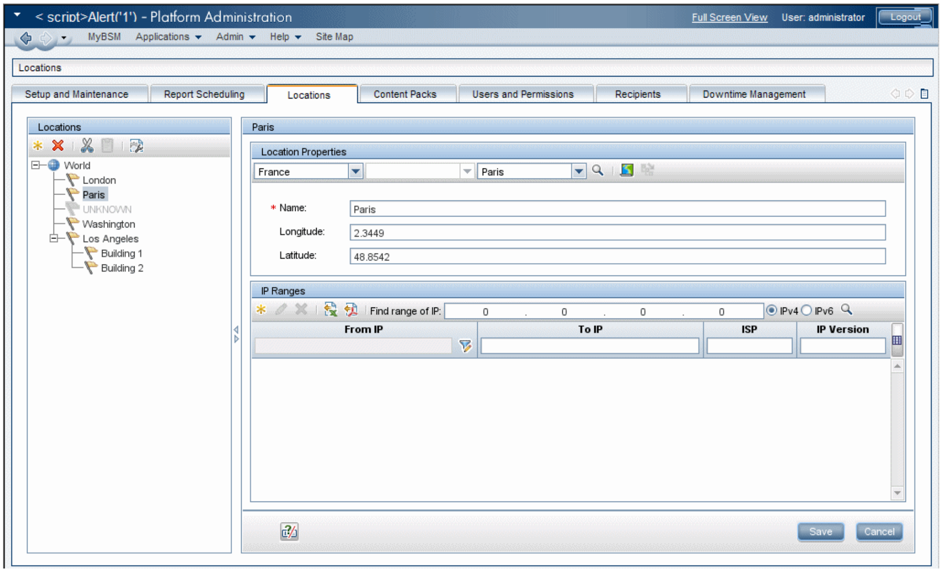
Location Manager User Interface

This section includes:

- Location Manager Page on page 167
- New/Edit IP Range Dialog Box on page 174
- Geographical Map Dialog Box on page 175

Location Manager Page

This page enables you to manage locations and assign them IP ranges.



* Name: Paris

Longitude: 2.3449

Latitude: 48.8542

Find range of IP: 0 . 0 . 0 . 0 ● IPv4 ○ IPv6

To access	Select **Admin** > **Platform** > **Locations**
Relevant tasks	"How to Populate the Location Manager" on page 162
See also	"Location Manager Overview" on page 156

Locations Area - Left Pane

In the Locations area, on the left pane of the Locations page, you can add, delete, move, and search for locations, and set a location as the default container. Locations appear in a tree structure, with a maximum of seven hierarchical levels, whose root is called **World**.

User interface elements are described below. You can also access these actions from a context menu by right-clicking on the Locations area of the left pane:

UI Elements	Description
✱	**Add location**. Click to add a new location below the selected location. Opens the Location Properties area.
✗	**Delete location**. Click to delete a location and its children locations. A **Confirmation** window opens, asking if you are sure you want to delete the location, and warning that the location may be in use by other BSM components and that there is no undo for this action. If you delete a location, any IP ranges assigned to it or its children can be moved to its parent location. To do this, select the **Move IP Ranges to the Parent Location** check box in the **Confirmation** window.
✂	**Cut location**. Click to cut a location. The location is copied to the clipboard, and can be pasted below another element in the locations tree. **Note:** When a location is cut, it remains visible, grayed out, in its former place on the tree, until it has been pasted in a different position. To deselect a cut location before it has been pasted to a different position, and return it to its original position, click **Cut location** again.

UI Elements	Description
📋	**Paste location.** Available when a location has been cut and the user has navigated to another part of the tree. **Note:** Locations may be pasted under other locations, creating a hierarchical tree with a maximum of seven levels under the root. Assigning the same name to brother locations under the same parent, or to a location under World and a location in another place in the tree, is not permitted.
	Set as default container. Click to set a particular location as the default container. This is the parent location for all automatically discovered locations. For more information, see "Location Manager Overview" on page 156.

Location Properties Area

In the Location Properties area, you can set a geographical location and its coordinates from a predefined list of countries and areas, states, and cities; or name a logical location and set its geographical coordinates. Defining a location as a geographical location allows auto-discovery to automatically assign discovered IP addresses to the location. To define a location as a geographical location, select the appropriate country/state/city (country alone, country/state, or country/city may be selected as well) and click 🔍.

Note: Geographical location can only be set from a predefined list. If you manually enter the name of a location, it is created as a logical location.

User interface elements are described below:

UI Elements	Description
<Country or Area>/ <State>/<City>	Use the first and third drop-down controls to select country or area and city. When USA is selected as country, the middle drop-down becomes available, and can be used to select a particular state.
🔍	**Set geographical location.** Click to locate the geographical coordinates (longitude and latitude) of the selected country/state/city and automatically enter name and coordinates into the appropriate fields under Location Properties, thus defining the location as a geographical location.
🗺	**Select Location Coordinates.** Click to launch the Geographical Map dialog box, which can be used to select the geographical coordinates of any location. If geographical coordinates were previously entered into the **Longitude** and **Latitude** boxes, these are passed to the Geographical Map dialog box, which opens with a pin on that location. For more information, see "Geographical Map Dialog Box" on page 175.
⧉	**Get coordinates from nearest parent.** Click to copy the geographical coordinates of the closest parent location with coordinates, to the selected location.

UI Elements	Description
Name	Enter the name of the location in the **Name** text box. **Notes:** ➤ The name field is mandatory. Assigning the same name to brother locations under the same parent, or to a location under World and a location in another place in the tree, is not permitted. Assigning the same name to more than one location under different parents is permitted, but a small caution symbol displays, indicating that the name has already been defined for another location in the tree and suggesting that the name here be changed. ➤ If you change a name of geographical location, it becomes a logical location.
Longitude/Latitude	Enter the longitude and latitude of the location in the longitude and latitude text boxes. If you select a location from the predefined drop-down lists of countries, states, and cities, or from the Geographical Map dialog box, the longitude and latitude boxes are filled automatically.

IP Ranges Area

You can use the IP Ranges area to assign IP ranges to a location. Real User Monitor (RUM) then uses these ranges to assign newly discovered pages and other CIs to particular locations.

The table of IP ranges may contain thousands of pages. To view the table in a single file, you can export it in Excel or Adobe Acrobat (PDF) formats.

User interface elements are described below:

UI Elements	**Description**
✳	**New IP Range**. Click to create a new IP range. Opens the New IP Range dialog box. **Note:** A particular IP range can be assigned to only one location at a time. ➤ If you try to assign an IP range that overlaps with a parent IP range, a message displays, warning that this action will remove the IP range from the parent location. (Only the area of overlapping ranges is removed, and the parent IP ranges are adjusted accordingly.) Click **Remove from Parent** to remove the overlapping IP range from the parent and reassign it to the selected location, or **Cancel**. ➤ If you try to assign an IP range that overlaps with a range already assigned to another location (not a parent), an error message is displayed and a different IP range must be chosen.
✎	**Edit IP Range**. Click to edit a selected IP range. Opens the Edit IP Range dialog box.
✖	**Delete IP Range**. Click to delete one or more selected IP ranges.
X	**Export to Excel**. Click to export IP range information for the selected location to an Excel spreadsheet.
📄	**Export to PDF**. Click to export IP range information for the selected location to an Adobe Acrobat file.
▥	**Change Visible Columns.** Click to select which columns of IP range information are visible in the IP Ranges area. The Choose Columns to Display dialog box opens. **Note:** Columns not displayed on screen are also not exported to Excel or Adobe Acrobat (PDF) files.

UI Elements	Description
Find Range of IP	To find an existing range in which a particular IP address is located: ➤ Select the appropriate radio button: ➤ **IPv4** (Internet Protocol version 4) for addresses consisting of four numbers, each ranging from 0 to 255, in dot-decimal notation) ➤ **IPv6** (Internet Protocol version 6) for addresses consisting of eight hexadecimal numbers, each ranging from 0 to FFFF, in colon-separated notation) ➤ Enter the IP address in the **Find Range of IP** box. ➤ Click 🔍. The range in which the IP address is found is highlighted. **Note:** This searches for the IP range in the currently selected location only.
From IP/To IP, ISP, IP Version	To filter the IP ranges for a particular string of text in their lower and upper IP range limits, ISP names, or IP versions, enter the string in the **From IP**, **To IP**, **ISP**, or **IP Version** boxes. These boxes may be used in combination with each other. An asterisk (*) may be used as a wildcard to represent one or more characters. For example: ➤ To filter for IPv6 addresses, enter "6" in the **IP Version** box ➤ To filter for IPv4 address ranges whose upper limits end in 0, enter "*.*.*.0" in the **From IP** box.

New/Edit IP Range Dialog Box

To access	Select **Admin** > **Platform** > **Locations** and click ✱ under IP Ranges.

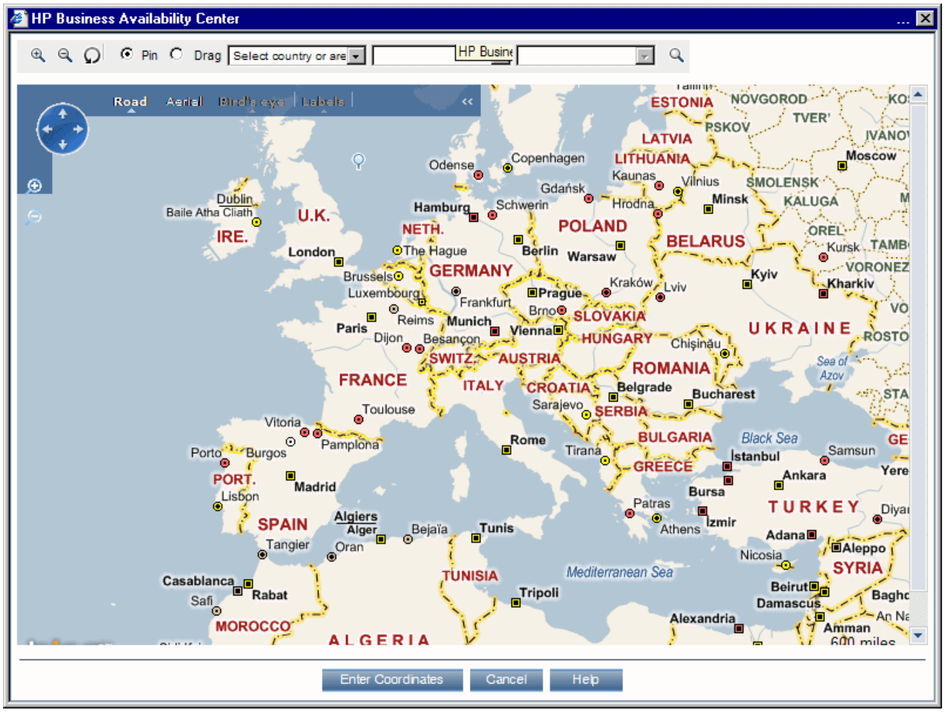
User interface elements are described below:

UI Elements	Description
IP version	Choose **IPv4** or **IPv6** to select: ➤ Internet Protocol version 4 (for IP addresses consisting of four numbers, each ranging from 0 to 255, in dot-decimal notation) ➤ Internet Protocol version 6 (for IP addresses consisting of eight hexadecimal numbers, each ranging from 0 to FFFF, in colon-separated notation)
From IP/To IP	Use the **From IP** and **To IP** boxes to set the range of IP addresses for the location. ➤ For IPv4, as you enter an IP address in the **From IP** box, a corresponding address ending with 255 is automatically entered into the **To IP** box. All values in both boxes may be changed to any permissible value (0-255), but the address in the **To IP** box must be the same or higher than the address in the **From IP** box. ➤ For IPv6, as you enter an IP address in the **From IP** box, the same address is automatically entered into the **To IP** box. All values in both boxes may be changed to any permissible value (0-FFFF), and the address in the **To IP** box may be higher, the same, or lower than the address in the **From IP** box.
ISP	Specify the Internet Service Provider in the **ISP** box.

Geographical Map Dialog Box

This dialog box enables you to select the geographical coordinates of any location.

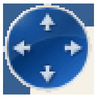
Note: Users who are not connected to the Internet see another version of this map.



To access	From the Location Properties area of the Locations page, click 🗺 .
Important information	If geographical coordinates were previously entered into the **Longitude** and **Latitude** boxes, these are passed to the Geographical Map dialog box, which opens with a pin on that location.
Relevant tasks	"How to Populate the Location Manager" on page 162
See also	"Location Manager Page" on page 167

User interface elements are described below:

UI Elements	Description
🔍	**Zoom In**. Click to zoom in on the map. **Note:** This icon is located on the toolbar. Another **Zoom In** icon with identical functionality appears on the map, itself.
🔍	**Zoom Out**. Click to zoom out on the map. **Note:** This icon is located on the toolbar. Another **Zoom Out** icon with identical functionality appears on the map, itself.
⟳	**Reset**. If you open Geographical Map at particular coordinates and then pan elsewhere, click **Reset** to recenter the map at the starting coordinates.
Pin/Drag radio buttons	Select **Pin** to move the pin to any location on the map by clicking on that location. Double-clicking moves the pin and zooms in on the location. Select **Drag** to drag the map.
<**Country or Area**>/ <**State**>/<**City**>	Use the first and third drop-down controls to select country or area and city. When USA is selected as country, the middle drop-down becomes available, and can be used to select a particular state.
🔍	**Find location on map.** Click to locate the selected country or area and city on the map.

UI Elements	Description
	**Pan in Any Direction.** Hold down the mouse button on this control and drag to pan across the map.
Road View	Click to see a road map of the world.
Aerial View	Click to see an aerial photographic map of the world.
Bird's Eye	The bird's-eye view is disabled.
Labels	In Aerial View, click to display or hide map labels. This is disabled in Road View.
Enter Coordinates	Click to automatically copy the coordinates of the pinned location to the **Longitude** and **Latitude** boxes of the Location Properties area.

XML Tag Reference

Following are tables that list all the elements and attributes that are used in the mass upload XML file.

Elements Table

Element	Description	Attributes
locations_manager	Initial element in a block containing Location Manager data	
customer_hierarchy	Initial element in a hierarchy of locations for a particular customer	customer_id
locations_list	Initial element in a list of locations	
location	Initial element in block defining attributes for a particular location	location_name
latitude	Latitude of the location, in degrees	
longitude	Longitude of the location, in degrees	
ip_ranges	Initial element in a list of IP address ranges for a particular location	

Element	Description	Attributes
ip_range	Initial element in block defining attributes for a particular IP address range	ip_v6
start_ip	Lower limit of IP address range IP address ranges may be IPv4 or IPv6. Location Manager supports the following notation formats: IPv4 – number of 4 bytes IPv4 – string in x.x.x.x format IPv6 – number of 16 bytes IPv6 – string in x:x:x:x:x:x:x:x format IPv6 – IPv6 regular expression	
end_ip	Upper limit of IP address range. For supported IPv4 and IPv6 notation formats, see start_ip, above.	
isp	Name of ISP for the range	

Attribute Table

Attribute	Parent Element	Description	Example
customer_id	customer_hierarchy	Number. Unique and mandatory. ID number of the customer for whom a hierarchy of locations is built.	<customer_hierarchy customer_id="1">

Attribute	Parent Element	Description	Example
location_name	location	String. Mandatory. Not unique (several locations can have the same name). Name of a particular location.	<location location_name="Los Angeles">
ip_v6	ip_range	Boolean. ="true" if IP addresses for a particular range are in IP version 6 format. Otherwise, they are in IP version 4 format.	<ip_range ip_v6="true">

Implied Attribute Table

The following attributes are exported when exporting the current hierarchy as XML but are not required when defining new locations in the XML. When updating an existing location through XML, these attributes need to be preserved:

Attribute	Parent Element	Description
original_geo_location_id	location	Used to identify geographical locations
location_type	location	Possible values: ➤ "undefined" (default) ➤ "country" ➤ "state" ➤ "city"
location_id	location	The real ID of an existing location

Example:

```
<location location_name="UNKNOWN" location_type="undefined"
location_id="47a3711c334fd8577858c6da60b3e0e6"
original_geo_location_id="Unknown_Unknown">
```

11

Content Packs

This chapter includes:

Concepts

Tasks

Reference

Concepts

Content Packs Manager

Content is information that BSM uses to describe and enrich the objects or configuration items that you are monitoring in your IT environment. The objects can be, for example, network hardware, operating systems, applications, services or users. Content is used to enrich the configuration item data.

Content for a specific management area can be contained in a dedicated content pack. A content pack can contain a complete snapshot of all, or any part of, your content -- the rules, tools, mappings, indicators and assignments that you define and configure to help users manage your IT environment. Content packs are used to exchange customized data between instances of BSM, for example in test and production environments.

For details about the types of content you can include in a content pack, see "Content Pack Content Types" on page 208.

The Content Packs Manager helps you manage packs of content data. It enables you to create a content pack, save it in a file, install or update content, and take content from one installed instance of BSM and upload it to another, using the export and import features.

BSM provides a number of content packs definitions for Smart Plug-ins (SPIs) that you can either use in the default configuration or, if necessary, modify to suit the demands of your environment.

Note: To install new or update existing content in the ODB, you use Packages. For details, see Package Manager, in the *ODB Administration Guide*.

You can use the Content Packs Manager to perform the following tasks:

- Define the contents of a content pack and save the definition. For details, see "Defining Content Packs" on page 184.
- Manage dependencies between content packs. For details, see "Dependencies in Content Packs" on page 185.
- Export a content pack (definition and content) and the data it references to a file called a content pack. For details, see "Exporting Content Packs" on page 187.
- Import a content pack (definition and content) and the data it references. For details, see "Importing Content Packs" on page 188.

Note: You can use permissions to grant and restrict access to the Content Packs Manager. Permissions for using the Content Packs Manager are found in **Admin** > **Platform** > **Users and Permissions** > select **Operations Management** context > **Administrative UIs** > **Content Packs**.

Content Packs Manager Interfaces

The Content Packs manager has two interfaces:

- **BSM Content Packs graphical user interface (GUI)**

  You can start the BSM Content Packs manager using one of the following menu options:

  Admin > **Platform** > **Content Packs**

  Admin > **Operations Management** > **Manage Content** > **Content Packs**

  For details, see "Content Packs Manager Graphical User Interface" on page 192.

- **ContentManager command-line interface (CLI)**

  The features and functionality of the Content Pack manager are also accessible using the **ContentManager** command-line interface. You can access the ContentManager command-line interface directly, in a shell, or remotely, for example, in a script.

For details, see "Content Pack Manager Command-Line Interface" on page 211.

Note: You cannot use the ContentManager command-line interface to create a content pack definition.

Defining Content Packs

A content pack definition contains a list of the data to be included in a content pack when you use the Export feature to prepare a content pack for exchange with another BSM installation.

The content pack definition defines the original relationships to CI types and any relationships between the included items. The content pack definition does not include the CI types themselves. To exchange CI types, use the features provided by the ODB.

The **Content Packs Definitions** pane enables you to view and manage the content pack definitions. For example, you can perform the following actions:

- Create, modify, and save a content pack definition
- Delete a content pack definition
- Export or import an existing definition along with the data it references

Creating a content pack is a two-step process. First you create the content pack definition in the Content Manager, and then you use the definition to export selected content to a content pack file in XML format.

Dependencies in Content Packs

Some content in BSM is part of a hierarchy that may relate to and depend upon other content. When you select content for inclusion in a content pack, its dependent content must also be included, either as part of the same content pack, or referred to from another content pack that will also be uploaded. For example, if you include a KPI assignment, any indicators, KPIs, menus, or rules necessary for this KPI assignment must also be included.

Automatically Including Dependent Content

If you select content that has dependent content, and the dependent content is not part of another content pack, the dependent content is automatically included in the content pack definition along with the content that requires it.

For example, the correlation rule **Database Affects WebApp** requires two indicators: the DB Tablespace indicator **Extend TS** and the J2EE Application indicator **Web application state**. If you include Database Affects WebApp in a content pack definition and the indicators **Extend TS** and **Web application state** are not included in other content packs, they are automatically included in this content pack definition.

Referencing Dependent Content Included in Another Content Pack

If dependent content is already included in another content pack, by default the new content pack references its inclusion in the other content pack rather than including it in both. You can, however, use the Dependencies page to also add it to the included content in the new content pack.

For example, if content pack definition A includes the indicator **Extend TS** and now you select the correlation rule **Database Affects WebApp** (which depends on **Extend TS**) for inclusion in Content Pack B, Content Pack B references the inclusion of **Extend TS** in Content Pack A.

On the Content Pack B Dependencies page, **Extend TS** is listed in bold, under Content Pack A. To include **Extend TS** in Content Pack B (and thus, in both contact packs), select it and click **Add to Included Content**.

Deleting Referenced Content Pack

If you delete a referenced content pack containing dependent content, the dependent content is automatically added to the content pack definition that depends on it.

For example, if Content Pack B includes the correlation rule **Database Affects WebApp** and references the dependent indicator **Extend TS** in Content Pack A, and you delete Content Pack A, **Extend TS** is automatically included in Content Pack B.

Note: You are warned via a pop-up message if you delete a referenced content pack containing dependent content.

Setting Dependency

If dependent content is included in more than one other content pack, you can select which content pack to reference. This is called setting dependency.

For example, if Content Packs A and B both include the indicator **Extend TS** and you select the correlation rule **Database Affects WebApp** (which depends on **Extend TS**) for inclusion in Content Pack C, you can set dependency in Content Pack C to reference **Extend TS** in either Content Pack A or B.

Deleting Referenced Content Pack on Which Dependency Was Set

If you delete a referenced content pack on which dependency was set, the dependent content is automatically added to the content pack definition that depends on it. You can set dependency to another content pack manually, but it is not set automatically.

For example, if Content Packs A and B both include the indicator **Extend TS,** and Content Pack C includes the correlation rule **Database Affects WebApp** (which depends on **Extend TS**) and has dependency set to reference **Extend TS** in Content Pack A, and then you delete Content Pack A, **Extend TS** is automatically included in Content Pack C. You can then set dependency to **Extend TS** in Content Pack B, but it is not set automatically.

Exporting Content Packs

Using the Content Packs Manager, you can export configuration data to a file. The content pack contains the references to configuration data, and the referenced data. The exported content pack is an XML file whose contents you can view in a text editor.

The configuration data in a content pack makes references to configuration items stored in the ODB used by the system from which the content pack was exported. If these configuration items are not present in the ODB used by the system into which you want to import the content pack, the configuration data in the content pack cannot work.

Tip: Use the features provided by the ODB to export and import configuration items.

For details about exporting content packs, see "Export content packs" on page 190.

Importing Content Packs

When starting an import action, you can specify whether to overwrite any existing data or leave the existing data unchanged (**Ignore**), only adding new data.

If you want to run a test of the import operation without actually importing any of the listed data, you can use the **Test** feature. The Test feature is a useful way to list any unresolved dependencies (for example, to unknown CI types) contained in the imported content pack definition.

For details about the task, see "Import content packs" on page 190. For details about the user interface and the options available in the import operation, see "Import Content Pack Dialog" on page 206.

Tasks

How to Create and Manage Content Packs

The following steps describe how to create, export and import content packs.

- "Create and edit content pack definitions" on page 189
- "Export content packs" on page 190
- "Import content packs" on page 190

Create and edit content pack definitions

To create and edit a content pack definition:

1 Open the Content Packs Manager: **Admin** > **Platform** > **Content Packs**.

- To create a new content pack definition, select the ✱ button. The **Create New Content Pack Definition** wizard opens.
- To edit an existing content pack definition, select it and click ✎. The Edit Content Pack Definition dialog box opens.

2 In the General page of the wizard, or the General tab of the dialog box, the fields **Display Name**, **Name**, and **Version** are required.

Name must be unique, and is limited to a maximum length of 80 characters. The first character must be a letter (A-Z, a-z) or an underscore (_). All other characters may be letters, numbers, or underscores. No leading or trailing spaces are allowed. When you export the content pack, this is the default file name for the XML file, with **OMi Content Pack -** as a prefix.

Display Name is the name displayed in the Content Pack Definitions list, and need not be unique. It is limited to a maximum length of 255 characters.

Version is a free text field. Use **Version** in combination with **Display Name** to manage revision control of your content packs.

3 Continue to follow the wizard pages or edit the tabs of the dialog box to select content, set dependencies, and see a summary of your content pack definition's contents and any problems found.

For details on the user interface of and all the available options, see "Create New Content Pack Definition Wizard" on page 197.

Export content packs

To export a content pack:

1 Open the Content Packs Manager: **Admin** > **Platform** > **Content Packs**

2 In the **Content Pack Definitions** pane, select the content pack that you want to export.

3 To export the selected content pack to an XML-format file, select the button, select the location where you want to save the content pack, and select **Save**.

Tip: By default, BSM saves the content pack to the file system on the system where you are running the Content Packs Manager. If you want to save the file in an alternative location, make sure that you have access to that location.

Import content packs

To import a content pack:

1 Open the Content Packs Manager: **Admin** > **Platform** > **Content Packs**

Select the button in the **Content Pack Definitions** pane to open the Import Content Pack dialog box.

2 In the Import Content Pack dialog box, use the **Browse (...)** button to locate the content pack you want to import. The default location for content packs is:

<HPBSM root directory>\conf\opr\

In a distributed deployment, this directory is located on the data processing server.

Note: By default, BSM looks for content packs in the file system on the system where you start the browser session. If the browser is running on a remote system, you must navigate to the file system of the BSM host.

3 Choose **Overwrite** to overwrite existing items with the same ID, or **Create** to only import new items, leaving existing items as they are. You can also select **Test** to run the import in test mode. In test mode, changes are not committed, so you can see if any problems exist before running an actual import.

Unresolved references in the imported definition (for example, to unknown CI types) are not allowed.

4 Select **Import** to start the import or test operation.

For details about the Import Content Pack dialog box, see "Import Content Pack Dialog" on page 206.

Reference

Content Packs Manager Graphical User Interface

This section includes:

- Create New Content Pack Definition Wizard on page 197

Content Packs Page

This area enables you to manage content pack definitions. A content pack definition describes the items included in a content pack. A content pack is a snapshot of the configuration data and other items that you have defined to help manage the resources in the IT environment you are monitoring with BSM. The Content Packs Manager displays a list of all known content pack definitions.

To access	➤ **Admin** > **Platform** > **Content Packs** ➤ **Admin** > **Operations Management** > **Manage Content** > **Content Packs**
Important information	BSM provides several ways to perform actions with buttons or menu items. The buttons in the **Content Pack Definitions** pane duplicate the options available in shortcut menus.
Relevant tasks	"How to Create and Manage Content Packs" on page 189
See also	"Content Packs Manager" on page 182

Definitions Pane

The **Content Pack Definitions** pane displays a list of all the content pack definitions that are available for your environment.

UI elements listed in the following table.

UI Elements	Description
🔄	**Refresh.** Refreshes the contents of the displayed list. Use if new content becomes available while you are working or you have uploaded new contents (for example, from the command-line interface).
✳	**New Item.** Opens the **Create New Content Pack Definition** wizard. For details about the wizard, see "Create New Content Pack Definition Wizard" on page 197.
✏	**Edit Item.** Opens the Edit Content Pack Definition dialog box, which enables to you edit the name, version, and description; content to be included; and dependencies for the selected content pack. This dialog box presents the same screens as the **Create New Content Pack Definition** wizard, but in tab format. For details, see "Create New Content Pack Definition Wizard" on page 197.
❌	**Delete Item.** Deletes the selected content pack definition (but not referenced content such as indicators and KPIs) from the list of definitions displayed.
XML	**Import Content Pack Definitions and Content.** Opens the Import Content Pack dialog box, which enables you to specify or browse to a file that contains the definition details for import. You can choose to overwrite existing items with the same ID, or only to import new items, leaving existing items as they are. You can also run the import in test mode, so that changes are not committed. Unresolved references in the imported definition (for example, to unknown CI types) are not allowed. For details, see "Import Content Pack Dialog" on page 206.

UI Elements	Description
XML	**Export Content Pack Definition and Content.** Opens the Select Location for Download dialog box, which enables you to specify or browse to a file location where you want to export the definition details
?	**Get Help.** Displays help about the active window, pane, or dialog box

Details Pane

The **Details** pane provides high-level information concerning the properties of the selected content pack definition and a short summary of the content pack definition's content and any problems found.

User interface elements are described below:

UI Elements	Description
General	Displays the name, display name, version, dependent content packs, and a description of the selected content pack definition

UI Elements	Description
Summary	Displays a summary of the selected content pack definition's contents, including: ➤ **Selected Content**. Displays a list of the content, grouped by content type, selected for inclusion in the selected Content Pack Definition. The total number of items included in the content pack per content type is indicated in brackets, for example: (10). Expanding the group displays the names of each item of that type included in the Content Pack Definition. ➤ **Referenced Content Included In This Content Pack**. Displays a list of the referenced content, grouped by content type, included in this content pack. The total number of referenced items in this content pack per content type is indicated in brackets, for example: (10). Expanding the group displays the names of each referenced item of that type. ➤ **Referenced Content from Other Content Packs**. Displays a list of the dependent content, grouped by content type, referenced from other content packs. The total number of dependent items from other content packs per content type is indicated in brackets, for example: (10). Expanding the group displays the names of each referenced item of that type, including the display name and version of each referenced content pack.
Problems Found	Displays information on any problems, such as unresolved dependencies (content that is included in the selected content pack definition but no longer exists in BSM), found in the selected content pack definition

Create New Content Pack Definition Wizard

This wizard enables you to create a new content pack definition, giving it a name, version, and description; selecting the content to be included; setting dependencies; and diagnosing problems.

To access	**Admin** > **Platform** > **Content Packs** or **Admin** > **Operations Management** > **Manage Content** > **Content Packs** Click ✳
Relevant tasks	"How to Create and Manage Content Packs" on page 189
Wizard map	This wizard contains: General Page > Content Page > Dependencies Page > Summary Page
See also	"Content Packs Manager" on page 182

General Page

This wizard page enables you to define the display name, name, version and description of a new content package.

Important information	➤ General information about this wizard is available here: "Create New Content Pack Definition Wizard" on page 197. ➤ This wizard page appears as the General tab in the Edit Content Pack Definition dialog box that opens when you click ✏ .
Wizard map	The Create New Content Pack Definition Wizard contains: **General Page** > Content Page > Dependencies Page > Summary Page
See also	"Content Packs Manager" on page 182

User interface elements are described below:

UI Elements	Description
ID	No action required. The content pack ID is assigned automatically when the content pack is first created. **Note:** ID field is only displayed in the General tab of the Edit Content Pack Definition dialog box, not on the General page of the **Create New Content Pack Definition** wizard.
Display Name	Name displayed in Content Pack Definitions list. This name does not have to be unique. It is limited to a maximum length of 255 characters.
Name	Name of the content pack definition. The name must be unique, and is limited to a maximum length of 80 characters. The first character must be a letter (A-Z, a-z) or an underscore (_). All other characters may be letters, numbers, or underscores. No leading or trailing spaces are allowed. When you export the content pack, this is the default file name for the XML file, with **OMi Content Pack -** as a prefix.
Version	Required, free text field. Use to control versions of your content packs.
Description	Brief description (limited to 1024 characters) of the content pack definition you want to add to (or have selected in) the **Content Pack Definitions** pane. Use the Description box to remind other users of the scope and content of the content pack.

Content Page

This wizard page enables you to select the content to be included in a new content pack definition.

Important information	➤ General information about this wizard is available here: "Create New Content Pack Definition Wizard" on page 197. ➤ This wizard page appears as the Content tab in the Edit Content Pack Definition dialog box that opens when you click ✏ .
Wizard map	The Create New Content Pack Definition Wizard contains: General Page > **Content Page** > Dependencies Page > Summary Page
See also	"Content Packs Manager" on page 182

User interface elements are described below:

UI Elements	**Description**
⟳	**Refresh:** Refreshes the contents of the displayed list. Use if new content becomes available while you are working or you have uploaded new contents (for example, from the command-line interface).
(⇨)	**Add to Included Content**: Adds the selected item(s) to the list of included content. If included content has already been included in another content pack, it is listed in the **Content in Other Content Packs** pane, and can safely be excluded from the content pack you are creating. It is not necessary to include content in multiple content packs. **Tip:** Selecting a CI type automatically selects all assigned content of the CI type and also all assigned content for child CI types. Selecting specific content, such as an individual indicator or KPI, automatically selects the reference to the CI type to which the content is related.

UI Elements	Description
⧉↘	**Expand Selection:** Expands the Available Content or Included Content list to display items belonging to the selected group.
⧉↖	**Collapse Others:** Collapses all open branches except for the selected branch.
?	**Get Help:** Displays help about the active window, pane, or dialog box
︾	**Expand**: Expands the **Filter** pane to display available filters
︽	**Collapse**: Collapses the **Filter** pane
⊞	Expands the selected folder
⊟	Collapses the selected folder
(⇦)	**Exclude**: Removes the selected item(s) from the list of included content
(⇚)	**Exclude All**: Removes all item from the list of included content
⧉↘	**Display All Selected Content Pack Items**: Expands the Included Content list to display all items selected for inclusion in the content pack.

UI Elements	Description
🔍	**Search Content**: Use the Search field to find the content in the **Available Content** or **Included Content** pane: Enter a search string in the Search box and click 🔍 . The first content to match the specified string is highlighted. If that content is not initially visible, the tree expands to display it. To find the next occurrence of content matching the specified string, click 🔍 again. The search string must be at least three characters long. Searching is started as soon as the third character is entered and the first match is highlighted. This prerequisite avoids searches being started too often and resources being blocked. Names with less than three characters cannot be found.
Available Content	Hierarchical list representing the available content in your IT environment. **Tip**: To include content in a content pack definition, drag it from the **Available Content** pane to the **Included Content** pane or select it and click the **Add to Included Content** button. BSM warns you if content already exists in other content packs when you perform an include operation. Color coding: ➤ Folder with no content: gray ➤ Selected content: bold ➤ Referenced content: italic ➤ Dependent content pack definition with version number: blue For details, see "Content Pack Content Types" on page 208.
Filter: Show only CI types with assigned content	Filters the CI Types tree to display only CI types that have content assigned to them.

UI Elements	Description
Included Content	List of content selected for inclusion in a content pack, along with any dependent content. **Tip**: To exclude an item, select an item (or group of items) and select the **Exclude** button. Color coding: ➤ Folder with no content: gray ➤ Selected content: bold ➤ Referenced content: italic ➤ Dependent content pack definition with version number: blue
Content in Other Content Packs	If content selected for inclusion is included in other content packs, it is listed here to indicate that it can be removed from this content pack. It is not necessary to include the same content in multiple content packs, and the recommended practice is not to do so.

Shortcut Menus

BSM provides many shortcut menus. The shortcut menus enable quick and direct access to information about selected elements and actions that you can perform on them.

You display a shortcut menu by right-clicking an element in the GUI. The information available and the actions that are possible from a shortcut menu depend on the element you right-click and the context in which it exists.

The shortcut menu in the Content tab includes the following elements:

UI Elements (A-Z)	Description
Add to Included Content	Adds the selected item(s) to the list of included content
Collapse Others	Collapses all open branches except for the selected branch

UI Elements (A-Z)	Description
Display All Selected Content Pack Items	Expands the Included Content list to display all items selected for inclusion in the content pack
Exclude	Removes the selected item(s) from the list of included content
Exclude All	Removes all item from the list of included content
Expand Selection	Expands the Available Content or Included Content list to display items belonging to the selected group

Dependencies Page

This wizard page enables you to set dependencies on dependent content that is included in more than one other content pack.

Important information	➤ General information about this wizard is available here: "Create New Content Pack Definition Wizard" on page 197. ➤ This wizard page appears as the Dependencies tab in the Edit Content Pack Definition dialog box that opens when you click ✏ .
Wizard map	The Create New Content Pack Definition Wizard contains: General Page > Content Page > **Dependencies Page** > Summary Page
See also	"Content Packs Manager" on page 182 "Dependencies in Content Packs" on page 185

User interface elements are described below:

UI Elements	**Description**
🔄	**Refresh.** Refreshes the contents of the displayed list of dependencies. Use if new content becomes available while you are working or you have uploaded new contents (for example, from the command-line interface).
↗	**Set Dependency.** If referenced content is also included in other content pack definitions, a message indicating this is displayed: "There is content referenced that is also included in other content pack definitions. To set the dependency to a specific content pack definition, select the content listed under this content pack definition and choose the "Set Dependency" action." To choose which content pack to reference, select the dependent content in that content pack and click **Set Dependency**. The dependent content in the referenced content pack is displayed in bold, indicating that dependency has been set on it.
(⇒)	**Add to Included Content.** Adds the selected dependent content to the list of content included in this content pack.

Summary Page

This wizard page enables you to see summary information regarding the content, dependencies, and any problems found in a new content pack definition.

Important information	➤ General information about this wizard is available here: "Create New Content Pack Definition Wizard" on page 197. ➤ This wizard page appears as the Summary tab in the Edit Content Pack Definition dialog box that opens when you click ✎ .
Wizard map	The Create New Content Pack Definition Wizard contains: General Page > Content Page > Dependencies Page > **Summary Page**
See also	"Content Packs Manager" on page 182

User interface elements are described in the table below.

In each section, the total number of objects in that category is indicated in brackets, for example: (10). Expanding the group displays the names of each object of that type in the group. Indicators also show CI type, that is, the type of configuration item to which the indicator is assigned (for example: **Application**, **Host**, or **Oracle System**).

UI Elements	Description
Selected Content	Displays a list of the selected content, grouped by content type, included in the selected content pack definition
Dependent Content Included in this Content Pack	Displays a list of the dependent content, grouped by content type, included in the selected content pack definition

UI Elements	Description
Dependent Content from other Content Packs	Displays a list of the dependent content referenced from other content packs, including the display name and version of each referenced content pack
Problems Found	Displays information on any problems, such as unresolved dependencies (content that is included in the selected content pack definition but no longer exists in BSM), found in the selected content pack definition

Import Content Pack Dialog

The Import Content Pack dialog box enables you to locate the content pack that you want to import and how you want the import to be performed.

Note: A content pack contains the items to import. A content pack definition lists the items included in the content pack.

To access	**Admin** > **Platform** > **Content Packs** or **Admin** > **Operations Management** > **Manage Content** > **Content Packs** Click XML
Relevant tasks	"Import content packs" on page 190

The Import Content Pack dialog box displays the UI elements listed in the following table.

UI Element	Description
Content Pack File	Enables you to browse to the location of the content pack file that you want to import. Content pack files are in XML format.
Overwrite	Allows BSM to overwrite any existing content pack definition or the items it references during the import process. Imports all objects contained within the content pack, including the content pack definition. Any objects existing in the target system with IDs that match objects in the specified content pack are overwritten. Any new objects are created. If any IDs do not match, the entire import is aborted.
Create	Imports all objects contained within the content pack, including the content pack definition, and ignores any objects in the content pack, including the content pack definition, that currently exist within the target system.
Test	Runs a simulated import operation using the selected content pack definition, but does not commit any changes to BSM.
Import	Starts the specified content data import and closes the Import Content Pack dialog box.

Content Pack Content Types

The following table gives an overview of the types of content that you can include in a content pack:

Content Type	Description
Automatic User Group Assignments	You can configure BSM to automatically assign incoming events to available user groups. Automatic assigning of events to user groups responsible for solving these events significantly improves the efficiency of event management.
CI Type tree	Configuration items (CIs) represent physical or logical entities in the system. For example, CIs can represent hardware, software, services, business processes, and so on. CI types are categories for each CI. Each CI type provides a template for creating the CI and its associated properties. The CI type tree organizes CI types into a hierarchical format based on the dependencies in your organization's IT environment. To include event type indicators (ETIs) or health indicators (HIs) in a content pack, drill down to the relevant indicators within the CI Type tree. The CI Type tree includes a number of Content Types that have a reference to a CI Type, such as: ➤ Indicators ➤ Mapping Rules ➤ Tool Definitions ➤ CI Type to Graph Families Mappings ➤ Configuration Item TQL View Mappings ➤ Graph Family to CI Type Assignments **Note:** When CI types and their children have no assigned content, their entries appear dimmed. When objects are directly assigned to a CI type, their entries appear in bold type.
Correlation Rules	Correlation rules associate selected CI types with defined indicator values to trigger a correlation process. The correlation process results in the highlighting of one or more configuration items as causes.

Content Type	Description
Event Filters for Mapping Rules	You can define mapping rules that search filtered events for strings and values which are then used to set an indicator value. The filter can use any of the available event attributes. For example, you can define a mapping rule that considers only those events that have a critical or major severity status and are assigned to a particular user or user group. A mapping rule filter is designed for use with its associate mapping rule.
Event Filters for User Group assignment	You can configure rules to automatically assign incoming events to available user groups. Automatic assigning of events to user groups responsible for solving these events significantly improves the efficiency of event management. Each event is assigned to an appropriate user group as soon as it is received. All operators in a user group are allowed to work on those events assigned to that user group.
Graph Families	Graphing is organized using a graph family tree, on which the graph family is the high-level group. (Sub-groups of graphs that are logically grouped within the family are referred to as categories.) A default graph in a graph family contains the most important metrics to measure the performance of any resource or application. You can map graph families or categories to a CI.
HI Assignments	Health indicators (HIs) provide fine-grained information on the CIs that represent your monitored business elements and processes. HI assignments define which HIs are assigned to new CIs in the system, based on each CI's CI type (CIT).
KPI Assignments	Key performance indicators (KPIs) are high-level indicators of CI performance and availability. KPI assignments define which KPIs are assigned to new CIs in the system, based on each CI's CI type (CIT).

Content Type	Description
Key Performance Indicators (KPIs)	KPIs are high-level indicators of CI performance and availability, which apply calculation rules to the data provided by HIs to determine CI status. KPIs help you to monitor how well your business is achieving its objectives, and to track critical performance variables over time.
Menus	Menu settings define shortcut menus for CIs, for example to launch configuration tools, start custom tools for specific CI types, and display graphs.
Propagations	By default, when a KPI is assigned to a CI, the KPI is automatically propagated to the CI's parents. Propagation rules enable you to define exceptions to the default KPI propagation, and to propagate other KPIs, the same KPI using a different rule, or no KPIs.
Rules	A business rule is the basic object that receives events (either samples or application messages), deals with processing the data, and holds the process results. Health indicator rules use sample data to calculate HIs; KPI rules use the results of HI calculations to calculate KPIs.
Script Definitions for Custom Actions	You can create script definitions to run custom actions on events. For example, you can add a text string to certain events to make them easier to identify in the Event Browser.
Script Definitions for Event Processing	Event processing enables you to execute any number of user defined scripts during event processing. For example, it is possible to add data to an event from a Microsoft Excel file or an SQL database. If Groovy scripts are specified in the Event Pipeline Script and Step Settings, the event is forwarded to the EPI Server.
Tool Categories	Tool categories are used to grant controlled access to tools. Each tool is assigned a category, and for users to be able to use the tools with a certain category, they must be granted execution permissions for the Tool Category.

Content Pack Manager Command-Line Interface

This section describes the options and parameters available in the ContentManager command-line interface.

The ContentManager command-line interface is located in:

<*BSM_Install_Dir*>\opr\bin

The ContentManager command accepts the following options:

```
ContentManager
        (-h | -version | (-l | -d <content_pack_name> |
        -i <in_file> [-f] [-t] |
        -snapshot [-o <out_file>] | [-e <content_pack_name> [-o <out_file>]])
        (([-ssl] [-server <gateway_server>] [-p <port>]) | [-u <URL>]))
        [-username <user_name>] [-password <password>] [v-]
```

The following table gives more information about the options recognized by the ContentManager command:

Option	Description
-d,-delete <content_pack_name>	Deletes the content pack definition specified in <content_pack_name>. It does not delete the content pack's content. Content includes definitions for event type indicators, health indicators, calculation rules for key performance indicators (KPI), topology-based correlation rules, tool definitions, view mappings, and graph families.
-e,-export <content_pack_name>	Exports the named content pack definition and its content to the file specified using the -output option.
-f, -force-overwrite	Imports all objects contained within the content pack, including the content pack definition. Any objects existing in the target system with IDs that match objects in the specified content pack are overwritten. Any new objects are created. If any IDs do not match, the entire import is aborted. If any of the content exists and force overwrite is not specified, the import fails with an error.

Option	Description
-h,-help	Displays a summary of the command options and exits.
-i,-import <input_file>	Imports the content pack definition and its content from the specified file.
-l,-list	Lists the content pack definitions.
-m,-multi <in_folder>	Imports all Content Pack Definitions and their content from a directory. The default behavior is to ignore any objects in the Content Packs, including the Content Pack Definitions, which currently exist within the target system. No dependency checks are made which can result in required content packs being missing.
-o,-output <out_file>	Specifies the name of the file to which you want the command to write during the export operation.
-password	Requests the password of the user specified in the -username option, whose account is being used for authentication purposes.
-p,-port	Sets the port number. The default port numbers are 80 for HTTP and 443 for HTTPS. Do not specify this option in conjunction with the -url option.
-server	Sets the target BSM server using either a hostname or an IP address. The specified server must be a BSM gateway server. Do not specify this option in conjunction with the -url option.
-skipcheck	Omits the content pack consistency check. The content pack consistency check verifies if dependent content that is not part of another content pack is either in the content pack itself or already imported.
-snapshot	Exports a snapshot of all content that can be managed by Content Packs Manager.
-ssl	Sets the protocol to HTTPS. The default protocol is HTTP. Do not specify this option in conjunction with the -url option. If you do not use the -port option to specify a non-standard port, the command uses the standard port number reserved for HTTPS: 443.

Option	Description
-t,-test	Runs import in preview mode and display the results immediately. No changes are committed to the database.
-u, -url <URL>	Specifies the URL of the BSM gateway server to access. The default value is: http://localhost:80/opr-admin-server Do not specify this option in conjunction with the -server option.
-username <user name>	The name of the user, whose account is being used for authentication purposes.
-v, -verbose	Prints verbose output.
-version	Prints the version information of the command and exits.

The **ContentManager** command displays the following values to indicate the exit status of the requested operation:

Exit Status	Description
0	Successful completion
1	Failure of requested operation
300-399	HTTP Redirection (300-399)
400-499	HTTP Client Error (400-499)
500-599	HTTP Internal Server Error (500-599)

The exit status numbers (300-599) reflect a standard HTTP-status category (and number), for example: Redirection (300-399). For more information about a specific HTTP error status, for example: 307, which signifies a temporary HTTP re-direct, see the publicly available HTTP documentation.

Troubleshooting and Limitations

This section provides troubleshooting help related to content management, including but not limited to: creating, modifying, and enabling configuration items.

Content Not Included in Content Pack

Make sure you perform the Include action at the correct level in the configuration item type hierarchy so that *all* elements assigned to the selected configuration item type (and any children) are included at the same time.

Unresolved References to CIs on Import

Content pack contains references to configuration items that do not exist on the target system. Make sure that the Override and Ignore options are correctly specified before starting the import.

12

Downtime Management

This chapter includes:

Concepts

Tasks

Reference

Concepts

Downtime Management - Overview

Downtime or other scheduled events can skew CI data. You may want to exclude these periods of time from being calculated for events, alerts, reports, views, or SLAs. Downtimes are configured based on associated CIs. For example, you might want to exclude a recurring maintenance event or a holiday for a specific host CI whose physical host you know will be down for that period of time.

You define and manage downtimes using the Downtime Management page in Platform Admin. HP Business Service Management enables you to:

- Configure the downtime to occur once or to recur weekly or monthly.
- Select multiple CIs to be affected by the downtime.

When configuring a downtime, you select specific instances of CIs from the available views. You can select CIs of the following CI types for the downtime:

- node
- running software
- business process
- business application
- ci collection
- infrastructure service
- business service

Downtime Actions

You can select what action is taken during the downtime on the CIs specified in the downtime configuration. Downtime can impact the following:

- **Alerts and Events**. Events are suppressed and no CI Status alerts, EUM alerts, or notifications are sent for any of the CIs associated with the downtime.
- **KPIs**. KPIs attached to the CI and impacted CIs are not updated and display the downtime for the CI in Service Health. For details on how downtime configurations affect Service Health, see "KPI Status Colors and Definitions" in *Using Service Health*.
- **Reports**. End User Management Reports are not updated and display the downtime for the CI. For details on how downtime configurations affect reports, see "Downtime Information in Reports" in *Reports*.
- **SLAs**. Selected SLAs that are attached to the CI are not updated. You can select which SLAs to include in the downtime. For details on how downtime configurations affect SLAs, see "Adjusting SLA Data - Overview" in *Using Service Level Management*.
- **Monitoring**. Business Process Monitor and SiteScope monitoring stops for any of the CIs associated with the downtime. For details on how downtime configurations affect SiteScope monitoring, see "CI Downtime" in *Using System Availability Management*.

The options you select in the downtime wizard are combinations of the above actions, grouped in this order. This means that each option includes the previous options listed. The actions that are taken in BSM during the downtime depends on the option selected during downtime configuration.

Events in Operations Management

When you select an action option that includes suppressing events in a downtime on a selected CI, the result in the Operations Management application depends on how the downtime behavior is configured in Operations Management. For details, see "Downtime Configuration" in *Using HP Operations Manager i*.

Tasks

How to Create and Manage Downtimes for CIs

This task describes how to create and manage downtimes for the CIs in your system.

This task includes the following steps:

- "Prerequisites" on page 218
- "Configure how events are handled in Operations Management - optional" on page 219
- "Run the Create Downtime wizard" on page 219
- "Results" on page 219

1 Prerequisites

Plan how you want the downtime to affect the CIs in your system. Before working in the wizard:

- When determining which CIs may need downtimes, take into consideration CIs whose status is impacted by other CIs. If a CI's status is impacted by a CI you selected for the downtime, that CI is also be affected by the downtime. You can select only CIs from the following CI types:
  - node
  - running_software
  - business_process
  - business_application
  - ci_collection
  - infrastructure_service
  - business_service

- Determine which actions should be applied to which CIs. The options for what happens during downtime are to:
  - Suppress events, alerts and notifications
  - Enforce downtime on KPI calculations; and suppress events, alerts and notifications
  - Enforce downtime on Reports and KPI calculations; and suppress events, alerts and notifications
  - Stop monitoring for Business Process Monitors and SiteScope; enforce downtime on Reports and KPI calculations; and suppress events, alerts and notifications

2 Configure how events are handled in Operations Management - optional

You can manage how events associated with CIs that are in downtime are handled. You do this in **Admin** > **Operations Management** > **Tune Operations Management** > **Downtime Behavior.**

For details on this topic, see "Downtime Configuration" in *Using HP Operations Manager i*.

3 Run the Create Downtime wizard

Go to **Admin** > **Platform** > **Downtime** and click the **Add Downtime** button.

For user interface details, see "New Downtime Wizard" on page 225.

4 Results

After running the wizard, the details of the downtime are displayed in the Downtime Manager page. You can export the details of the downtimes to a .pdf or Excel file.

For user interface details, see "Downtime Management Page" on page 221.

Tip: To limit the downtimes in the exported file to a specified selection, you can filter the visible downtimes in the Downtime Manager and then export to a .pdf or Excel file. You can filter by any combination of one or more columns, including: Name, CIs, Status, Action, Scheduling, Next Occurrence, Modified By, Approved By, Planned, and Category.

Reference

Downtime Management User Interface

This section includes:

- Downtime Management Page on page 221
- New Downtime Wizard on page 225

Downtime Management Page

Displays the list of scheduled downtimes configured for the associated CIs.

To access:	Select **Admin** > **Platform** > **Downtime Management**
Important information	➤ To add, edit or delete downtimes, you must have Full permission on the Downtime resource. In addition, you should have View permission on the Views to which CIs in the downtime belong. For details on permissions, see "Permissions Overview" on page 246. ➤ The values you see in this page are view only. To edit any of the values for a downtime, highlight the downtime and click **Edit**. The Downtime Wizard opens and you can edit the value in the page in which it appears. ➤ For downtimes that have already occurred, only the following fields are editable: ➤ Properties page - all fields ➤ Scheduling page - **End by** date in **Range of recurrence** ➤ Notification page - **Selected Recipients** ➤ Each column includes the option of filtering the list by the contents of the column. For example, you can select a category type in the category column and see only those downtimes configured with that category.

Relevant tasks	"How to Create and Manage Downtimes for CIs" on page 218
See also	"Downtime Management - Overview" on page 216

User interface elements are described below

UI Element (A–Z)	Description
✳	**Create new downtime.** Opens the New Downtime wizard where you configure a new downtime. For details, see "New Downtime Wizard" on page 225.
✏	**Edit downtime.** Opens the Edit Dowtime wizard, which enables to you edit the configuration of an existing downtime. This wizard presents the same screens as the New Downtime wizard. For details, see "New Downtime Wizard" on page 225.
⧉	**Duplicate downtime.** Clones the settings of an existing downtime to a new downtime.
✖	**Delete downtime(s).** Deletes selected downtime(s).
📊	**Export to Excel.** Exports the table of configured downtimes to a file in Excel format.
📄	**Export to PDF.** Exports the table of configured downtimes to a PDF file.
Action	The action that takes place when the downtime is in active status. You configure the action for the downtime in the New Downtime wizard. For details about the possible actions, see "Action Page" on page 230.
CIs	The CIs associated with the downtime. These are the CIs that are impacted when the downtime is in active status.
Modified by	The user who last created or modified the downtime configuration.
Name	The name of the downtime as configured in the Downtime wizard.

UI Element (A–Z)	Description
Next Occurrence	The date and time of the next occurrence of the downtime. This field is updated automatically.
Scheduling	Displays the: ➤ Date, time, and duration For recurring downtimes, also displays: ➤ What day of the week or month the downtime is scheduled to recur ➤ Duration
Status	Displays whether the downtime is currently: ➤ **Active.** The CIs are currently in downtime and the action selected for the downtime is now taking place. ➤ **Inactive.** The downtime is configured but it is currently not the time for the downtime to take place. ➤ **Completed**. The time for the downtime has passed and the actions configured for the downtime have occurred.
Optional Columns	
Approved by	Indicates if there was an approval for the downtime and who approved it.

UI Element (A–Z)	Description
Category	The category assigned to the downtime. Options include: ➤ Application installation ➤ Application maintenance ➤ Hardware installation ➤ Hardware maintenance ➤ Network maintenance ➤ Operating system reconfiguration ➤ Other ➤ Security issue You can also create up to two of your own customized categories using Infrastructure Settings. To add a custom downtime category, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**: ➤ Select **Foundations**. ➤ Select **Downtime**. ➤ In the **Downtime - General settings** table, edit the **Downtime category** value to the name you want to use as a customized category for the downtime. The name you enter appears as an option in the list of available downtime categories after you restart BSM.
Planned	Indicates whether the downtime is planned or not.

New Downtime Wizard

This wizard enables you to create and edit downtimes for the CIs in your model.

To access	**Admin** > **Platform** > **Downtime** > click the **Create new downtime** button, or select existing downtime and click the **Edit downtime** button.
Relevant tasks	"How to Create and Manage Downtimes for CIs" on page 218
Wizard map	This New Downtime Wizard contains: Properties Page > Select CIs Page > Scheduling Page > Action Page > Notification Page > Preview Page
See also	"Downtime Management - Overview" on page 216

Properties Page

This wizard page enables you to configure the general properties of the downtime.

Important information	For downtimes that have already occurred, all of the fields in the Properties page are editable.
Wizard map	This New Downtime Wizard contains: Properties Page > Select CIs Page > Scheduling Page > Action Page > Notification Page > Preview Page
See also	"Downtime Management - Overview" on page 216

User interface elements are described below:

UI Elements	Description
Downtime Name	Cannot exceed 200 characters.
Downtime Description	This description also appears in the "Downtime Information Area" in *Reports*.

UI Elements	Description
Approved by	You can enter the person or department who approved this downtime. Cannot exceed 50 characters.
Planned	Select if you want this downtime marked as planned. You can create downtimes that are unplanned. This is for information purposes only.
Downtime Category	Select a category from the drop-down menu. This category describes the reason for the downtime. You can also create up to two of your own customized categories using Infrastructure Settings. To add a custom downtime category, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**: ➤ Select **Foundations**. ➤ Select **Downtime**. ➤ In the **Downtime - General settings** table, edit the **Downtime category** value to the name you want to use as a customized category for the downtime. The name you enter appears as an option in the list of available downtime categories after you restart BSM.

Select CIs Page

This wizard page enables you to select the CIs that are affected by the downtime.

Important information	For downtimes that have already occurred, you cannot edit the selected CIs in this page.
Wizard map	This New Downtime Wizard contains: Properties Page > Select CIs Page > Scheduling Page > Action Page > Notification Page > Preview Page
See also	"Downtime Management - Overview" on page 216

User interface elements are described below:

UI Elements (A-Z)	Description
Available CIs	Select from the list the view that contains the CIs to be affected by this downtime. You can use the ☰ button to browse and perform a search among the available views. Highlight a CI from the view to move it to the Selected CIs list. Hold the Ctrl key for selecting multiple CIs. All views that the user has permission to see may be selected. You can select CIs only of the following CI types: ➤ node ➤ running software ➤ business process ➤ business application ➤ ci collection ➤ infrastructure service ➤ business service
Selected CIs	Once CIs are selected, they appear in the Selected CIs list. To remove a CI from a downtime, select the CI in the Selected CIs and click the back arrow to move it back to the Available CIs list.

Scheduling Page

This wizard page enables you to configure the schedule for the downtime.

Important information	➤ You cannot schedule a downtime in the past. ➤ For downtimes that have already occurred, only the following field is editable in the Scheduling page: **End by** date in **Range of recurrence** To cancel a recurring downtime that has already occured at least once, edit the downtime and modify this field.
Wizard map	This New Downtime Wizard contains: Properties Page > Select CIs Page > Scheduling Page > Action Page > Notification Page > Preview Page
See also	"Downtime Management - Overview" on page 216

User interface elements are described below:

UI Elements	Description
Time of occurrence	➤ **Start**. The dropdown list includes times set for every half hour on the hour and half hour. To select a different time of day, select the closest half hour and edit the field to enter the actual time you want the downtime to start. For example, for 2:10 am, select 2:00 am and edit the minutes to indicate 2:10 am. ➤ **End**. You can select an end time and the duration automatically updates. Or select the duration and the end time automatically updates. ➤ **Duration.** Includes options from 5 minutes to one week. The downtime duration must be in increments of 5 minutes and be defined in lengths of minutes, hours, days, or weeks. If the length of time you want to specify does not appear, for example 1 1/2 hours, then enter the end time and the duration automatically updates. To select a time greater than 1 week, select 1 week and edit the field to the correct number of weeks.
Recurrence pattern	Select one of the following: ➤ **Once.** The downtime happens only once as scheduled and does not recur. Select the calendar date for the occurrence. ➤ **Weekly.** Select the day of the week for the scheduled weekly recurrence. ➤ **Monthly.** Select a day in the month from the dropdown list for the scheduled monthly recurrence.
Range of recurrence	If you selected **Weekly** or **Monthly**: ➤ You must define a **Start** date. ➤ Select either an **End by** date or **No end date**.
Time Zone	All time zones are displayed in relation to GMT.

Action Page

This wizard page enables you to define the set of actions taken during the downtime.

Important information	For downtimes that have already occurred, no fields in the Action page are editable.
Wizard map	This New Downtime Wizard contains: Properties Page > Select CIs Page > Scheduling Page > Action Page > Notification Page > Preview Page
See also	"Downtime Management - Overview" on page 216

User interface elements are described below:

UI Elements	Description
Take no action	There is no action taken on the associated CIs or the CI monitoring, alerts, reports, or SLAs. **Note:** During this downtime, the affected CI doesn't change its status to **Downtime**. CI Status Alerts configured to be triggered if the CI changes its status.
Suppress events, alerts & notifications	➤ No events, alerts, or notifications are sent for any of the CIs associated with the downtime. ➤ Monitoring continues, and reports, status in Service Health, and SLAs are updated. **Note:** During the downtime period, the affected CI may change its status, and the status change may trigger the relevant CI Status alert.
Enforce downtime on KPI calculations; suppress events, alerts & notifications	➤ KPI calculations are not run and status in Service Health is not updated, and instead display the downtime for the CI. ➤ No events, alerts, or notifications are sent for any of the CIs associated with the downtime. ➤ Reporting and monitoring continue. SLAs are updated.

UI Elements	Description
Enforce downtime on Reports and KPI calculations; suppress events, alerts & notifications	➤ Report data is not updated and the downtime is displayed for the associated CIs. ➤ Selected SLAs are not updated for those SLAs affected by CIs associated with the downtime. ➤ KPI calculations are not run and status in Service Health is not updated, and instead display the downtime for the CI. ➤ No events, alerts, or notifications are sent for any of the CIs associated with the downtime. ➤ Monitoring continues.
Stop active monitoring; enforce downtime on Reports and KPI calculations; suppress events, alerts & notifications	➤ Business Process Monitor and SiteScope monitoring stops. ➤ Report data is not updated and the downtime is displayed for the associated CIs. ➤ Selected SLAs are not updated for those SLAs affected by CIs associated with the downtime. ➤ KPI calculations are not run and status in Service Health is not updated, and instead display the downtime for the CI. ➤ No events, alerts, or notifications are sent for any of the CIs associated with the downtime. **Note:** If you configure a downtime period for an Application CI (whose data is updated by BPM monitoring), Downtime Manager automatically sends an event to the BPM Agent when the downtime period starts. The agent stops sending samples to BSM. The samples that are suppressed are the BPM samples that correspond to the Transaction CIs, which are child CIs of the Application CIs on which the downtime is configured. There is one sample per transaction.

Notification Page

This wizard page enables you to select recipients to receive notification of the downtime. Notifications are sent by email at the time of downtime occurrence and immediately after it completes. You can select only those recipients with an email address defined.

Important information	For downtimes that have already occurred, you can edit the **Selected Recipients** in the Notification page.
Wizard map	This New Downtime Wizard contains: Properties Page > Select CIs Page > Scheduling Page > Action Page > Notification Page > Preview Page
See also	"Downtime Management - Overview" on page 216

User interface elements are described below:

UI Elements	Description
✳	Opens the **New recipient** dialog box to create a recipient that is not yet in the list of available recipients. The recipients you create are available as recipients in all of BSM. For details on creating recipients, see "How to Configure and Manage Recipients" on page 359.
Available Recipients	Lists the available recipients for downtime notification by means of either email, SMS, or pager.
Selected Recipients	Lists the selected recipients for downtime notification by means of either Email, SMS, or Pager. Either one, two or all three means of notification may be selected.

Preview Page

This wizard page enables you to preview a summary of your Downtime settings.

Wizard map	This New Downtime Wizard contains: Properties Page > Select CIs Page > Scheduling Page > Action Page > Notification Page > Preview Page
See also	"Downtime Management - Overview" on page 216

User interface elements are described below:

UI Elements	Description
Preview table	Table listing all the values configured for this downtime. Gives you the opportunity to click the **Back** button to return to a page that has a value that should be modified or deleted. Once you click **Finish** on this page, the downtime is added to the system and displayed in the Downtime Manager page.

Troubleshooting and Limitations

This section describes troubleshooting and limitations for the Downtime Manager.

This section contains the following topics:

➤ "Downtime and Daylight Saving Time" on page 234

Downtime and Daylight Saving Time

In time zones that observe Daylight Saving Time (DST), downtime calculations take into account the transitions between Standard and Daylight Time, using the following rules:

Note: The examples that follow use the daylight saving changes observed throughout most of the United States.

- March 14 2010 -- when 2:00 am arrives, the clock moves forward to 3:00 am. Thus, the period 2:00-2:59 am does not exist.
- November 7 2010 -- when 2:00 am arrives, the clock moves back to 1:00 am. Thus, the period 1:00-1:59 am appears twice.

In other time zones, the behavior is the same, but the transition dates and times may vary.

These examples are summarized in the table "DST Changes Affecting Downtime - Example Summary" on page 237.

Spring (Standard to Daylight Time)

- When downtime starts before the DST change and ends the day after the change, its end time is as expected, but the duration is 1 hour less than defined.

  Example 1:

  Monthly downtime starting 14th day of month at 1:30 am and ending on 15th day of month at 2:40 am. Duration is 1 day, 1 hour, and 10 minutes.

  No DST change: Downtime starts on 14th at 1:30 am and ends on 15th at 2:40 am. Duration is 1 day, 1 hour, 10 minutes.

  DST change on March 14 2010: Downtime starts on 14th at 1:30 am and ends on 15th on 2:40 am, but the duration is 1 day, 0 hours, 10 minutes (1 hour less than defined).

- When downtime starts before the DST change and ends the same day as the change, but after the change, its end time is 1 hour more than defined, but its duration is as defined.

  Example 2:

  Monthly downtime on 13th day of month, starting at 11 pm (23:00), for a duration of 5 hours.

  No DST change: Downtime starts on 13th at 11:00 pm and ends on 14th at 4:00 am.

  DST change on March 14 2010: Downtime starts on 13th at 11:00 pm and ends on 14th at 5:00 am, and the duration remains 5 hours.

- When downtime is defined to start during the skipped hour, the start time shifts 1 hour forward and keeps the defined duration.

  Example 3:

  Monthly downtime on 14th day of month, starting at 2:30 am, for a duration of 2 hours.

  No DST change: Downtime starts on 14th at 2:30 am and ends on 14th at 4:30 am.

  DST change on March 14 2010: Downtime starts on 14th at 3:30 am and ends on 14th at 5:30 am, and the duration remains 2 hours.

- When downtime is defined to start before the DST change and end during the skipped hour, the end time shifts 1 hour forward and keeps the defined duration.

  Example 4:

  Monthly downtime on 13th day of month, starting at 1:30 am, for a duration of 1 day, 1 hour, and 10 minutes.

  No DST change: Downtime starts on 13th at 1:30 am and ends on 14th at 2:40 am. The duration is 1 day, 1 hour, and 10 minutes.

  DST change on March 14 2010: Downtime starts on 13th at 1:30 am and ends on 14th at 3:40 am, and the duration remains as defined -- 1 day, 1 hour, and 10 minutes.

- When downtime is defined to start and end during the skipped hour, downtime takes place one hour later than defined.

Example 5:

Monthly downtime on 14th day of month, starting at 2:00 am, for a duration of 1 hour.

No DST change: Downtime starts on 14th at 2:00 am and ends on 14th at 3:00 am.

DST change on March 14 2010: Downtime starts on 14th at 3:00 am and ends on 14th at 4:00 am, and the duration remains as defined -- 1 hour.

Fall (Daylight Time to Standard Time)

- When downtime starts and ends after the DST change, its end time and duration are as defined.
- When downtime starts before the DST change (same day as change or day before) and ends after the change during the day of the change, the end time is 1 hour less than expected, and duration is as defined.

Example 6:

Two monthly downtimes, both starting on the 7th day of month at midnight. The first downtime duration is 1 hour, and the second is 2 hours.

No DST change: The first downtime is on 7th from 0:00 to 1:00 am (1 hour duration), and the second on 7th from 0:00 to 2:00 am (2 hours duration).

DST change on November 7 2010: The first downtime starts on 7th at 0:00 Daylight Time and ends on 7th at 1:00 am Daylight Time, with a duration of 1 hour. The second downtime starts on 7th at 0:00 Daylight Time and ends on 7th at 1:00 am Standard Time, and the duration remains 2 hours.

Example 7:

Monthly downtime on 7th day of month, starting at midnight, for a duration of 4 hours.

No DST change: Downtime starts on 7th at 0:00 and ends on 7th at 4:00 am.

DST change on November 7 2010: Downtime starts on 7th at 0:00 and ends on 7th at 3:00 am, and the duration remains as defined -- 4 hours.

Example 8:

Monthly downtime on 6th day of month, starting at 8:00 pm (20:00), for a duration of 7 hours.

No DST change: Downtime starts on 6th at 8:00 pm and ends on 7th at 3:00 am.

DST change on November 7 2010: Downtime starts on 6th at 8:00 pm and ends on 7th at 2:00 am, and the duration remains as defined -- 7 hours.

➤ When downtime starts before the DST change and ends the day after the change, the end time is as expected, and duration is 1 hour more than defined.

Example 9:

Monthly downtime on 7th day of month, starting at midnight (0:00), for a duration of 1 day, 1 hour (25 hours).

No DST change: Downtime starts on 7th at 0:00 and ends on 8th at 1:00 am.

DST change on November 7 2010: Downtime starts on 7th at 0:00 and ends on 8th at 1:00 am, but the duration is 26 hours.

DST Changes Affecting Downtime - Example Summary

Example	Downtime as Set/With DST Change	Start Time	End Time	Duration
1	Set	14th at 1:30 am	15th at 2:40 am	1 day, 1 hour, 10 minutes
	With DST Change	14th at 1:30 am	15th at 2:40 am	1 day, 0 hours, 10 minutes
2	Set	13th at 11:00 pm	14th at 4:00 am	5 hours
	With DST Change	13th at 11:00 pm	14th at 5:00 am	5 hours

Example	Downtime as Set/With DST Change		Start Time	End Time	Duration
3	**Set**		14th at 2:30 am	14th at 4:30 am	2 hours
	With DST Change		14th at 3:30 am	14th at 5:30 am	2 hours
4	**Set**		13th at 1:30 am	14th at 2:40 am	1 day, 1 hour, and 10 minutes
	With DST Change		13th at 1:30 am	14th at 3:40 am	1 day, 1 hour, and 10 minutes
5	**Set**		14th at 2:00 am	14th at 3:00 am	1 hour
	With DST Change		14th at 3:00 am	14th at 4:00 am	1 hour
6	**1st**	**Set**	7th at 0:00	7th at 1:00 am	1 hour
		With DST Change	7th at 0:00	7th at 1:00 am	1 hour
	2nd	**Set**	7th at 0:00	7th at 2:00 am	2 hours
		With DST Change	7th at 0:00	7th at 1:00 am Standard Time	2 hours
7	**Set**		7th at 0:00	7th at 4:00 am	4 hours
	With DST Change		7th at 0:00	7th at 3:00 am	4 hours
8	**Set**		6th at 8:00 pm	7th at 3:00 am	7 hours
	With DST Change		6th at 8:00 pm	7th at 2:00 am	7 hours

Example	Downtime as Set/With DST Change	Start Time	End Time	Duration
9	**Set**	7th at 0:00	8th at 1:00 am	25 hours
	With DST Change	7th at 0:00	8th at 1:00 am	26 hours

Editing Downtimes

- If while editing a downtime in the Downtime wizard its status changes from **Idle** to **Active**, the downtime cannot be saved.
- If you want to cancel a recurring downtime that has already occured at least once, edit the downtime's **End by** date in the Scheduling page.

Part IV

Users, Permissions, and Recipients

13

User Management

This chapter includes:

Concepts

Tasks

Reference

Concepts

User Management – Overview

You use the User Management interface to:

- **Configure HP Business Service Management Groups and Users.** Permissions enable you to restrict the scope of a user's access to predefined areas. Permissions can be granted either directly to a user or by means of a user group. 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.

  You may want to create different groups based on how users access the different resources in HP Business Service Management. Examples of criteria for grouping users that are relevant to your organization may be:

Functions 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

  You can change a user's parameters, including username and password, on the General tab. For details, see "General Tab (User Management)" on page 338.

  For details on creating groups and users, see "Groups/Users Pane" on page 351.

- **Define a superuser.** One superuser is defined for every installation of HP Business Service Management. This superuser's default login name and password are admin, admin. This original superuser is not listed among the users in User Management and therefore, this user's password can be changed only on the **General Settings** page in Personal Settings (**Admin** > **Personal Settings**). For details on the user interface for performing this task, see "User Account Page" on page 388.

  Superuser can be applied to other users in the system. These users with superuser permissions are listed, and can be modified, in User Management. For details on applying permissions, see "How to Assign Permissions" on page 269.

- **Assign recipient to user.** You can assign a recipient to a user. A recipient can receive alerts and scheduled reports. For details on recipients, see "Recipient Management Overview" on page 358.
- **Assign Permissions to Groups and Users.** The User Management interface is available only to users with appropriate permissions. A user's permissions are either inherited from assigned roles, or granted individually when its parameters are configured. For details on permissions, see "Permissions Overview" on page 246.
- **Set Group and User Hierarchy.** You can add users to groups and nest groups within other groups. For details, see "Group and User Hierarchy" on page 253.
- **Customize User Settings.** Select the page users see when entering BSM, and choose the menu items available on pages throughout BSM. For details, see "Customizing User Menus" on page 255.

Permissions Overview

You can assign permissions to the groups and users defined in your HP Business Service Management platform, enabling access to specific areas of HP Business Service Management.

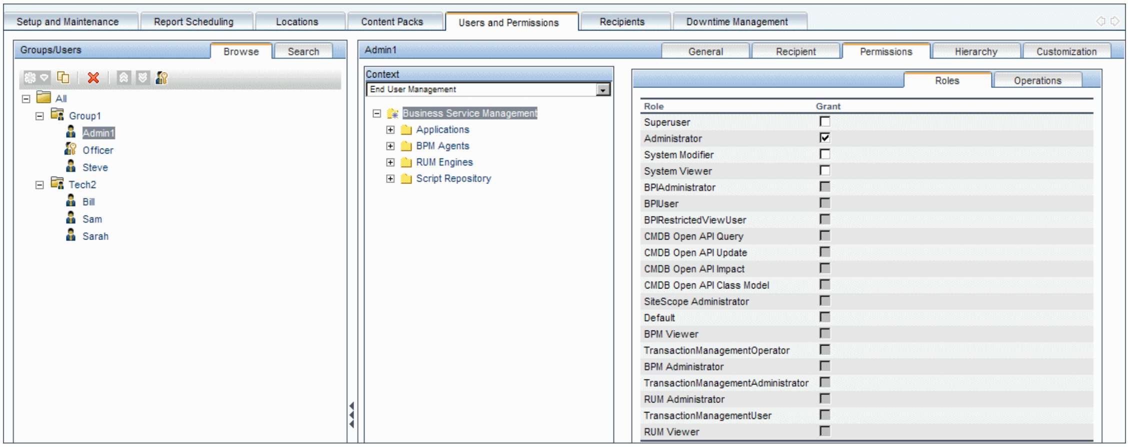
Granting permissions has the following components:

- user
- resource
- role or operation being granted

The Permissions tab includes the following areas:

- The resource tree area in the center of the page, containing the contexts, resources and resource instances on which permissions are assigned. For details, see "Understanding Permissions Resources" on page 247.
- The roles and operations area on the right side of the page. For details on roles, see "Roles" on page 251. For details on operations, see "Operations" on page 251.

Additionally, the **Groups/Users** pane is continually visible on the left side of the page.



All
Group1
Admin1
Officer
Steve
Tech2
Bill
Sam
Sarah

Context: End User Management

Business Service Management
Applications
BPM Agents
RUM Engines
Script Repository

Role	Grant
Superuser	☐
Administrator	☑
System Modifier	☐
System Viewer	☐
BPIAdministrator	☐
BPIUser	☐
BPIRestrictedViewUser	☐
CMDB Open API Query	☐
CMDB Open API Update	☐
CMDB Open API Impact	☐
CMDB Open API Class Model	☐
SiteScope Administrator	☐
Default	☐
BPM Viewer	☐
TransactionManagementOperator	☐
BPM Administrator	☐
TransactionManagementAdministrator	☐
RUM Administrator	☐
TransactionManagementUser	☐
RUM Viewer	☐

For details on assigning permissions, see "How to Assign Permissions" on page 269.

Note:

- If you have upgraded from a previous version of HP Business Service Management 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 251.
- You can export users and groups, together with their assigned roles, from one HP Business Service Management machine to another. For details, contact HP Software Support.

Understanding Permissions Resources

HP Business Service Management enables you to fine-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 Service Management 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.

This section also includes:

- "Resources and Resource Instances" on page 248
- "Guidelines for Working with Resources" on page 250

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. After 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 types:

- Resources that are functions or options within the system that do not have any other instances or types.

  Example:

  The Outlier Value resource determines whether the user can edit the outlier threshold value. It has no instances.

- Resources that do have instances - permissions can be applied only on the resource type and affect all instances of the resource.

Example:

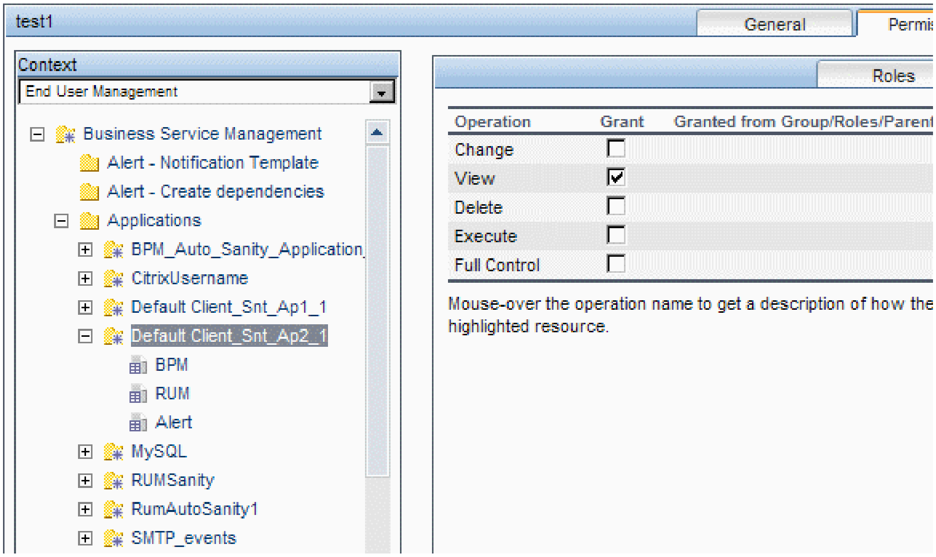
The Category resource includes all categories defined in End User Management Administration. **Change** permissions granted on the categories resource enables a user to modify all the categories defined in the system. You cannot grant or remove permissions for specific categories, only for every category 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 Applications resource collection within the End User Management context. The Applications resource includes instances only if applications have been defined in the system. Some instances may be defined by default, but others only exist if defined by the user. If there are applications defined in the system, each of these appears as an instance of the Applications resource.

Because BPM, RUM, and alerts are defined in your platform per application, the BPM, RUM, and Alerts resources appear under each of the instances of the application resource.

You can apply permissions to the Applications resource level. This provides the user with access to all applications created in the system. If you want to restrict a user's access to specific applications that relate to the user's tasks, you can apply permissions to those specific applications, and can also apply or removed permissions to specific resources per application.



Context: End User Management

Operation	Grant	Granted from Group/Roles/Parent
Change	□	
View	☑	
Delete	□	
Execute	□	
Full Control	□	

Mouse-over the operation name to get a description of how the highlighted resource.

Guidelines for Working with Resources

- The Business Service Management resource refers to all contexts in HP Business Service Management.
- Only roles and not operations can be applied to the Business Service Management resource. For details, see "Roles" on page 251.
- To manage the permissions on a subresource, you must provide the user with at least **View** permission on the selected resource's parent.
- You grant **Add** permission only on a resource and not on an instance of a resource.
- When a user defines or creates an instance of a resource, for example creates a Business Process profile, that user has **Full Control** permission on that resource instance and all of its child resources.

Roles

HP Business Service Management enables you to apply permissions using 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.

Roles are organized by context, which define what resources and operations have been preconfigured and included in the roles. For details on how each operation applies to a specific resource, see "Operations" on page 251.

Roles can be applied only to specific resources:

- Roles that include resources from several contexts can be applied only to the **Business Service Management** resource. **Business Service Management** 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 Roles Applied Across BSM" on page 282.

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 Service Management, see "User Management Operations" on page 309.

Security Officer

The security officer is a user who has security privileges to view sensitive information in the system. The security officer is typically not a regular BSM user and receives access to configure certain sensitive reporting information. In Real User Monitor, the security officer can configure settings for masking sensitive data. For details, see "Sensitive Data Area" in *Real User Monitor*. This user does not generally access the other areas of BSM.

There can be only one user in the system assigned as security officer. Only the user with superuser permissions can assign the security officer for the first time. Thereafter, only the user assigned as security officer can pass on the security office designation to another user, or change his or her own password. The superuser can no longer assign security officer status.

The security officer is designated by highlighting a user in the User Management tree and clicking on the Security Officer icon. For details on the user interface, see "Groups/Users Pane" on page 351.

No other user in the system can delete the user assigned as security officer. The security officer designation must be assigned to a different user by the security officer before the user who is the current security officer can be deleted from the system.

In unforeseen circumstances, when the security officer is no longer able to access the system and reassign the security officer designation to another user, the administrator can use the JMX console to clear the security officer designation from the user. For details on how to perform this task procedure, see "How to Remove Security Officer Status Using the JMX Console" on page 273.

Group and User Hierarchy

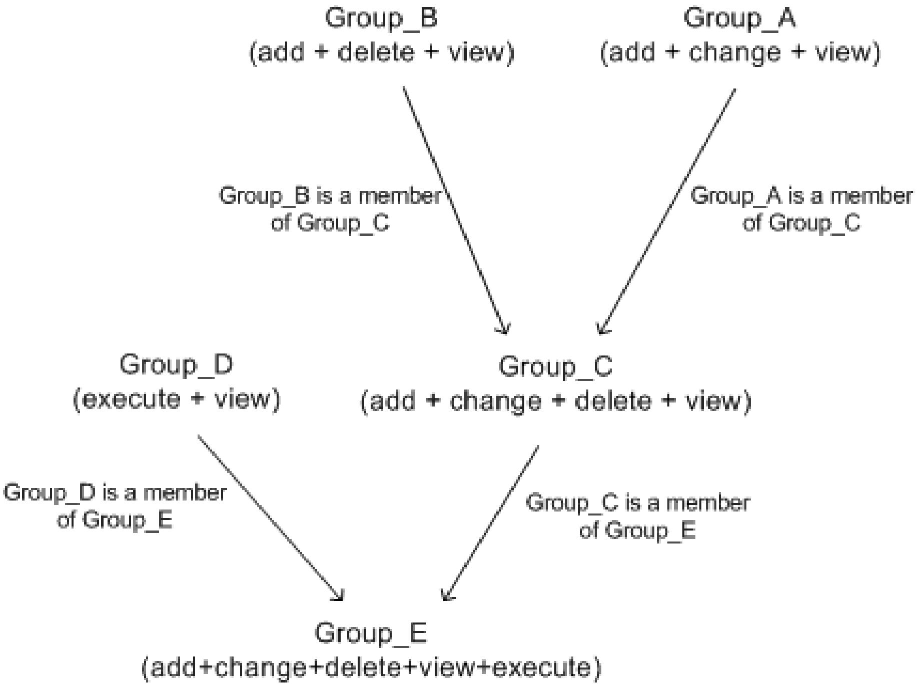
You can nest groups to make managing user and group permissions easier. Instead of assigning access permissions to each group one at a time, you can nest a group to inherit the permissions of its direct parent.

When nesting groups, 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.

Example:

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.


Group_B
(add + delete + view)
Group_A
(add + change + view)
Group_B is a member of Group_C
Group_A is a member of Group_C
Group_D
(execute + view)
Group_C
(add + change + delete + view)
Group_D is a member of Group_E
Group_C is a member of Group_E
Group_E
(add+change+delete+view+execute)

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 previous example refer to the same resource.

For details on setting up nested groups, see "How to Configure Group and User Hierarchy" on page 271.

Customizing User Menus

You can customize user menus to:

- Select the default context that is displayed for specific users when logging into HP Business Service Management.
- Specify the first page that is displayed for specific users in each of the different parts of HP Business Service Management.
- Select whole contexts and applications to hide per user.
- Specify the tabs and options that are available on pages throughout HP Business Service Management.

Customizing the entry page, menu items, and tabs enables the interface to display only the areas of HP Business Service Management that are relevant to specific users.

For details on customizing user menus, see "How to Customize User Menus" on page 274.

You customize user menus on the Customization tab. For details on the Customization tab user interface, see "Customization Tab (User Management)" on page 336.

Tasks

How to Configure Users and Permissions - Workflow

This task describes a suggested working order for the User Management application. You can configure User Management settings in any other logical order you choose.

Tip: For a use-case scenario related to this task, see "How to Configure Users and Permissions - Use-Case Scenario" on page 259.

This task includes the following steps:

- ➤ "Prerequisites" on page 257
- ➤ "Create Groups" on page 257
- ➤ "Assign Permissions to Groups" on page 258
- ➤ "Create Users" on page 258
- ➤ "Configure User and Group Hierarchy" on page 258
- ➤ "Customize User Settings" on page 258
- ➤ "Configure and Manage Recipients" on page 258

1 Prerequisites

Before you configure the User Management portal, you should map out the required users and groups and their relevant permission levels before defining them in HP Business Service Management. For example, enter the following information in a spreadsheet:

- A list of users required to administer the system, as well as the end users who are to access Service Health 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 *Using Service Health*.
- If multiple users require similar system permissions, a list of roles and the users that should belong to each group.
- The permissions that each user or group requires. 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 247.

2 Create Groups

You create groups in the **Groups/Users** pane as follows:

a Click the **New Group/User** button in the Browse tab, after selecting an existing group or the root group.

b Select **Create Group** and enter the group's information in the Create Group dialog box. For user interface details, see "Create Group Dialog Box" on page 334.

3 Assign Permissions to Groups

HP Business Service Management enables you to apply permissions to groups and users for specific resources and instances of those resources that are defined in the system. For task details, see "How to Assign Permissions" on page 269.

4 Create Users

You create users and then place them into the appropriate groups. For user interface details, see "Groups/Users Pane" on page 351.

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 task details, see "How to Configure Group and User Hierarchy" on page 271.

6 Customize User Settings

In the Customization tab, you customize the menu items that are displayed in different contexts for users. For task details, see "How to Customize User Menus" on page 274.

7 Configure and Manage Recipients

You create recipients by defining one or more notification methods, the template to use for alert notices, and a notification schedule to receive reports. You create recipients and manage existing recipients in the Recipients page. For user interface details, see "How to Configure and Manage Recipients" on page 359.

How to Configure Users and Permissions - Use-Case Scenario

This use-case scenario describes how to configure users and groups in the User Management portal.

Note: For a task related to this scenario, see "How to Configure Users and Permissions - Workflow" on page 256.

This scenario includes the following steps:

- "Mapping Out Users and Groups" on page 259
- "Creating Groups" on page 260
- "Assigning Permissions to Groups" on page 261
- "Creating Users" on page 262
- "Configuring User and Group Hierarchy" on page 262
- "Customizing User Settings" on page 267

1 Mapping Out Users and Groups

Jane Smith is the System Administrator at NewSoft Company, and wants to configure users and groups to be authorized to use HP Business Service Management, as well as end users who will be accessing Service Health 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.

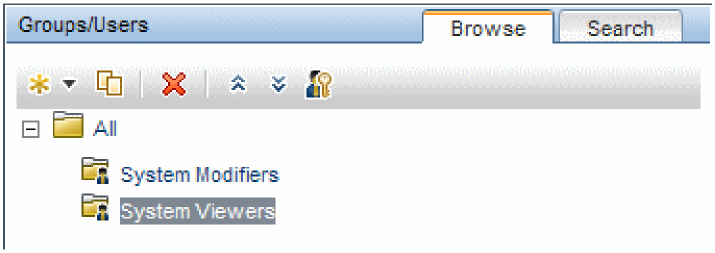
With this information, she then decides to create one group with the permission level of System Modifiers, and another with the permission level of System Viewers. Further, one of the users is assigned additional roles of SiteScope Administrator.

2 Creating Groups

Jane groups 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

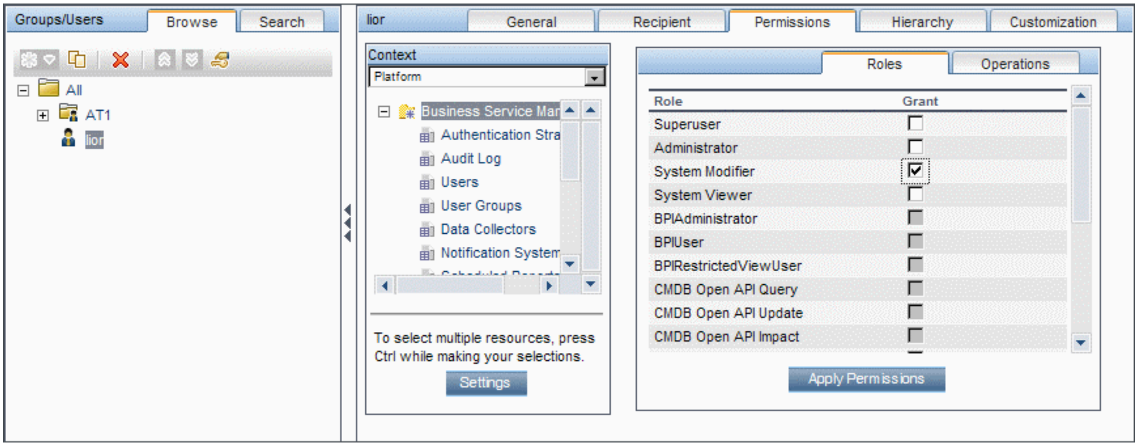
The **Groups/Users** pane appears as follows:



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, and chooses the Root instance (**Business Service Management**) from any context. In the **Roles** tab, she selects **System Modifier** and then clicks **Apply Permissions**. She then selects **System Viewers** in the **Groups/Users** pane and chooses **System Viewer** in the **Roles** tab, clicking **Apply Permissions**.

The results are displayed on the Permissions tab as follows:

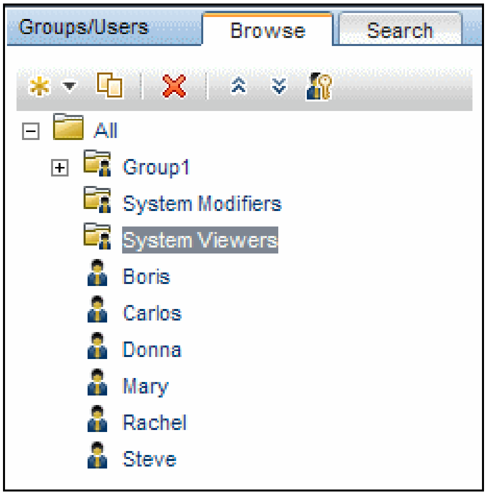


Role	Grant
Superuser	□
Administrator	□
System Modifier	☑
System Viewer	□
BPIAdministrator	□
BPIUser	□
BPIRestrictedViewUser	□
CMDB Open API Query	□
CMDB Open API Update	□
CMDB Open API Impact	□

To select multiple resources, press Ctrl while making your selections.

4 Creating Users

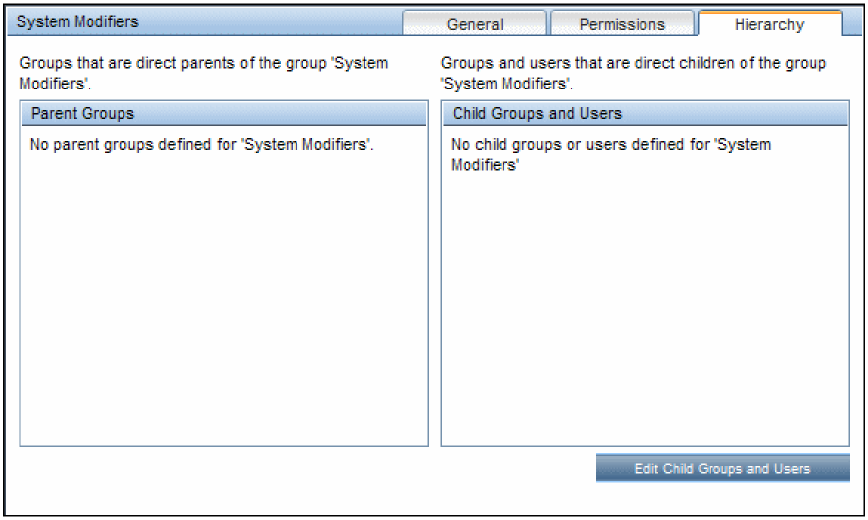
Jane must now create users to nest within the groups, in accordance with the desired permission levels of the individual users. She clicks the **New Group/User** button in the **Groups/Users** pane and while on the Root group, (**All**), she selects **Create User** and configures settings for each new 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 Service Management, 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:



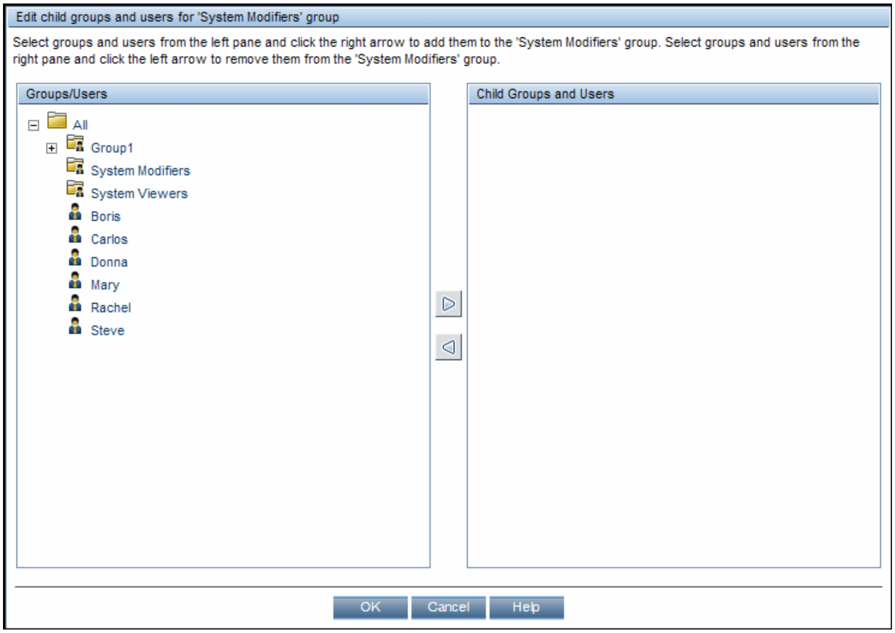
Groups that are direct parents of the group 'System Modifiers'.

No parent groups defined for 'System Modifiers'.

Groups and users that are direct children of the group 'System Modifiers'.

No child groups or users defined for 'System Modifiers'

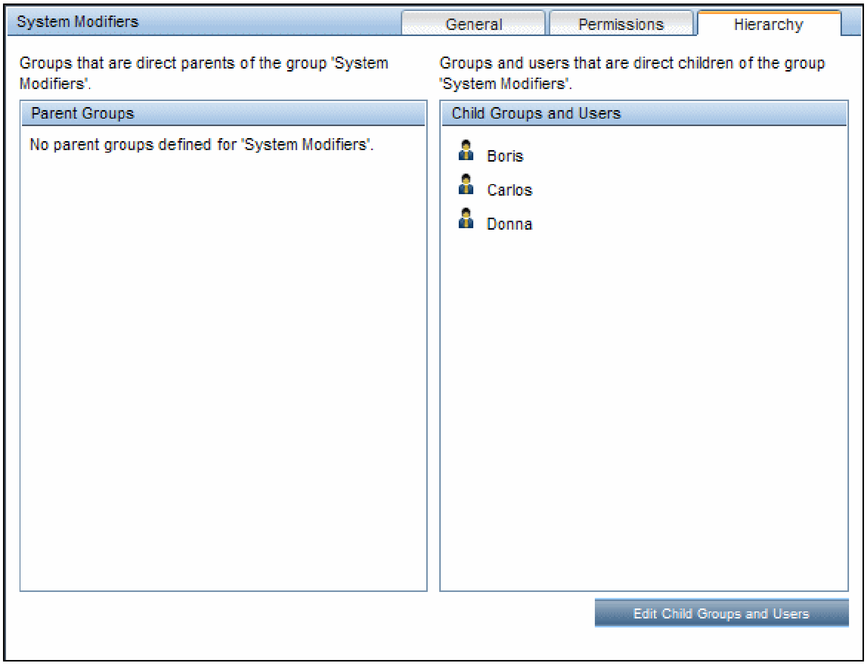
Jane clicks the **Edit Child Groups and Users** button to open the Edit Child Groups and Users dialog box:



Edit child groups and users for 'System Modifiers' group

Select groups and users from the left pane and click the right arrow to add them to the 'System Modifiers' group. Select groups and users from the right pane and click the left arrow to remove them from the 'System Modifiers' group.

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:



Groups that are direct parents of the group 'System Modifiers'.

Parent Groups

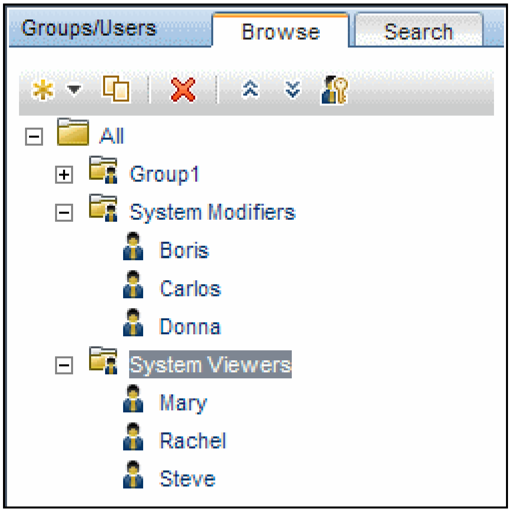
No parent groups defined for 'System Modifiers'.

Groups and users that are direct children of the group 'System Modifiers'.

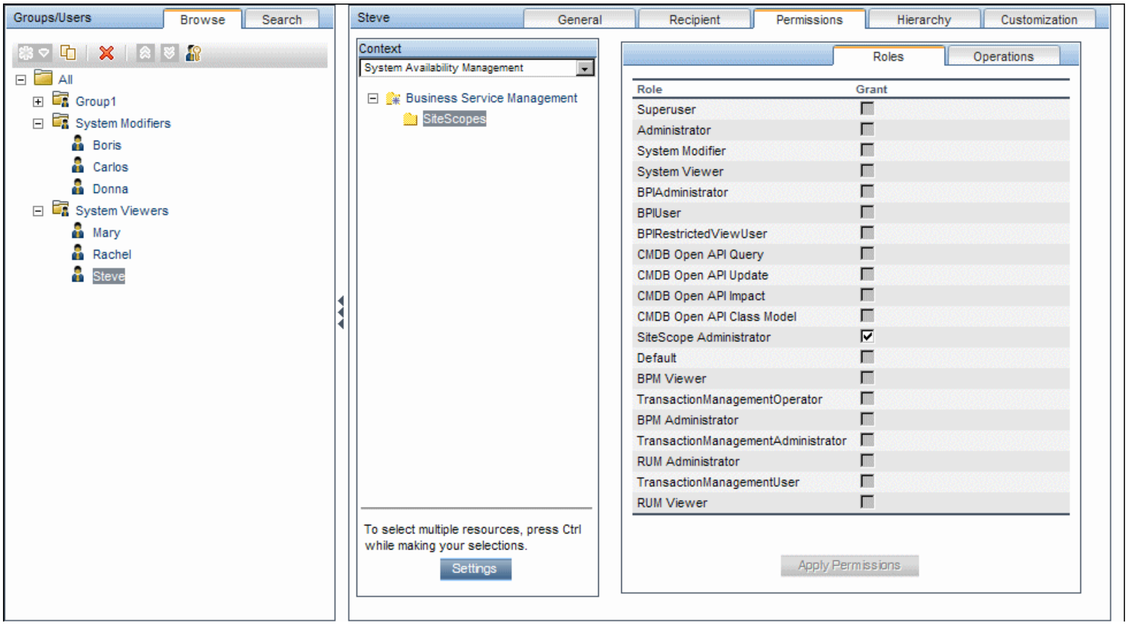
Child Groups and Users

- Boris
- Carlos
- Donna

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 **Roles** tab, and clicks **Apply Permissions**. The resulting screen appears as follows:



Context: System Availability Management

To select multiple resources, press Ctrl while making your selections.

Role	Grant
Superuser	□
Administrator	□
System Modifier	□
System Viewer	□
BPIAdministrator	□
BPIUser	□
BPIRestrictedViewUser	□
CMDB Open API Query	□
CMDB Open API Update	□
CMDB Open API Impact	□
CMDB Open API Class Model	□
SiteScope Administrator	☑
Default	□
BPM Viewer	□
TransactionManagementOperator	□
BPM Administrator	□
TransactionManagementAdministrator	□
RUM Administrator	□
TransactionManagementUser	□
RUM Viewer	□

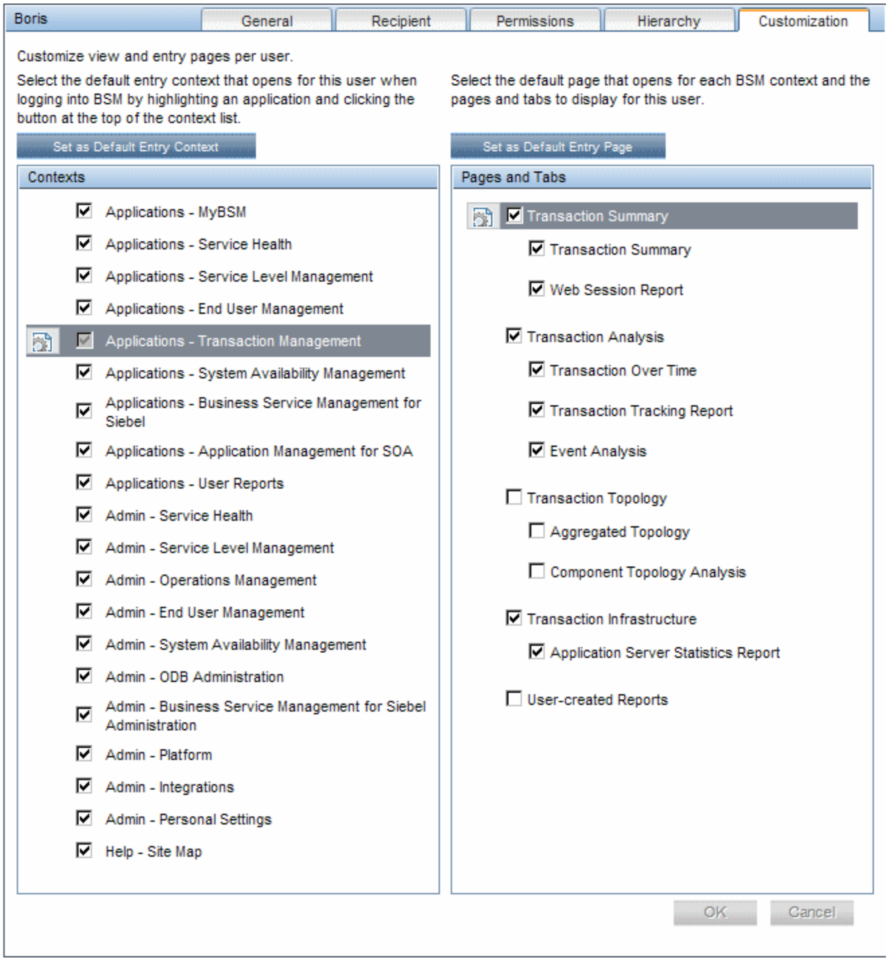
6 Customizing User Settings

Jane now sets the page each user sees when entering BSM, and the menu items available to them on pages throughout BSM. 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 Service Management. 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 Service Management page by selecting or clearing the relevant check boxes. For example, the **Transaction Topology** and **User-created reports** pages are cleared to ensure that they are not visible on the **Applications - Transaction Management** context when the user logs in.

The configured settings are displayed on the customization tab as follows:



Boris

Customize view and entry pages per user.

Select the default entry context that opens for this user when logging into BSM by highlighting an application and clicking the button at the top of the context list.

Contexts

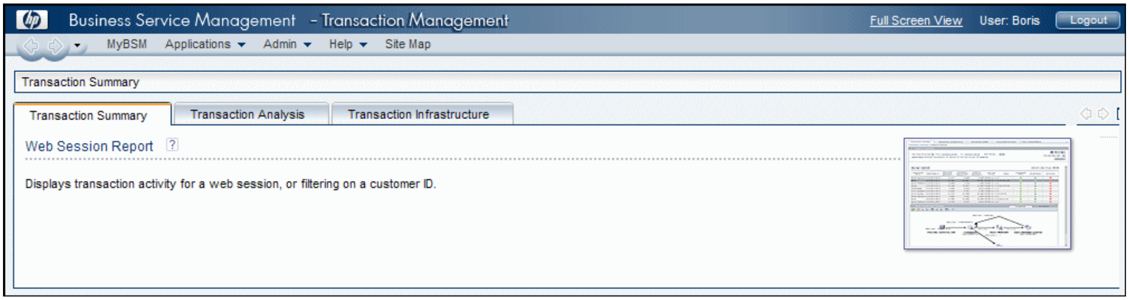
- ☑ Applications - MyBSM
- ☑ Applications - Service Health
- ☑ Applications - Service Level Management
- ☑ Applications - End User Management
- ☑ Applications - Transaction Management
- ☑ Applications - System Availability Management
- ☑ Applications - Business Service Management for Siebel
- ☑ Applications - Application Management for SOA
- ☑ Applications - User Reports
- ☑ Admin - Service Health
- ☑ Admin - Service Level Management
- ☑ Admin - Operations Management
- ☑ Admin - End User Management
- ☑ Admin - System Availability Management
- ☑ Admin - ODB Administration
- ☑ Admin - Business Service Management for Siebel Administration
- ☑ Admin - Platform
- ☑ Admin - Integrations
- ☑ Admin - Personal Settings
- ☑ Help - Site Map

Select the default page that opens for each BSM context and the pages and tabs to display for this user.

Pages and Tabs

- ☑ Transaction Summary
  - ☑ Transaction Summary
  - ☑ Web Session Report
- ☑ Transaction Analysis
  - ☑ Transaction Over Time
  - ☑ Transaction Tracking Report
  - ☑ Event Analysis
- □ Transaction Topology
  - □ Aggregated Topology
  - □ Component Topology Analysis
- ☑ Transaction Infrastructure
  - ☑ Application Server Statistics Report
- □ User-created Reports

The login page that the user sees according to the customized configurations is as follows:



Web Session Report

Displays transaction activity for a web session, or filtering on a customer ID.

How to Assign Permissions

This task describes how to configure group and user permissions in User Management. For the applied permissions to take effect, the user for whom permissions have been granted or removed must log out and log in again to HP Business Service Management.

This task includes the following steps:

- "Prerequisites" on page 270
- "Select a Group or User" on page 270
- "Select a Context" on page 270
- "Assign a Group" on page 270
- "Assign Operations - Optional" on page 270
- "Configure Permissions Settings - Optional" on page 270

1 Prerequisites

Ensure that groups and users are configured in your system. For user interface details, see "Groups/Users Pane" on page 351.

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 "Resource Contexts" on page 346.

4 Assign a Role

Permissions are assigned using roles. 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 Applied Across BSM" on page 282.

5 Assign Operations - Optional

Optionally, you can assign individual operations in the **Operations** tab that the group or user can perform in HP Business Service Management. For details on the available operations, see "User Management Operations" on page 309.

6 Configure Permissions Settings - Optional

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 user interface details, see "Resource Tree Pane" on page 345.

How to 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 (User Management)" on page 341.

This task includes the following steps:

- "Prerequisites" on page 271
- "View Group and User Hierarchy" on page 271
- "Nest Groups and Users" on page 271
- "Results" on page 272

1 Prerequisites

Ensure that you have configured at least one group and one user in the **Groups/Users** pane. For user interface details, see "Groups/Users Pane" on page 351.

2 View Group and User Hierarchy

Select a group or user in the **Groups/Users** pane, and select the **Hierarchy** tab on the right side of the page to view the parent and child groups of the group or user, if applicable.

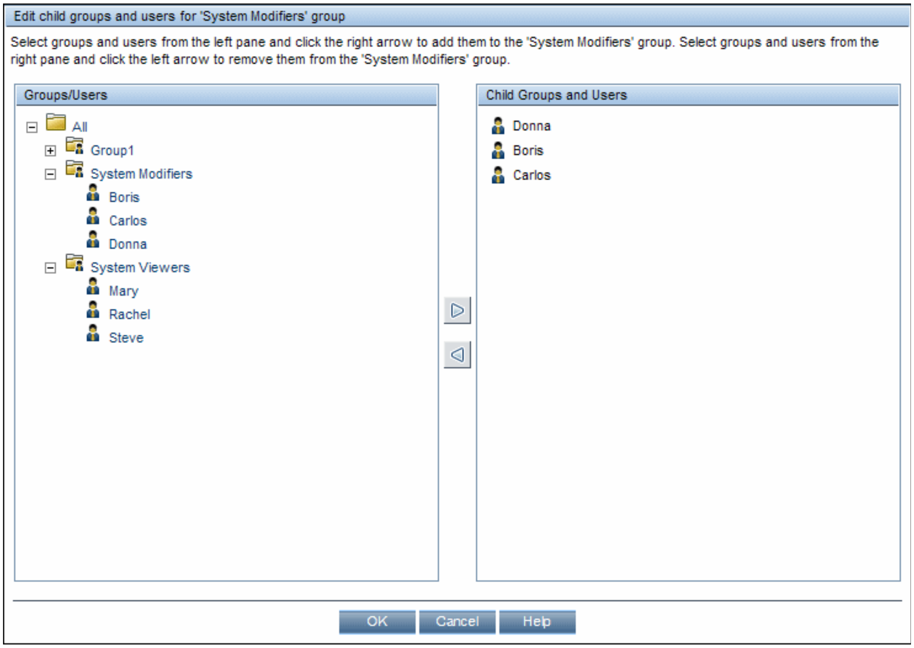
3 Nest Groups and Users

You choose a group in the **Groups/Users** pane, and choose groups and users to nest beneath it.

a Click a group or user in the **Browse** tab of the **Groups/Users** pane on the left side of the screen.

b Click the **Hierarchy** tab on the right side of the screen.

c 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.



Edit child groups and users for 'System Modifiers' group

Select groups and users from the left pane and click the right arrow to add them to the 'System Modifiers' group. Select groups and users from the right pane and click the left arrow to remove them from the 'System Modifiers' group.

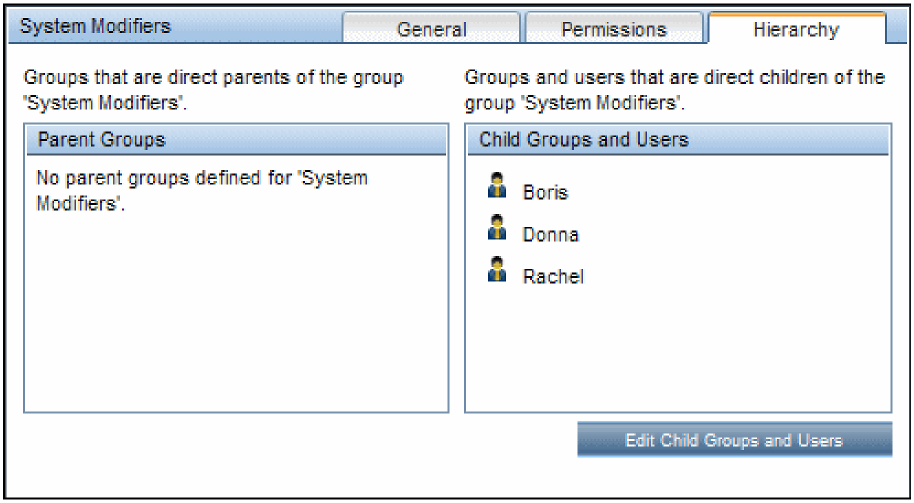
d Assign users and nest groups by selecting the user or group in the **Groups/Users** pane, and clicking on the left-to-right arrow to move the group or user to the **Child Groups and Users** pane.

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.

4 Results

The nested groups and users appear in the Child Groups and Users pane in the Hierarchy tab.

Example:



Groups that are direct parents of the group 'System Modifiers'.

No parent groups defined for 'System Modifiers'.

Groups and users that are direct children of the group 'System Modifiers'.

- Boris
- Donna
- Rachel

How to Remove Security Officer Status Using the JMX Console

This task describes how to remove security officer status from a user using the JMX console. This may be necessary if under unforeseen circumstances, the security officer cannot remove the status himself. Once the security officer is assigned, there is no other user authorized to make this change within the User Management interface. For details on this topic, see "Security Officer" on page 252.

To remove a security officer:

1. Enter the URL of the JMX console (**http://<Gateway or Data Processing 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:
   - Domain name: **Foundations**
   - Service: **Infrastructure Settings Manager**

- Setting: **setCustomerSettingDefaultValue**

4 Modify the parameter values as follows:

- **Context Name**: enter security
- **Setting Name**: enter secured.user.login.name
- **New Value**: leave empty

5 Click **Invoke**.

How to Customize User Menus

This task describes how to customize the page users see when entering HP Business Service Management, and choose the menu items available on pages throughout HP Business Service Management.

Tip: For a use-case scenario related to this task, see "How to Customize User Menus - Use-Case Scenario" on page 276.

This task includes the following steps:

- "Prerequisites" on page 274
- "Select a User" on page 275
- "Assign a Default Context" on page 275
- "Select Contexts and Applications to Hide/Display" on page 275
- "Select Context Pages and Tabs" on page 275
- "Assign a Default Entry Page" on page 275
- "Results" on page 275

1 Prerequisites

Ensure that you have configured at least one user in the **Groups/Users** pane. For user interface details, see "Groups/Users Pane" on page 351.

2 Select a User

Select 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 Service Management, and click **Set as Default Entry Context**. For user interface details, see "Customization Tab (User Management)" on page 336.

4 Select Contexts and Applications to Hide/Display

In the **Context** pane, clear the check boxes of the contexts and applications that you want hidden from the user. By default, all contexts and applications are selected.

5 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.

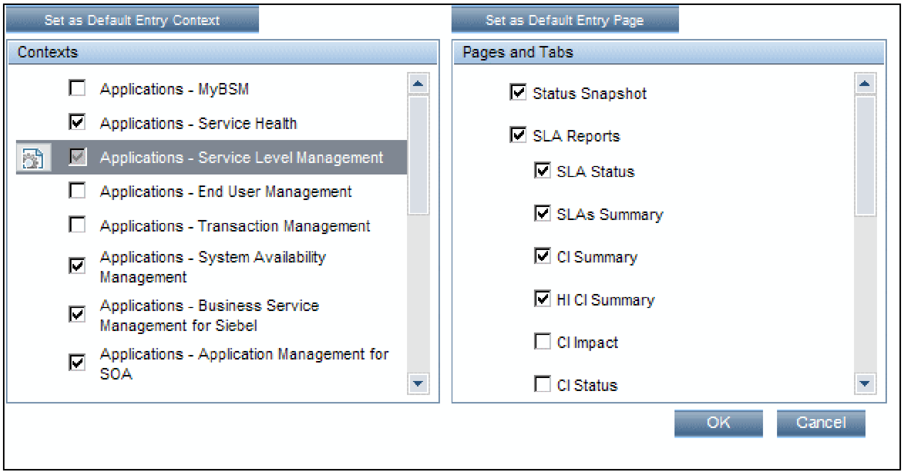
6 Assign a Default Entry Page

Select a page or tab to be the default entry page for the selected context, and click **Set as Default Entry Page**.

7 Results

The **Default Entry** icon appears next to the default entry context and page. Applications and context visible to the user are selected in the **Contexts** pane. Pages and tabs visible to the user are selected in the **Pages and Tabs** pane.

Example:



Contexts

- □ Applications - MyBSM
- ☑ Applications - Service Health
- ☑ Applications - Service Level Management
- □ Applications - End User Management
- □ Applications - Transaction Management
- ☑ Applications - System Availability Management
- ☑ Applications - Business Service Management for Siebel
- ☑ Applications - Application Management for SOA

Pages and Tabs

- ☑ Status Snapshot
- ☑ SLA Reports
  - ☑ SLA Status
  - ☑ SLAs Summary
  - ☑ CI Summary
  - ☑ HI CI Summary
  - □ CI Impact
  - □ CI Status

How to Customize User Menus - Use-Case Scenario

This use-case scenario describes how to customize user menus for individual users.

Note: For a task related to this scenario, see "How to Customize User Menus" on page 274.

This scenario includes the following steps:

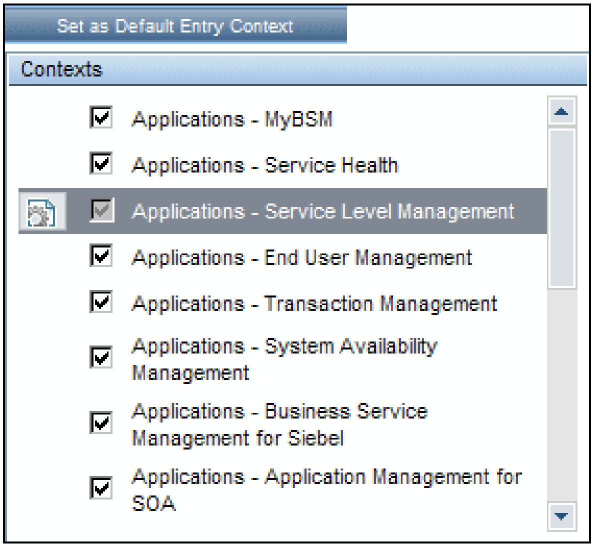
- "Choosing a User" on page 277
- "Assigning a Default Context" on page 277
- "Selecting Context Pages and Tabs" on page 278
- "Results" on page 278

1 Choosing a User

Mary, the administrator of ABC Insurance Company, is creating several users in the User Management section of HP Business Service Management. She decides that the user John Smith should be able to view only certain pages and tabs in HP Business Service Management, and that a specific page should appear on his screen when he logs into HP Business Service Management.

2 Assigning a Default Context

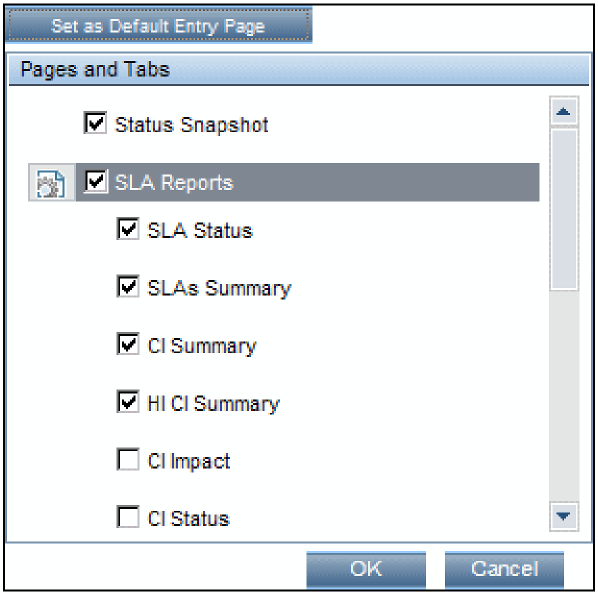
Since John's chief responsibility at ABC relates to service level management, Mary designates the Applications - Service Level Management page as the default entry context. Mary selects **Applications - Service Level Management** in the Contexts pane, and clicks **Set as Default Entry Context**. The **Applications - Service Level Management** context is indicated as the default entry context with the default entry icon, as appears in the following image:



Set as Default Entry Context
Contexts
☑ Applications - MyBSM
☑ Applications - Service Health
☑ Applications - Service Level Management
☑ Applications - End User Management
☑ Applications - Transaction Management
☑ Applications - System Availability Management
☑ Applications - Business Service Management for Siebel
☑ Applications - Application Management for SOA

3 Selecting Context Pages and Tabs

Since John is not authorized to view Outage Reports, that option is cleared in the Pages and Tabs pane, leaving the remaining pages and tabs checked to be visible when John logs into HP Business Service Management. As SLA Reports are of the highest priority for ABC Insurance, Mary designates this as the first page for John to see upon logging in. She selects **SLA Reports** in the Pages and Tabs pane, and then clicks **Set as Default Entry Page**. **SLA Reports** is indicated as the default entry page with the default entry icon, as appears in the following image:



☑ Status Snapshot

☑ SLA Reports

☑ SLA Status

☑ SLAs Summary

☑ CI Summary

☑ HI CI Summary

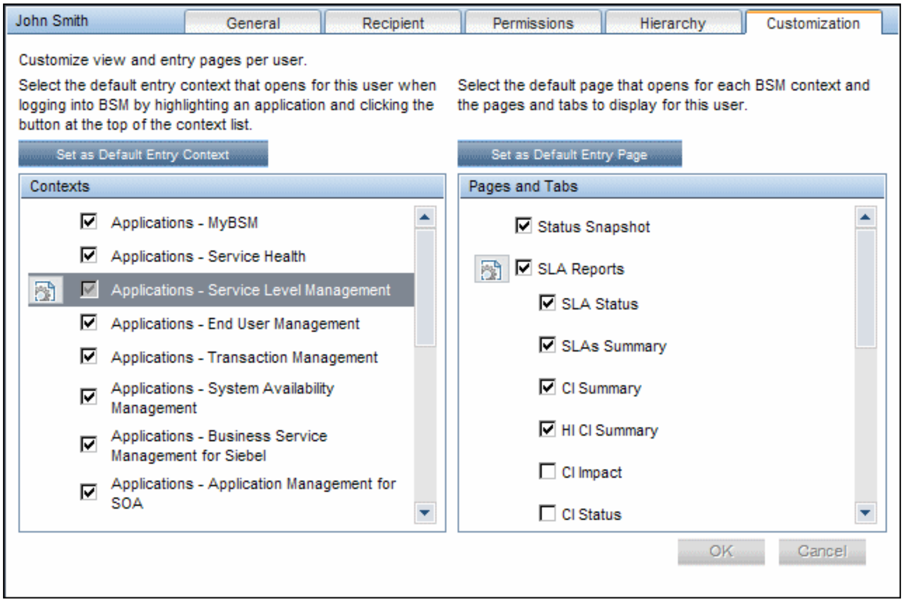
□ CI Impact

□ CI Status

4 Results

The context that opens when John Smith logs into HP Business Service Management is the **Service Level Management** context on the Applications menu. The **SLA Reports** page opens, and the Status Snapshot, Alerts, and SLA Management pages are also available to him.

The configured Customization tab in User Management appears as follows:



Customize view and entry pages per user.

Select the default entry context that opens for this user when logging into BSM by highlighting an application and clicking the button at the top of the context list.

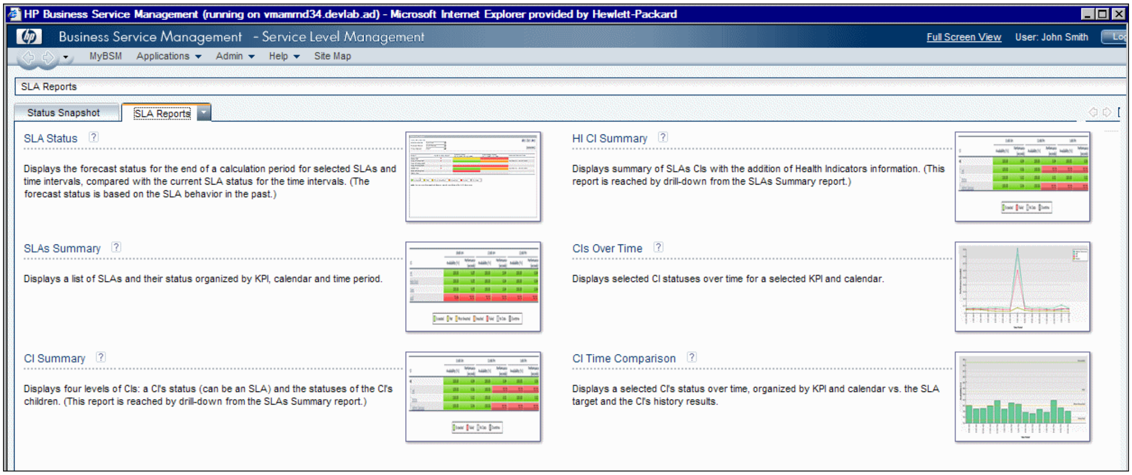
Select the default page that opens for each BSM context and the pages and tabs to display for this user.

Contexts

- ☑ Applications - MyBSM
- ☑ Applications - Service Health
- ☑ Applications - Service Level Management
- ☑ Applications - End User Management
- ☑ Applications - Transaction Management
- ☑ Applications - System Availability Management
- ☑ Applications - Business Service Management for Siebel
- ☑ Applications - Application Management for SOA

Pages and Tabs

- ☑ Status Snapshot
- ☑ SLA Reports
  - ☑ SLA Status
  - ☑ SLAs Summary
  - ☑ CI Summary
  - ☑ HI CI Summary
  - ☐ CI Impact
  - ☐ CI Status


HP Business Service Management (running on vmamnd34.devlab.ad) - Microsoft Internet Explorer provided by Hewlett-Packard
Business Service Management - Service Level Management
Full Screen View
User: John Smith
MyBSM
Applications
Admin
Help
Site Map
SLA Reports
Status Snapshot
SLA Reports

SLA Status

Displays the forecast status for the end of a calculation period for selected SLAs and time intervals, compared with the current SLA status for the time intervals. (The forecast status is based on the SLA behavior in the past.)

HI CI Summary

Displays summary of SLAs CIs with the addition of Health Indicators information. (This report is reached by drill-down from the SLAs Summary report.)

SLAs Summary

Displays a list of SLAs and their status organized by KPI, calendar and time period.

CIs Over Time

Displays selected CI statuses over time for a selected KPI and calendar.

CI Summary

Displays four levels of CIs: a CI's status (can be an SLA) and the statuses of the CI's children. (This report is reached by drill-down from the SLAs Summary report.)

CI Time Comparison

Displays a selected CI's status over time, organized by KPI and calendar vs. the SLA target and the CI's history results.

How to Add a Custom Pager or SMS Service Provider

If your pager or SMS service provider does not appear on the default provider list, and the provider uses an email gateway, you can manually add your provider to HP Business Service Management. After doing so, your provider appears on the list.

To add a provider that uses an email gateway, manually add the gateway information to the management database. If necessary, ask your database administrator for assistance.

To add a provider that uses an email gateway:

1 Open the **NOTIFICATION_PROVIDERS** table in the management database.

2 In the **NP_NOTIFICATION_PROVIDER_NAME** column, add the name of the provider to the bottom of the list.

Add the name exactly as you want it to appear in the provider list that opens in the SMS tab of the Recipient Properties wizard. For details, see "SMS Tab" on page 374.

Note the ID number that is automatically assigned to the provider.

3 Close the **NOTIFICATION_PROVIDERS** table, and open the **NOTIFPROVIDER_NOTIFTYPE** table.

4 In the **NN_NOTIF_PROVIDER_ID** column, add the ID number that was assigned to the new provider in step 2 on page 280.

5 In the **NN_NOTIF_TYPE_ID** column, assign the provider one of the following notification types:

➤ **102** – for pager service provider

➤ **101** – for SMS service provider

6 Close the **NOTIFPROVIDER_NOTIFTYPE** table, and open the **NOTIFICATION_PROVIDER_PROP** table.

7 In the **NPP_NOTIFICATION_PROVIDER_ID** column, add the ID number that was assigned to the new provider in step 2 on page 280.

Note that you add the ID number to two consecutive rows.

8. In the **NPP_NPROVIDER_PROP_NAME** and **NPP_NPROVIDER_PROP_VALUE** columns, add the following new property names and values for the provider, one beneath the other (for examples, see existing entries):

Property Name	Property Value	Description
EMAIL_SUFFIX	<email_suffix>	The gateway's email suffix. For example, if the gateway email address is 12345@xyz.com, enter xyz.com as the property value for EMAIL_SUFFIX.
EMAIL_MAX_LEN	<max_length>	The maximum message length, in characters, of the body of the email message. For example, 500. When determining this value, take into consideration the maximum length limit imposed by your service provider, as well as limitations to your pager or mobile phone.

9. In the **NPP_NPROVIDER_PROP_DATATYPE_ID** column, specify an ID value as follows:

   - for EMAIL_SUFFIX, specify: 1
   - for EMAIL_MAX_LEN, specify: 2

10. Restart HP Business Service Management.

Reference

User Management Roles Applied Across BSM

The following roles can be applied across all contexts within BSM. 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 noted accordingly.

For details about roles that can be applied only to specific contexts, see "User Management Roles Applied to Specific Contexts" on page 303.

This section describes the following roles:

- "Superuser" on page 282
- "Administrator" on page 283
- "System Modifier" on page 292
- "System Viewer" on page 297
- "BPM Viewer" on page 300
- "BPM Administrator" on page 300
- "RUM Administrator" on page 302
- "RUM Viewer" on page 302

Superuser

The **Superuser** role can be applied only to the **Business Service Management** 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.

Caution: The default superuser does not have permissions to write to Business Service Management from the UCMDB WS API. Specific roles exist for that purpose. For details, see "CMDB Open API Query" on page 304 and "CMDB Open API Update" on page 305.

Administrator

The **Administrator** role can be applied only to the **Business Service Management** 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.

Business Process Insight

Resource	Allowed Operations
Business Process Insight Application	View
Business Process Insight Administration	Full Control

Diagnostics

Resource	Allowed Operations
Opal	Change
	View
	Execute
	Full Control

End User Management

Resource	Allowed Operations
Alert - Create dependencies	Change
Applications	Add
	View
BPM Agents	View
RUM Engines	View
Script Repository	Add
	Change
	View
	Delete
	Full Control

ODB

Resource	Allowed Operations
Views	Add
	Change
	View
	Delete
	Full Control
ODB	Full Control
CI Search	Full Control
Data Modifier	Full Control
Get Related	Full Control
ITU Manager	Full Control
Modeling Studio	Full Control

Operations Management

Resource	Allowed Operations
Events assigned to user	Work On/Resolve
	Close
	Reopen
	Assign To
	Launch Operator Action
	Launch Automatic Action
	Transfer Control
	Close Transferred
	Add/Remove Event Relations
	Change Severity
	Change Priority
	Change Title
	Change Description
	Change Solution
	Add/Delete/Update Annotations
	Add/Delete/Update Custom Attributes

Resource	Allowed Operations
Events not assigned to user	View
	Work On/Resolve
	Close
	Reopen
	Assign To
	Launch Operator Action
	Launch Automatic Action
	Transfer Control
	Close Transferred
	Add/Remove Event Relations
	Change Severity
	Change Priority
	Change Title
	Change Description
	Change Solution
	Add/Delete/Update Annotations
	Add/Delete/Update Custom Attributes
Health Indicators	Reset
Administrative UIs	View
Tool Categories	Execute

Operations Orchestration Integration

Resource	**Allowed Operations**
Administration	Add
	Change
	View
	Delete
	Full Control
Execution	Execute
	Full Control

Platform

Resource	**Allowed Operations**
Audit Log	View
	Full Control
Users	Add
	Change
	View
	Delete
	Full Control
User Groups	Add
	Change
	View
	Delete
	Full Control
Data Collectors	Change
	View

Resource	**Allowed Operations**
Scheduled Reports	Add
	Change
	View
	Delete
	Full Control
Recipients	Add
	Change
	View
	Delete
	Full Control
Custom Data Types	Add
	Change
	View
	Delete
	Full Control
Downtime	View
	Full Control
Databases	Add
	Change
	View
	Delete
	Full Control

Service Health

Resource	Allowed Operations
User Pages	Full Control
Predefined Pages	View
User Components	Full Control

Service Level Management

Resource	Allowed Operations
SLAs	Add
	Change
	View
	Delete
	Full Control

System Availability Management

Resource	Allowed Operations
SiteScopes	Add

Transaction Management

Resource	Allowed Operations
TransactionVision Processing Servers	Change
	Full Control
TransactionVision Analyzers	Change
	Execute
	Full Control

Resource	Allowed Operations
TransactionVision Job Managers	Change
	Execute
	Full Control
TransactionVision Query Engines	Change
	Execute
	Full Control
Administration	Change
	Full Control
User Data	View
	Full Control
Applications	Add

User Defined Reports

Resource	Allowed Operations
Custom Reports	Add
	Change
	View
	Full Control
Trend Reports	Add
	Change
	View
	Full Control
Custom Links	Change
	View
	Full Control
Excel Reports	Change
	View
	Full Control
Default Footer/Header	Change
	Full Control
Favorite Filter	Change
	Delete
	Full Control
Annotation	Change
	Delete
	Full Control

Resource	**Allowed Operations**
Service Report	Change
	Delete
	Full Control

System Modifier

The **System Modifier** role can be applied only to the **Business Service Management** resource.

A system modifier can view and change any and all of the resources within HP Business Service Management. 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 Service Management.

Business Process Insight

Resource	**Allowed Operations**
Business Process Insight Application	View
Business Process Insight Administration	Full Control

Diagnostics

Resource	**Allowed Operations**
Opal	Change
	View
	Execute

End User Management

Resource	Allowed Operations
Alert - Notification Template	Change
	View
Alert - Create dependencies	Change
Applications	Change
	View
BPM Agents	View
RUM Engines	View
Script Repository	View
	Full Control

ODB

Resource	Allowed Operations
Views	Change
	View
CI Search	Full Control
Get Related	Full Control
ITU Manager	Full Control
Modeling Studio	Full Control

Operations Orchestration Integration

Resource	Allowed Operations
Administration	Change
	View
Execution	Execute

Platform

Resource	Allowed Operations
Audit Log	View
Users	Change
	View
User Groups	Change
	View
Data Collectors	Change
	View
Scheduled Reports	Change
	View
Recipients	Change
	View
Custom Data Types	Change
	View
Send SNMP trap	Change
Run executable file	Change
Log to Event Viewer	Change
Downtime	Full Control
Databases	Change
	View
System Recipient Template	Change
	View

Service Health

Resource	Allowed Operations
User Pages	Full Control
Predefined Pages	View
User Components	Full Control

Service Level Management

Resource	Allowed Operations
SLAs	Change
	View

System Availability Management

Resource	Allowed Operations
SiteScopes	Change
	View

Transaction Management

Resource	Allowed Operations
TransactionVision Processing Servers	Change
TransactionVision Analyzers	Change
	Execute
TransactionVision Job Managers	Change
	Execute
TransactionVision Query Engines	Change
	Execute
Administration	Change

Resource	Allowed Operations
Applications	Change
	View

User Defined Reports

Resource	Allowed Operations
Custom Reports	Add
	Change
	View
Trend Reports	Add
	Change
	View
Custom Links	Change
	View
Excel Reports	Change
	View
Default Footer/Header	Change
Favorite Filter	Change
	Delete
Annotation	Change
	Delete
Service Report	Change
	Delete

System Viewer

The System Viewer role can be applied only to the **Business Service Management** resource.

A system viewer can only view resources within HP Business Service Management 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.

Business Process Insight

Resource	Allowed Operations
Business Process Insight Application	View

Diagnostics

Resource	Allowed Operations
Opal	View

End User Management

Resource	Allowed Operations
Alert - Notification Template	View
Applications	View
BPM Agents	View
RUM Engines	View
Script Repository	View

ODB

Resource	Allowed Operations
Views	View
CI Search	Full Control

Resource	Allowed Operations
Get Related	Full Control
ITU Manager	Full Control
Modeling Studio	Full Control

Operations Orchestration Integration

Resource	Allowed Operations
Administration	View

Platform

Resource	Allowed Operations
Audit Log	View
Users	View
User Groups	View
Data Collectors	View
Scheduled Reports	View
Recipients	View
Custom Data Types	View
Downtime	View
Databases	View
System Recipient Template	View

Service Health

Resource	Allowed Operations
Predefined Pages	View

Service Level Management

Resource	Allowed Operations
SLAs	View

System Availability Management

Resource	Allowed Operations
SiteScopes	View

Transaction Management

Resource	Allowed Operations
Applications	View

User Defined Reports

Resource	Allowed Operations
Custom Reports	Add
	View
Trend Reports	Add
	View
Custom Links	View
Excel Reports	View

BPM Viewer

The **BPM Viewer** role can be applied only to the **Business Service Management** 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 BPM Profile in the previous version is upgraded to the BPM Viewer role for that profile.

End User Management

Resource	Allowed Operations
Applications	View
BPM Agents	View
Script Repository	View

BPM Administrator

The **BPM Administrator** role can be applied only to the **Business Service Management** resource.

The BPM Administrator can manage all of the platform's BPM profiles, including permissions on all the profiles.

Any administrator who was added as a user on a specific BPM profile in the previous version is upgraded to the BPM 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 283).

End User Management

Resource	Allowed Operations
Applications	Add
	Change
	View
	Delete
	Execute
	Full Control
BPM Agents	View
Script Repository	Add
	Change
	View
	Delete
	Full Control

RUM Administrator

The **RUM Administrator** role can be applied only to the **Business Service Management** resource.

End User Management

Resource	Allowed Operations
Applications	Add
	Change
	View
	Delete
	Execute
	Full Control
RUM Engines	View

RUM Viewer

The **RUM Viewer** role can be applied only to the **Business Service Management** 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 RUM profile in the previous version is upgraded to the **RUM Viewer** role for that profile.

End User Management

Resource	Allowed Operations
Applications	View
RUM Engines	View

User Management Roles Applied to Specific Contexts

The following roles can be applied only to specific contexts within BSM. Details of the resources and contexts on which roles can be applied appear within the description of each role below.

For details about roles that can be applied across BSM, see "User Management Roles Applied Across BSM" on page 282.

This section describes the following roles:

- "BPIAdministrator" on page 303
- "BPIUser" on page 304
- "BPIRestrictedViewUser" on page 304
- "CMDB Open API Query" on page 304
- "CMDB Open API Update" on page 305
- "CMDB Open API Impact" on page 305
- "CMDB Open API Class Model" on page 305
- "SiteScope Administrator" on page 306
- "Default" on page 306
- "TransactionManagementOperator" on page 307
- "TransactionManagementAdministrator" on page 308
- "TransactionManagementUser" on page 309

BPIAdministrator

The **BPIAdministrator** role can be applied only to the **Business Process Insight Administration** resource in the **Business Process Insight** context.

Context	Resource	Allowed Operations
Business Process Insight	Business Process Insight Application	Full Control
	Business Process Insight Administration	Full Control

BPIUser

The **BPIUser** role can be applied only to the **Business Process Insight Application** resource in the **Business Process Insight** context.

Context	Resource	Allowed Operations
Business Process Insight	Business Process Insight Application	View
	Business Process Insight Process Administration	View

BPIRestrictedViewUser

The **BPIRestrictedViewUser** role can be applied only to the **Business Process Insight Application** resource in the **Business Process Insight** context.

Context	Resource	Allowed Operations
Business Process Insight	Business Process Insight Application	View only those deployed BPI processes to which View permission has been granted
	Business Process Insight Process Administration	

CMDB Open API Query

The **CMDB Open API Query** role can be applied only to the **ODB Open API** resource in the **ODB** context.

This role enables users to query the CMDB (Configuration Management Database) for communication with third-party applications.

Context	Resource	Allowed Operations
ODB	ODB Open API	View

CMDB Open API Update

The **CMDB Open API Update** role can be applied only to the **ODB Open API** resource in the **ODB** context.

This role enables users to update the CMDB (Configuration Management Database) for communication with third-party applications.

Context	Resource	Allowed Operations
ODB	ODB Open API	Change

CMDB Open API Impact

The **CMDB Open API Impact** role can be applied only to the **ODB Open API** resource in the **ODB** context.

This role enables users to impact operations on the CMDB.

Context	Resource	Allowed Operations
ODB	ODB Open API	View

CMDB Open API Class Model

The **CMDB Open API Class Model** role can be applied only to the **ODB Open API** resource in the **ODB** context.

This role enables users to perform operations on CITs.

Context	Resource	Allowed Operations
ODB	ODB Open API	View

SiteScope Administrator

The **SiteScope Administrator** role can be applied only to the **SiteScopes** resource in the **System Availability Management** context 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 Operations
System Availability Management	SiteScopes	Add
		Change
		View
		Delete
		Execute
		Full Control

Default

The **Default** role can be applied only to the **Custom Reports** resource in the **User Defined Reports** context.

Context	Resource	Allowed Operations
User Defined Reports	Custom Reports	Add
	Trend Reports	Add

TransactionManagementOperator

The **TransactionManagementOperator** role can be applied only to the **TransactionVision Analyzers** resource in the **Transaction Management** context.

Context	Resource	Allowed Operations
Transaction Management	TransactionVision Analyzers	Execute
	TransactionVision Job Managers	Execute
	TransactionVision Query Engines	Execute
	Administration	Change
	Applications	View

TransactionManagementAdministrator

The **TransactionManagementAdministrator** role can be applied only to the **TransactionVision Processing Servers** resource in the **Transaction Management** context. The **TransactionManagementAdministrator** role is useful in providing added security by enabling users to have Full Control access of TransactionVision administration, but not enabling access to the User Data resource.

Context	Resource	Allowed Operations
Transaction Management	TransactionVision Processing Servers	Change
		Full Control
	TransactionVision Analyzers	Change
		Execute
		Full Control
	TransactionVision Job Managers	Change
		Execute
		Full Control
	TransactionVision Query Engines	Change
		Execute
		Full Control
	Administration	Change
		Full Control
	Applications	Add
		Change
		View
		Full Control

TransactionManagementUser

The **TransactionManagementUser** role can be applied only to the **Applications** resource in the **Transaction Management** context.

Context	Resource	Allowed Operations
Transaction Management	Applications	View

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

This section describes the following HP Business Service Management contexts, and the operations that can be applied to them:

- "Business Process Insight" on page 310
- "Diagnostics" on page 310
- "End User Management" on page 311
- "ODB" on page 313
- "Operations Management" on page 315
- "Operations Orchestration Integration" on page 320
- "Platform" on page 321
- "Service Health" on page 326
- "Service Level Management" on page 327
- "System Availability Management" on page 328
- "Transaction Management" on page 330
- "User Defined Reports" on page 332

Business Process Insight

Use the **Business Process Insight** context to assign permissions to the Business Process Insight instance configured within the system.

Resources	Operation	Description
Business Process Insight Application	View	Enables entering the Business Process Insight application.
Business Process Insight Administration	Full Control	Enables performing all available operations on Business Process Insight administration, and granting and removing permissions for other users.
Business Process Insight Process Definition	View	Enables viewing of a process in the Business Process Insight application.

Diagnostics

Resources	Operation	Description
Opal	Change	Enables viewing Diagnostics administration and configuring the Diagnostics settings
	View	Enables viewing HP Diagnostics when accessing Diagnostics from BSM.
	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

End User Management

The **End User Management** context enables you to define the operations permitted for the End User Management application. Operations assigned to a folder affect all folders contained beneath it.

Resources	Operation	Description
Alert - Notification Template	Add	Enables creating and cloning a notification template.
	Change	Enables editing the properties of a customer-specific notification template.
	View	Enables viewing the properties of a notification template.
	Delete	Enables deleting a notification template.
	Full Control	Enables performing all available operations on a notification template, and granting and removing permissions for those operations.
Alert - 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.

Resources	**Operation**	**Description**
Applications	Add	Enables adding applications
	Change	Enables changing applications
	View	Enables viewing applications
	Delete	Enables deleting applications
	Execute	Enables starting and stopping applications
	Full Control	Enables performing all available operations on applications, and granting and removing permissions for those operations
BPM Agents	View	Enables viewing BPM agents and specific instances of BPMBPM agents
RUM Engines	View	Enables viewing Real User Monitor engine details.
Script Repository	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.
	Delete	Enables deleting a script from the script repository.
	Full Control	Enables performing all available operations on scripts in the script repository, and granting and removing permissions for those operations.

ODB

The ODB context enables you to define the operations permitted for the views defined in IT Universe Administration and viewed in the Model Explorer, Service Health, and Service Level Management.

Tip: If a user has permissions on a view in ODB, 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 and cloning views.
	Change	Enables editing views.
	View	Enables viewing views
	Delete	Enables removing views.
	Full Control	Enables performing all available operations on views.
ODB	Full Control	Enables administrative operations for all of the ODB, except ITU Manager and Modeling Studio.
CI Search	Full Control	Enables the CI Search option from any location in the ODB.
Data Modifier	Full Control	Enables the Data Modifier option from any location in the ODB.
Get Related	Full Control	Enables the Get Related CIs option from any location in the ODB.

Resources	Operation	Description
ITU Manager	Full Control	Allows the user to enter the ITU Manager. Once inside, the available functionality within the ITU Universe Manager depends on permissions the user has been granted on views.
Modeling Studio	Full Control	Allows the user to enter the Modeling Studio. Once inside, the available functionality within the ITU Universe Manager depends on permissions the user has been granted on views.
ODB Open API	Change	Enables running of updates in ODB Open API.
	View	Enables running of queries in ODB Open API.

Operations Management

Note: The **Operations Management** context is available only if you have installed HP OMi on your BSM machine. For details on the HP OMi context, see "User Context Pane" in *Using HP Operations Manager i*.

The HP Operations Manager *i* (HP OMi) context enables you to assign permissions to work with the Operations Manager context. For details on the operations available for the HP Operations Manager *i* (HP OMi) context, see "User Operations Tab" in *Using HP Operations Manager i*.

Resources	Operation	Description
Events assigned to user	Work On / Resolve	Enables the user to set the life cycle status for events that are assigned to them to Work On or Resolve
	Close	Enables the user to set the life cycle status for events that are assigned to them to Closed
	Reopen	Enables the user to set the life cycle status for Closed events that are assigned to them to Open. The events can now be reassigned for further investigation and resolution. **Note:** Reopening symptom events with a closed cause is not possible.
	Assign To	Enables the user to assign events that are assigned to them to a specific user
	Launch Operator Action	Enables the user to run HP Operations Manager operator actions for events assigned to them containing event-related actions

Resources	Operation	Description
Events assigned to user	Launch Automatic Action	Enables the user to run HP Operations Manager automatic actions for events assigned to them containing event-related actions.
	Transfer Control	Enables the user to transfer control of events assigned to them in the Event Browser to an external manager.
	Close Transferred	Enables the user to close events assigned to them in the Event Browser for which control has been transferred to an external manager.
	Add/Remove Event Relations	Enables the user to add and remove relations between events assigned to them in the Event Browser.
	Change Severity	Enables the user to change severity of events assigned to them
	Change Priority	Enables the user to change priority of events assigned to them
	Change Title	Enables the user to change title of events assigned to them
	Change Description	Enables the user to change description of events assigned to them
	Change Solution	Enables the user to change solution of events assigned to them
	Add/Delete/Update Annotations	Enables the user to create, modify and delete annotations for events assigned to them.
	Add/Delete/Update Custom Attributes	Enables the user to create, modify and delete custom attributes for events assigned to them.

Resources	**Operation**	**Description**
Events not assigned to user	View	Enables the user to view events not assigned to them
	Work On / Resolve	Enables the user to set the life cycle status for events not assigned to them to Work On or Resolve
	Close	Enables the user to set the life cycle status for events not assigned to them to Closed
	Reopen	Enables the user to set the life cycle status for Closed events not assigned to them to Open. The events can now be reassigned for further investigation and resolution. **Note:** Reopening symptom events with a closed cause is not possible.
	Assign To	Enables the user to assign events not assigned to them to a specific user or group
	Launch Operator Action	Enables the user to run HP Operations Manager operator actions for events not assigned to them containing event-related actions
	Launch Automatic Action	Enables the user to run HP Operations Manager automatic actions for events not assigned to them containing event-related actions
	Transfer Control	Enables the user to transfer control of events not assigned to them in the Event Browser to an external manager.

Resources	**Operation**	**Description**
Events not assigned to user	Close Transferred	Enables the user to close events not assigned to them in the Event Browser for which control has been transferred to an external manager.
	Add/Remove Event Relations	Enables the user to add and remove relations between events not assigned to them in the Event Browser.
	Change Severity	Enables the user to change severity of events not assigned to them
	Change Priority	Enables the user to change priority of events not assigned to them
	Change Title	Enables the user to change title of events not assigned to them
	Change Description	Enables the user to change description of events not assigned to them
	Change Solution	Enables the user to change solution of events not assigned to them
	Add/Delete/Up date Annotations	Enables the user to create, modify and delete annotations for events not assigned to them.
	Add/Delete/Up date Custom Attributes	Enables the user to create, modify and delete custom attributes for events not assigned to them.
Health Indicators	Reset	Enables the user to clear the current status of a health indicator and reset the health indicator to the status specified in the default health indicator value

Resources	**Operation**	**Description**
Administrative UIs	View	Grants access to the Administration features in the Operations Management Administration, for example: ➤ Correlation Rules manager ➤ Content Packs manager ➤ Performance Graphs manager ➤ View Mappings manager ➤ Event Processing Customization ➤ Custom Actions Users who do not have read access to Operations Management Administration are not able to see the Operations Management Administration features or see an error message when they try to start an Administration manager
Tool Categories	Execute	Grants access to tool categories. Any tools belonging to a tools category to which a user has access can be executed by the user
Custom Actions	Execute	Grants access to custom actions. Any custom actions to which a user has access can be executed by the user

Operations Orchestration Integration

The **Operations Orchestration Administration** context enables you to define the operations permitted for the Operations Orchestration Administration application.

Resources	Operation	Description
Administration	Add	Enables adding a run book.
	View	Enables viewing run book administration.
	Change	Enables editing run book administration.
	Delete	Enables deleting a run book.
	Full Control	Enables performing all available operations on run book administration, and granting or removing permissions for other users.
Execution	Execute	Enables run book execution.
	Full Control	Enables performing all available operations on run book execution, and granting or removing permissions for other users.

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
Authentication Strategy	Change	Enables the **Configure** button on the Authentication Strategy page, which enables changing configurations on the Authentication Strategy Wizard.
	View	Enables viewing the Authentication Strategy Wizard.
	Full Control	Enables performing all available operations on the Authentication Strategy Wizard.
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.
Notification System	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 performing all available operations on sample types, and granting and removing permissions for those operations.
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.
Run executable file	Change	Enables selecting the option to run an executable file on alert, selecting and edition 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.

Resources	Operation	Description
Log To Event Viewer	Change	Enables selecting whether alerts should be logged in the Windows Event Viewer which is accessed from Window Administrative Tools.
	Full Control	Enables selecting whether alerts should be logged in the Windows Event Viewer, and granting and removing permissions on that operation.
Downtime	View	Enables viewing downtime properties
	Full Control	Enables performing all available operations on downtimes, 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
System Recipient Template	Add	Enables creating and cloning system recipient templates.
	Change	Enables editing system recipient templates properties.
	View	Enables viewing system recipient templates properties.
	Delete	Enables deleting a system recipient templates.
	Full Control	Enables performing all available operations on system recipient templates, and granting and removing permissions for those operations.

Service Health

Resources	Operation	Description
User Pages	Add	Enables adding user pages.
	Change	Enables editing user pages
	View	Enables viewing user pages
	Delete	Enables removing user pages
	Full Control	Enables performing all available operations on user pages
Predefined Pages	View	Enables viewing predefined pages

Resources	Operation	Description
User Components	Add	Enables adding and cloning component definitions
	Change	Enables editing component definitions
	View	Enables viewing component definitions
	Delete	Enables removing component definitions
	Full Control	Enables performing all available operations on component definitions

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.

System Availability Management

Use the System Availability Management context to assign permissions to the various SiteScopes configured within the system.

Note: The permission levels granted via the System Availability Management context override any permission levels granted in the SiteScope standalone 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.

Transaction Management

Resources	Operation	Description
TransactionVision Processing Servers	Change	Enables modifying TransactionVision processing servers
	Full Control	Enables performing all available operations on TransactionVision processing servers, and granting and removing permissions for those operations
TransactionVision Analyzers	Change	Enables modifying TransactionVision analyzers
	Execute	Enables starting and stopping TransactionVision analyzers
	Full Control	Enables performing all available operations on TransactionVision analyzers, and granting and removing permissions for those operations
TransactionVision Job Managers	Change	Enables modifying TransactionVision job managers
	Execute	Enables starting and stopping TransactionVision job managers
	Full Control	Enables performing all available operations on TransactionVision job managers, and granting and removing permissions for those operations

Resources	Operation	Description
TransactionVision Query Engines	Change	Enables modifying TransactionVision query engines
	Execute	Enables starting and stopping TransactionVision query engines
	Full Control	Enables performing all available operations on TransactionVision query engines, and granting and removing permissions for those operations
Administration	Change	Enables administration changes. Does not include TransactionVision specific changes
	Full Control	Enables performing all available operations on administration, and granting and removing permissions for those operations
User Data	View	Enables viewing user data in reports and in event details
	Full Control	Enables performing all available operations on user data, and granting and removing permissions for those operations
Applications	Add	Enables adding applications
	Change	Enables modifying applications
	View	Enables viewing applications
	Full Control	Enables performing all available operations on applications, and granting and removing permissions for those operations

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	Add	Enables adding 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	Add	Enables creating 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.
Favorite Filter	Change	Enables editing favorite filter.
	Delete	Enables deleting favorite filter
	Full Control	Enables performing all available operations on favorite filter, and granting and removing permissions for those operations.
Annotation	Change	Enables editing an annotation.
	Delete	Enables deleting an annotation.
	Full Control	Enables performing all available operations on annotations, and granting and removing permissions for those operations.

Resources	Operation	Description
Service Report	Change	Enables editing a service report.
	Delete	Enables deleting a service report.
	Full Control	Enables performing all available operations on service reports, and granting and removing permissions for those operations.

User Management User Interface

This section includes:

- Create Group Dialog Box on page 334
- Create User Dialog Box on page 335
- Customization Tab (User Management) on page 336
- General Tab (User Management) on page 338
- Recipient Tab (User Management) on page 341
- Hierarchy Tab (User Management) on page 341
- Permissions Tab (User Management) on page 344
- User Management Main Page on page 350

Create Group Dialog Box

This dialog box enables you to create groups.

To access	Select **Admin** > **Platform** > **Users and Permissions** > **User Management**, click the **Create**.
See also	"Group and User Hierarchy" on page 253

User interface elements are described below:

UI Elements (A-Z)	Description
Group description	Description of the group **Syntax Exceptions:** ➤ Cannot exceed 99 characters
Group name	The name of the group **Syntax Exceptions:** ➤ Cannot exceed 40 characters ➤ The following characters are not supported: " \ / [ ] : | < > + = ; , ? * % & ➤ The name must be unique

Create User Dialog Box

This dialog box enables you to create a user and a recipient linked to the user.

To access	Select **Admin** > **Platform** > **Users and Permissions** > **User Management**, click the **Create a user/group in the selected group** ✱ button, and select **Create User**.
Important information	The Create User dialog box includes the following tabs: ➤ **User Account.** For details, see "General Tab (User Management)" on page 338. ➤ **Recipient.** For details, see "Recipient Tab (User Management)" on page 341.
Relevant tasks	➤ "How to Configure Users and Permissions - Workflow" on page 256 ➤ "How to Customize User Menus" on page 274
See also	"User Management – Overview" on page 244

Customization Tab (User Management)

This tab enables you to select the page users see when entering HP Business Service Management, and choose the menu items available on pages throughout HP Business Service Management.

To access	Select **Admin** > **Platform** > **Users and Permissions** > **User Management**, select a user from the **Groups/Users** pane, and click the **Customization** tab.
Important information	The Customization tab is displayed only when a user has been selected in the **Groups/Users** pane on the left side of the page.
Relevant tasks	➤ "How to Configure Users and Permissions - Workflow" on page 256 ➤ "How to Customize User Menus" on page 274
See also	"Customizing User Menus" on page 255

User interface elements are described below:

UI Elements (A-Z)	Description
Contexts	Select an HP Business Service Management context. You can perform the following actions on the context: ➤ Select contexts and applications in the Contexts pane to be visible for the specified user. To hide a context or application, clear the check box. By default, all contexts are visible. ➤ Select pages and tabs in the Pages and Tabs pane to be visible for the specified user. By default, all pages and tabs are visible. ➤ Click the **Set as Default Entry Context** button to make it the context that is displayed when the user logs into HP Business Service Management. For details on HP Business Service Management contexts, see "Resource Contexts" on page 346.
Pages and Tabs	➤ Select the pages and tabs you want to be visible for the HP Business Service Management 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	Sets the selected context in the Contexts pane as the entry context that is displayed when the specified user logs into HP Business Service Management. **Note:** The **Default Entry Context** icon appears next to the specified context.
Set as Default Entry Page	Assigns 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.

General Tab (User Management)

This tab displays the parameters of the selected user or group.

To access	Select **Admin** > **Platform** > **Users and Permissions** > **User Management** > **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.
Relevant tasks	"How to Configure Users and Permissions - Workflow" on page 256
See also	➤ "User Management – Overview" on page 244 ➤ "Create Group Dialog Box" on page 334 ➤ "Create User Dialog Box" on page 335 ➤ "Groups/Users Pane" on page 351

User interface elements are described below when you select a user in the left pane:

UI Elements (A-Z)	Description
Confirm password	Re-enter the edited password that you entered in the **Password** field.
Login name	The name that the user uses to log into HP Business Service Management. **Syntax Exceptions:** ➤ Cannot exceed 99 characters ➤ The following characters are not supported: " \ / [ ] : | < > + = ; , ? * % & <space> ➤ The name must be unique **Notes:** ➤ The Login name appears as a tooltip when hovering over the user name in the Browse tab of the **Groups/Users** pane. ➤ The Login name cannot be changed.
Password	The password of the user used to log into HP Business Service Management. **Syntax Exceptions:** ➤ Cannot exceed 20 characters **Notes:** ➤ 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. ➤ Only the user assigned as security officer can change his or her own password
Time zone	The time zone of the user's location as specified in the Create User dialog box. **Note:** When you modify the time zone, the linked recipient offset from GMT is also updated after you confirm the change.

UI Elements (A-Z)	Description
User mode	The user mode, as configured in the Create User dialog box. Available options are: ➤ **Unspecified.** Leaves the user without a particular mode. Select this option if: ➤ HP Business Service Management 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 in the Create User dialog box. **Syntax Exceptions:** ➤ Cannot exceed 50 characters ➤ The following characters are not supported: " \ / [ ] : | < > + = ; , ? * % &

User interface elements are described below when you select a group in the left pane:

UI Elements (A-Z)	Description
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.

Recipient Tab (User Management)

This tab enables you to define recipients, their email, pager, and SMS information, and the template to use to send alert notices, or scheduled reports to those recipients.

For concept details, see "Recipient Management Overview" on page 358.

For user interface details, see "New or Edit Recipient Dialog Box" on page 366.

Hierarchy Tab (User Management)

This tab 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** > **User Management**, select a group or user from the **Groups/Users** pane, and click the **Hierarchy** tab. The Hierarchy tab displays: ➤ **Parent Groups.** The groups that the selected group is nested under. ➤ **Child Groups and Users.** The groups and users that are nested directly beneath the selected group.
Important information	➤ To nest a user, you must select the group into which you want to nest it and click the **Edit Child Groups and Users** button. ➤ When removing a nested group from its parent, the group itself is not deleted. ➤ When deleting a parent group, the child groups and users are not deleted. ➤ If HP Business Service Management groups have been synchronized with groups on an external LDAP server, HP Business Service Management users cannot be moved between groups, and only groups appear on the interface. For details on synchronizing groups, see "Synchronizing Users" on page 434.

Relevant tasks	➤ "How to Configure Users and Permissions - Workflow" on page 256 ➤ "How to Configure Group and User Hierarchy" on page 271
See also	"Group and User Hierarchy" on page 253

User interface elements are described below:

UI Elements (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	Opens the Edit Child Groups and Users window enabling you to nest or remove groups and users from the selected group. For details, see "Edit Child Groups and Users Dialog Box" on page 343. **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

User interface elements are described below:

UI Elements (A-Z)	Description
▷	Moves the group or user to the **Child Groups and Users** pane and nests the group or user under the specified group.
◁	Moves the group or user to the **Groups/Users** pane and removes 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.

Permissions Tab (User Management)

This tab 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** > **User Management** > **Permissions** tab. The **Permissions** tab is divided into the following areas: ➤ **Groups/Users** pane on the left side of the page. For details, see "Groups/Users Pane" on page 351. ➤ Resource tree pane in the center of the page. For details, see "Resource Tree Pane" on page 345. ➤ **Roles** tab on the right side of the page. For details, see "Roles Tab" on page 347. ➤ **Operations** tab on the right side of the page. For details, see "Operations Tab" on page 348.
Important information	➤ 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 via the Hierarchy tab. For details, see "Hierarchy Tab (User Management)" on page 341.
Relevant tasks	➤ "How to Configure Users and Permissions - Workflow" on page 256 ➤ "How to Assign Permissions" on page 269
See also	"Permissions Overview" on page 246

Resource Tree Pane

This tab displays the instances and resources available within each HP Business Service Management context for which you set permissions.

To access	Select **Admin** > **Platform** > **Users and Permissions** > **User Management** > **Permissions** tab. The types of resources displayed in the Resource Tree pane are: ➤ Resource with instances 📁 ➤ Instances of a resource 📁✳ **Note:** When a user defines or creates an instance of a resource, for example creates a Business Process profile, that user has **Full Control** permission on that resource instance and all of its child resources. ➤ Resource without instances ▦
Important information	➤ The **Business Service Management** resource refers to all contexts in HP Business Service Management 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. ➤ You can select multiple resources only when selecting instances. For information on instances, see "Resources and Resource Instances" on page 248.
Relevant tasks	"How to Assign Permissions" on page 269
See also	➤ "Understanding Permissions Resources" on page 247 ➤ "Resource Contexts" on page 346

User interface elements are described below:

UI Elements (A-Z)	Description
📁✳	An instance of a resource.
▦	A resource without instances.

UI Elements (A-Z)	Description
📁	A resource that has instances (a resource collection).
Select Context	Select an HP Business Service Management context for which to configure permissions. For details on the HP Business Service Management contexts, see "Resource Contexts" on page 346.
Settings	Applies 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 Service Management session.

Resource Contexts

The following contexts are included:

UI Elements (A-Z)	Description
Business Process Insight	Includes the resources enabling permissions for operating and administering the Business Process Insight application.
Diagnostics	Includes all the resources relating to HP Diagnostics

UI Elements (A-Z)	Description
End User Management	Includes all the resources relating to operating and administering the End User Management application
ODB	Includes all the resources for the ODB
Operations Management	Includes all the resources relating to the Operations Management application
Operations Orchestration Integration	Includes the resources enabling permissions for operating and administering the Operations Orchestration Administration application
Platform	Includes all the resources for administering the platform
Service Health	Includes all the resources relating to the Service Health application
Service Level Management	Includes the SLA resource
System Availability Management	Includes the various SiteScope groups
Transaction Management	Includes the resources relating to working with the TransactionVision application.
User Defined Reports	Includes the custom report, trend report, custom link, and Excel report resources.

Roles Tab

Displays the roles configurable for groups and users in HP Business Service Management.

To access	Select **Admin** > **Platform** > **Users and Permissions** > **User Management** > **Permissions** tab
Relevant tasks	"How to Assign Permissions" on page 269
See also	➤ "Understanding Permissions Resources" on page 247 ➤ "User Management Roles Applied Across BSM" on page 282

User interface elements are described below:

UI Elements (A-Z)	Description
Apply Permissions	Applies the permissions configured for the roles
Grant	Select the check box to assign the specified roles to the group or user.
Roles	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 Roles Applied Across BSM" on page 282.

Operations Tab

Displays the predefined operations configurable for groups and users in HP Business Service Management.

To access	Select **Admin** > **Platform** > **Users and Permissions** > **User Management** > **Permissions** tab
Relevant tasks	"How to Assign Permissions" on page 269
See also	➤ "Understanding Permissions Resources" on page 247 ➤ "User Management Operations" on page 309

User interface elements are described below:

UI Elements (A-Z)	Description
Apply Permissions	Applies the permissions configured for the resource.
Grant	Select the check box to assign the specified operation to the group or user.

UI Elements (A-Z)	Description
Granted from Group/Role/Parent	Displays those permissions that have been granted from either a group, a role, or a parent resource. **Note:** ➤ 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. **Note:** ➤ 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 "User Management Operations" on page 309.

User Management Main Page

This page displays information on the groups and users configured to access HP Business Service Management, including their respective permission levels.

To access	Select **Admin** > **Platform** > **Users and Permissions** > **User Management**
Important information	When you first access the User Management page or the cursor is located on the **All** node, the page includes: ➤ the **Groups/Users** pane. For details, see "Groups/Users Pane" on page 351. ➤ the **workflow** pane. The Workflow page displays introductory information about the User Management application, and a suggested workflow for configuring groups and users. When you select a **user**, the page includes the following tabs: ➤ **General.** For details, see "General Tab (User Management)" on page 338. ➤ **Recipient.** For details, see "Recipient Tab (User Management)" on page 341. ➤ **Permissions.** For details, see "Permissions Tab (User Management)" on page 344. ➤ **Hierarchy.** For details, see "Hierarchy Tab (User Management)" on page 341. ➤ **Customization.** For details, see "Customization Tab (User Management)" on page 336. When you select a **group**, the page includes the following tabs: ➤ **General.** For details, see "General Tab (User Management)" on page 338. ➤ **Permissions.** For details, see "Permissions Tab (User Management)" on page 344. ➤ **Hierarchy.** For details, see "Hierarchy Tab (User Management)" on page 341.

Relevant tasks	"How to Configure Users and Permissions - Workflow" on page 256
See also	➤ "User Management – Overview" on page 244 ➤ "Groups/Users Pane" on page 351

Groups/Users Pane

This pane displays the list of users and groups of users configured to access HP Business Service Management.

To access	Select **Admin** > **Platform** > **User Management**. The Groups/Users pane appears on the left side of the page, and is visible on all tabs 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.
Important information	➤ 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 with the cursor on a group, the users are automatically nested within that group.

Relevant tasks	"How to Configure Users and Permissions - Workflow" on page 256
See also	"User Management Main Page" on page 350

User interface elements are described below:

UI Elements	Description
✱ ▾	Creates a user or group. Depending on whether you choose to create a user or group, the **Create User** or **Create Group** window opens. For details, see "Create User Dialog Box" on page 335 or "Create Group Dialog Box" on page 334.
⧉	Clones the settings of an existing user or group to a new user or group
✖	Deletes the selected user or group. **Note:** When you delete a user, the linked recipient is also deleted.
⏫ ⏬	Collapses or expands the groups selected in the hierarchy tree. **Note:** Only previously loaded nodes are expanded.
👥 ▾	Click and select **Group Mappings** to map local groups to groups configured on the LDAP server, or **Delete Obsolete Users** to delete HP Business Service Management 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 354. **Note:** This button is displayed only if the Mapping option has been enabled in the Authentication Strategy Wizard. For details, see "Authentication Wizard" on page 400.

UI Elements	Description
🔑	Click to assign or view the Security Officer. The security officer is a user who can configure certain sensitive reporting information in the system, such as which RUM transaction parameters to include or exclude from certain reports (Session Details, Session Analyzer, etc). There can be only one security officer assigned in the system. Only a user with superuser permissions can assign the security officer for the first time. Only the security officer himself can assign it to another user or change his own password once it has been assigned. For details on this topic, see "Security Officer" on page 252.
👤	A configured user
📁	A configured group
🔑	Security officer
📁	Root node

Group Mappings Dialog Box

This dialog box enables you to map groups configured in HP Business Service Management to groups configured on the LDAP server.

To access	Select **Admin** > **Platform** > **Users and Permissions** > **User Management**. In the Groups/Users pane, click the **LDAP Configuration** button and select **Group Mappings**. The Group Mappings dialog box consists of the following panes: ➤ **Corporate Directory Pane.** For details, see "Corporate Directory Pane" on page 355. ➤ **BSMLocal Repository For Remote Group Pane: <group name>.** For details, see "BSM Local Repository for Remote Group: <group name> Pane" on page 356. ➤ **Local Groups to Remote Group Mappings.** Displays a table of the LDAP groups and the BSM groups that they are assigned to. The LDAP groups are displayed in the **Remote Group Name** column, and the BSM Groups are listed in the **Local Group Name** column.
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.

Corporate Directory Pane

This pane enables you to assign HP Business Service Management groups to LDAP groups, and to list the users in the LDAP groups.

Description	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 Service Management 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 Service Management groups, the HP Business Service Management 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.

BSM Local Repository for Remote Group: <group name> Pane

This pane displays the HP Business Service Management mapped to the LDAP group selected in the Corporate Directory Pane, and enables you to remove the mapped HP Business Service Management 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.

14

Recipient Management

This chapter includes:

Concepts

Tasks

Reference

Concepts

Recipient Management Overview

You can assign recipients to users. A recipient definition includes information about how to communicate with the recipient. Recipients can receive triggered alerts or scheduled reports:

- **Alerts.** For each recipient, you define one or more notification methods (email, pager, or SMS) and the template to use for alert notices. You can configure alerts so specific recipients receive information about the alerts when they are triggered. For details about alerts, see "Alerts Overview" on page 464.
- **Scheduled reports.** You can also configure, in the Report Manager, the scheduled intervals when recipients can receive reports or report items. Only those recipients who have been configured to receive email can be selected to receive scheduled reports. These recipients are listed in Available Recipients when configuring scheduled reports. For details about scheduled reports, see "Report Schedule Manager — Overview" on page 458.

For details on where to configure and manage recipients, see "Recipients Page" on page 363.

Tasks

How to Configure and Manage Recipients

This task describes a suggested working order for managing recipients.

You create recipients by defining one or more notification methods, the template to use for alert notices, and a notification schedule to receive reports. You create recipients and manage existing recipients in the Recipients page. For user interface details, see "Recipients Page" on page 363.

You can also create recipients while you are configuring users. Those recipients are automatically added to the list of recipients in the Recipients page in **Admin** > **Platform** > **Recipients** > **Recipient Management**.

The recipients you create in the Recipients page are automatically listed as available recipients when you configure users in **Admin** > **Platform** > **Users and Permissions** > **User Management**.

Add a Custom Pager or SMS Service Provider

If you are configuring alerts to be sent via pager or SMS, and your pager or SMS service provider does not appear on the default provider list, and the provider uses an email gateway, you can manually add your provider to HP Business Service Management. After doing so, your provider appears on the list.

To add a provider that uses an email gateway, manually add the gateway information to the management database. If necessary, ask your database administrator for assistance.

To add a provider that uses an email gateway:

1 Open the **NOTIFICATION_PROVIDERS** table in the management database.

2 In the **NP_NOTIFICATION_PROVIDER_NAME** column, add the name of the provider to the bottom of the list.

Add the name exactly as you want it to appear in the provider list that opens in the SMS tab of the Recipient Properties wizard. For details, see "SMS Tab" on page 374.

Note the ID number that is automatically assigned to the provider.

3. Close the **NOTIFICATION_PROVIDERS** table, and open the **NOTIFPROVIDER_NOTIFTYPE** table.

4. In the **NN_NOTIF_PROVIDER_ID** column, add the ID number that was assigned to the new provider in step 2 on page 359.

5. In the **NN_NOTIF_TYPE_ID** column, assign the provider one of the following notification types:

   - **102** – for pager service provider
   - **101** – for SMS service provider

6. Close the **NOTIFPROVIDER_NOTIFTYPE** table, and open the **NOTIFICATION_PROVIDER_PROP** table.

7. In the **NPP_NOTIFICATION_PROVIDER_ID** column, add the ID number that was assigned to the new provider in step 2 on page 359.

   Note that you add the ID number to two consecutive rows.

8 In the **NPP_NPROVIDER_PROP_NAME** and **NPP_NPROVIDER_PROP_VALUE** columns, add the following new property names and values for the provider, one beneath the other (for examples, see existing entries):

Property Name	Property Value	Description
EMAIL_SUFFIX	<email_suffix>	The gateway's email suffix. For example, if the gateway email address is 12345@xyz.com, enter xyz.com as the property value for EMAIL_SUFFIX.
EMAIL_MAX_LEN	<max_length>	The maximum message length, in characters, of the body of the email message. For example, 500. When determining this value, take into consideration the maximum length limit imposed by your service provider, as well as limitations to your pager or mobile phone.

9 In the **NPP_NPROVIDER_PROP_DATATYPE_ID** column, specify an ID value as follows:

- for EMAIL_SUFFIX, specify: 1
- for EMAIL_MAX_LEN, specify: 2

10 Restart HP Business Service Management.

Reference

Recipient Management User Interface

This section includes:

- Attach Recipient to a User Dialog Box on page 362
- Recipients Page on page 363
- New or Edit Recipient Dialog Box on page 366

Attach Recipient to a User Dialog Box

This dialog box enables you to select the user you want to attach to the selected recipient.

To access	Select **Admin** > **Platform** > **Recipients** > **Recipient Management** tab. Select a recipient in the table and click the **Attach user to selected recipient** button in the Recipient page.
See also	"Group and User Hierarchy" on page 253

User interface elements are described below:

UI Elements (A-Z)	Description
User Login	The name used to log into HP Business Service Management.
User Name	The name of the user, as configured in the User Management page.
Select	To assign a user to the selected recipient, select the user and click **Select**.

Recipients Page

Enables you to create or edit recipient information including the corresponding user and the email, SMS, and pager information. You can also, if you have the appropriate permissions, detach the current recipient from the user, attach existing recipients to the user, or delete the attached recipient.

To access	Select **Admin** > **Platform** > **Recipients** > **Recipient Management**
Important information	➤ How you access the Recipients page and what you see in the page depends on your user's permissions. For details, see "Permissions Tab (User Management)" on page 344. ➤ To filter the information displayed in the table, enter the string in the box at the top of the relevant column and press ENTER. Only the appropriate table lines are displayed. To reset the filter, erase the string you used to filter the information and press ENTER. ➤ There is a one-to-one relationship between the user and the recipient: a recipient can be assigned to one user or to no user, and a user can have a link to one recipient or to no recipient.
Relevant tasks	"How to Configure and Manage Recipients" on page 359
See also	"Recipient Management Overview" on page 358

User interface elements are described below:

UI Elements (A-Z)	Description
✳	**Add new recipient.** Opens the New Recipient dialog box. For details, see "New or Edit Recipient Dialog Box" on page 366.
✎	**Edit selected recipient.** Opens the Edit Recipient dialog box. For details, see "New or Edit Recipient Dialog Box" on page 366.

UI Elements (A-Z)	Description
❌	**Delete the recipient attached to the selected user.** Detaches the recipient and deletes the current recipient.
👤	**Attach user to selected recipient.** Select a recipient in the list of and click this button to open the Attach Recipient to a User dialog box where you can select the appropriate user. For details, see "Attach Recipient to a User Dialog Box" on page 362.
👤	**Detach user from selected recipient.** Detaches the current recipient from the corresponding user (listed in the page). A confirmation message is issued.
✉	**Update selected recipients email address from LDAP.** This icon appears only if LDAP is connected to the BSM application. Click to synchronizes the user data, meaning that the email information stored in the User Repository for the specific user updates the email recipient information corresponding to the user linked to the recipient.
Email	The email address of the recipient as defined in the General tab.
Linked User	The name of the user linked to the recipient. **Important:** Cannot exceed 49 characters. **Syntax Exceptions:** The following characters are not supported: ‘ ~ ! @ # $ % ^ & * - + = [ ] { } \ | / ? . , " ' : ; < >
Pager	The pager numbers of the recipient. **Syntax Exceptions:** ➤ The following characters are not supported: @ & " ' ... ➤ The following special characters are allowed: ( ) - _ + = [ ] { } | : ; < > . ,

UI Elements (A-Z)	Description
Recipient Name	The name of the recipient. **Important:** Cannot exceed 49 characters. **Syntax Exceptions:** The following characters are not supported: ‘ ~ ! @ # $ % ^ & * - + = [ ] { } \ | / ? . , " ’ : ; < >
SMS	The SMS numbers of the recipient. **Syntax Exceptions:** ➤ The following characters are not supported: @ & " ' ... ➤ The following special characters are allowed: ( ) - _ + = [ ] { } | : ; < > . ,

New or Edit Recipient Dialog Box

This tab enables you to define recipients their email, pager and SMS, and the template to use to send alert notices to those recipients.

To access	You can also access this page from: ➤ Select **Admin** > **Platform** > **Recipients** > **Recipient Management**, and click ✱ . ➤ Select **Admin** > **Platform** > **Users and Permissions** > **User Management**, select a user, and click the **Recipient** tab. ➤ Select **Admin** > **Personal Settings** > **Recipient**. ➤ Click the **New Recipient** button in the **Templates and Recipients** page in the Create New Alert wizard for CI Status alerts. For details, see "Templates and Recipients Page" in *Using Service Health*. ➤ Click the **New Recipient** button in the **Templates and Recipients** page in the Create New Alert wizard for SLA alerts. For details, see "Templates and Recipients Page" in *Using Service Level Management*. ➤ Click the **Create Recipient** button in the Attach Recipient dialog box for event-based alerts. For details, see "Attach Recipients Dialog Box"in *Using End User Management*. ➤ Click the **New Recipient** button in the **Report Manager Main** page. For details, see "Report Manager Main Page" in *Reports*.
Important information	➤ How you access the Recipients page and what you see in the page depends on your user's permissions. For details, see "Permissions Tab (User Management)" on page 344. ➤ There is a one-to-one relationship between the user and the recipient: a recipient can be assigned to one user or to no user, and a user can have a link to one recipient or to no recipient.
Relevant tasks	"How to Configure and Manage Recipients" on page 359
See also	"Recipient Management Overview" on page 358

User interface elements are described below:

UI Elements (A-Z)	Description
👤	**Attach user to selected recipient.** Select a recipient in the list of and click the button to open the Attach Recipient to a User dialog box where you can select the appropriate user. For details, see "Attach Recipient to a User Dialog Box" on page 362. **Note:** This button is displayed only when you access the dialog box from **Admin** > **Platform** > **Users and Permissions** > **User Management**.
👤	**Detach user from selected recipient.** Detaches the current recipient from the corresponding user (listed in the page). A confirmation message is issued. **Note:** This button is displayed only when you access the dialog box from **Admin** > **Platform** > **Users and Permissions** > **User Management**.
✖	**Delete the recipient attached to the selected user.** Detaches the recipient from the user and deletes the recipient. **Note:** This button is displayed only when you access the dialog box from **Admin** > **Platform** > **Users and Permissions** > **User Management**.
✉	**Update selected recipients email address from LDAP.** This icon appears only if LDAP is connected to the BSM application. Click to synchronize the user data, meaning that the email information stored in the User Repository for the specific user updates the email recipient information corresponding to the user linked to the recipient.

UI Elements (A-Z)	Description
Alert notification template	Select the template you want to use for the EUM alert notification, or any custom template already created. **Note:** When you change the selection in the **Alert notification template** field in the top part of the page, the changes are propagated to the Email, Pager, and SMS tabs in the same page. If you modify the selection in the **Alert notification template** field in the Email, Pager, or SMS tabs, the **Schedule for receiving alerts** changes to **Mixed Value**. When you change once more, the selection in the **Alert notification template** field in the top part of the page, the changes are propagated to the Email, Pager, and SMS tabs in the same page and the **Mixed Value** button is cleared. For details on alert notification templates and creating custom templates, see "How to Configure EUM Alerts Notification Templates" on page 488. **Note:** This field is relevant only for event-based alerts. For details on alert notification templates and creating custom templates, see "Notification Templates Page" on page 497. **Note:** ➤ The default template is **LONG**. ➤ For details on the parameters displayed in each template, see "Default Notification Templates" on page 378. ➤ The field lists the default templates and the custom templates. ➤ You must select the alert notification template and specify an alert notices schedule for alert recipients. You do not have to perform this procedure for recipients who are to receive only scheduled reports.

<table>
<tr><th>UI Elements (A-Z)</th><th>Description</th></tr>
<tr><td><b>Link to user</b></td><td>This field is displayed only when you access this page from:
➤ <b>Admin</b> > <b>Platform</b> > <b>Users and Permissions</b> > <b>User Management</b>, select a user in the tree and click the <b>Recipient</b> tab.
➤ <b>Admin</b> > <b>Personal Settings</b> > <b>Recipient</b>.</td></tr>
<tr><td><b>Recipient name</b></td><td>The name of the recipient.
<b>Important:</b> Cannot exceed 49 characters.
<b>Syntax Exception:</b> The following characters are not supported: ` ~ ! @ # $ % ^ & * - + [ ] { } \ | / ? " ' < ></td></tr>
</table>

UI Elements (A-Z)	Description
Schedule for receiving alerts	Enabled if you selected the **Per notification method** scheduling option for the recipient in the **Schedule for Receiving Alerts** in the General tab. Select: ➤ **Mixed value.** When you change the selection in the **Alert notification template** field in the top part of the page, the changes are propagated to the Email, Pager, and SMS tabs in the same page. If you modify the selection in the **Alert notification template** field in the Email, Pager, or SMS tabs, the **Schedule for receiving alerts** changes to **Mixed Value**. When you change once more, the selection in the **Alert notification template** field in the top part of the page, the changes are propagated to the Email, Pager, and SMS tabs in the same page and the **Mixed Value** button is cleared. ➤ **All Day.** If you want the recipient to receive email messages all day. ➤ **From... to.** If you want the recipient to receive email messages during the specified time period. The time range is calculated based on the GMT offset selected for the recipient. Scheduled reports are sent based on the schedule configured in the Scheduled Reports page and not on the schedule configured for the recipient. For details, see "How to Schedule a Report" in *Reports*.

UI Elements (A-Z)	Description
Time zone	Select the time zone for the recipient (GMT). Business Service Management uses the time zone to send alert notices and HP Software-as-a-Service notifications to the selected recipient. **Note:** ➤ The GMT time zone selected for the recipient is the time zone specified in the alert notifications that the recipient receives. For example, if an alert is triggered anywhere in the world and a notification is sent, the date and time of the alert are converted to the recipient local time. The alert also specifies the GMT offset of the recipient. ➤ If you defined a notification schedule for the recipient, the GMT time zone selected for the recipient is also the time zone that HP Business Service Management uses for calculating when to send the recipient notifications. For example, if you configure a recipient to receive pager alerts from 9:00 AM - 9:00 PM, and choose a GMT offset of -5 hours, the recipient receives alerts through a pager only from 9:00 AM - 9:00 PM Eastern Time. Scheduled reports are sent based on the schedule configured in the Scheduled Reports page and not on the schedule configured for the recipient. For details, see "How to Schedule a Report" in *Reports*. ➤ When you modify the time zone of the user to which the recipient is assigned, a confirmation message is issued to verify that you also want to propagate the time zone change to the recipient’s offset from GMT. If you change the recipient’s offset from GMT., the time zone of the user to which the recipient is assigned is not affected.

Communication Method Area

Important information	This area includes the following tabs: ➤ "Email Tab" on page 372 ➤ "SMS Tab" on page 374 ➤ "Pager Tab" on page 376

Email Tab

Enables you to specify multiple email addresses for the recipient, the type of notification template, which overrides the notification template selected in the global level in the page, the schedule for sending email notifications, and the security certificate if necessary.

To access	Select **Admin** > **Platform** > **Users and Permissions** > **User Management**, select a user in the tree and click the **Recipient** tab. In the Communication Method pane for the user, click the **Email** tab.
Important information	Only those recipients who have been configured to receive email can be selected to receive scheduled reports and are listed in Available Recipients when configuring scheduled reports. **Note:** The text displayed in email messages can only be in English except for the contents of fields inserted by the user that can be in any supported and relevant language. Those fields can be for example: Alert Name, Alert description, KPI name, and so on.

User interface elements are described below:

UI Elements (A-Z)	Description
Alert notification template	Select the template you want to use. For details, see "EUM Alerts Notification Templates" on page 486. **Note:** When you change the selection in the **Alert notification template** field in the top part of the page, the changes are propagated to the Email, Pager, and SMS tabs in the same page. If you modify the selection in the **Alert notification template** field in the Email, Pager, or SMS tabs, the **Schedule for receiving alerts** changes to **Mixed Value**. When you change once more, the selection in the **Alert notification template** field in the top part of the page, the changes are propagated to the Email, Pager, and SMS tabs in the same page and the **Mixed Value** button is cleared.
Email Addresses	Enter one or more email addresses. Separate multiple entries with a semi-colon (;).
Enable secure mail	Select this option if you want the recipient to receive encrypted mail. You must then copy, into the text box below the option, the contents of the certificate that the recipient uses to secure incoming email messages. **Note:** ➤ The encrypted mail option is supported only for alerts. Encrypted mail is not supported for scheduled reports or subscription and package notifications (HP Software-as-a-Service customers only). ➤ The encrypted mail option is supported only when the HP Business Service Management Data Processing Server is installed on a Windows machine.
Schedule for receiving Email messages	Select the schedule you want to use for receiving emails. For details, see **Schedule for receiving alerts** in "New or Edit Recipient Dialog Box" on page 366.

SMS Tab

This tab enables you to specify the SMS (short message service) service provider, the SMS numbers, the type of notification template, which overrides the notification template selected in the global level in the page, and the schedule for sending alert notifications to the SMS.

To access	Select **Admin** > **Platform** > **Users and Permissions** > **User Management**, select a user in the tree and click the **Recipient** tab. In the Communication Method pane for the user, click the **SMS** tab.
Important information	SMS is a text messaging service provided by most GSM-based cellular phone providers. SMS messages are useful to notify staff who are mobile, or who do not have email or pager access. Note that the maximum message length of SMS text messages is generally 160 characters. **Note:** You can use a pager or an SMS service provider that does not appear on the default list. For details, see "Add a Custom Pager or SMS Service Provider" on page 359.

User interface elements are described below:

UI Elements (A-Z)	Description
Alert notification template	Select the template you want to use. For details, see "EUM Alerts Notification Templates" on page 486. **Note:** When you change the selection in the **Alert notification template** field in the top part of the page, the changes are propagated to the Email, Pager, and SMS tabs in the same page. If you modify the selection in the **Alert notification template** field in the Email, Pager, or SMS tabs, the **Schedule for receiving alerts** changes to **Mixed Value**. When you change once more, the selection in the **Alert notification template** field in the top part of the page, the changes are propagated to the Email, Pager, and SMS tabs in the same page and the **Mixed Value** button is cleared.
Provider	Select an SMS service provider from the list: ➤ **Genie-UK** ➤ **Itineris** ➤ **SFR-France** ➤ **GoSMS-Israel** ➤ **MtnSMS-Global** **Note:** If your provider does not appear on the default provider list, and the provider uses an email gateway, you can manually add your provider to HP Business Service Management. For details, see "Add a Custom Pager or SMS Service Provider" on page 359.
Schedule for receiving SMS messages	Select the schedule you want to use for receiving SMS text messages. For details, see **Schedule for receiving alerts** in "New or Edit Recipient Dialog Box" on page 366.
SMS numbers	Type one or more SMS access numbers in the box. Separate multiple entries with a semi-colon (;).

Pager Tab

This tab enables you to specify the pager service provider, the pager numbers, the type of notification template, which overrides the notification template selected at the global level in the page, and the schedule for sending alert notification to the pager.

To access	Select **Admin** > **Platform** > **Users and Permissions** > **User Management**, select a user in the tree and click the **Recipient** tab. In the Communication Method pane for the user, click the **Pager** tab.
Important information	You can use a pager that does not appear on the default list. For details, see "Add a Custom Pager or SMS Service Provider" on page 359. **Note:** The text displayed in pager messages can only be in English except for the contents of fields inserted by the user that can be in any supported and relevant language. Those fields can be for example: Alert Name, Alert description, KPI name, and so on.

User interface elements are described below:

UI Elements (A-Z)	Description
Alert notification template	Select the template you want to use. For details, see "EUM Alerts Notification Templates" on page 486. **Note:** When you change the selection in the **Alert notification template** field in the top part of the page, the changes are propagated to the Email, Pager, and SMS tabs in the same page. If you modify the selection in the **Alert notification template** field in the Email, Pager, or SMS tabs, the **Schedule for receiving alerts** changes to **Mixed Value**. When you change once more, the selection in the **Alert notification template** field in the top part of the page, the changes are propagated to the Email, Pager, and SMS tabs in the same page and the **Mixed Value** button is cleared.
Pager Numbers	Enter one or more pager access numbers. Separate multiple entries with a semi-colon (;). **Note:** If your pager is numeric only, when creating an alert scheme in the Alert Wizard, you can only type a numeric user message.
Schedule for receiving pager message	Select the schedule you want to use for receiving pager messages. For details, see **Schedule for receiving alerts** in "New or Edit Recipient Dialog Box" on page 366
Type	Select a pager service provider. The following providers are supported: ➤ **MetroCall** ➤ **Arch** ➤ **AirTouch** ➤ **PageMci** ➤ **SkyTel** ➤ **PageNet** ➤ **PageMart** ➤ **AmeriPage** ➤ **Nextel** ➤ **PageOne**

Default Notification Templates

Important information	Each template enables you to display, in the notification, selected information that corresponds to specific parameters. For details on the parameters displayed in each template, see “Notification Template Properties Dialog Box” on page 490.

The following default notification templates are available:

UI Elements (A-Z)	Description
DEFAULT OM FOLLOW-UP FORMAT	
DEFAULT OM FORMAT	
DEFAULT_LOG_FORMAT	Includes all the elements needed to create a default long format notification for reports.
DEFAULT_POSITIVE_FORMAT	Includes all the elements needed to create a default long format notification for positive or follow-up alerts. For details on follow-up alerts, see "How to Configure a Template for Clear Alert Notifications" on page 489.
LONG	Includes all the elements needed to create a default long format notification.
SHORT	Includes all the elements needed to create a default short format notification.

15

Personal Settings

This chapter includes:

Concepts

Tasks

Reference

Concepts

Personal Settings Overview

Personal settings enable customization of the way HP Business Service Management presents information to individual users.

Individual users can configure personal settings to customize their specific user-related behavior of HP Business Service Management.

The Personal Settings tab contains the following options:

- **General Settings.** For details, see "User Account" on page 380.
- **Menu Customization.** For details, see "Menu Customization" on page 381.

User Account

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 user interface for changing your password and updating other Personal Settings, see "User Account Page" on page 388.

Menu Customization

On the Menu Customization tab, you can:

- Specify the default context that is displayed when logging into HP Business Service Management.
- Specify the first page that is displayed in each of the different parts of HP Business Service Management.
- Specify the tabs and options that are available on pages throughout HP Business Service Management.

Customizing your entry page, menu items, and tabs enables your interface to display only the areas of HP Business Service Management that are relevant to you. For details on the Menu Customization User Interface, see "Menu Customization Page" on page 390.

Tasks

How to Customize Your BSM Menus and Pages - Workflow

This task describes how to customize the page you see when entering HP Business Service Management, and choose the menu items available on pages throughout HP Business Service Management.

Tip: For a use-case scenario related to this task, see "How to Customize Your BSM Menus and Pages - Use-Case Scenario" on page 384.

This task includes the following steps:

- "Assign a Default Context" on page 382
- "Select Context Pages and Tabs" on page 382
- "Assign a Default Entry Page" on page 383
- "Results" on page 383

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 Service Management, and click **Set as Default Entry Context**. For user interface details, see "Menu Customization Page" on page 390.

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.

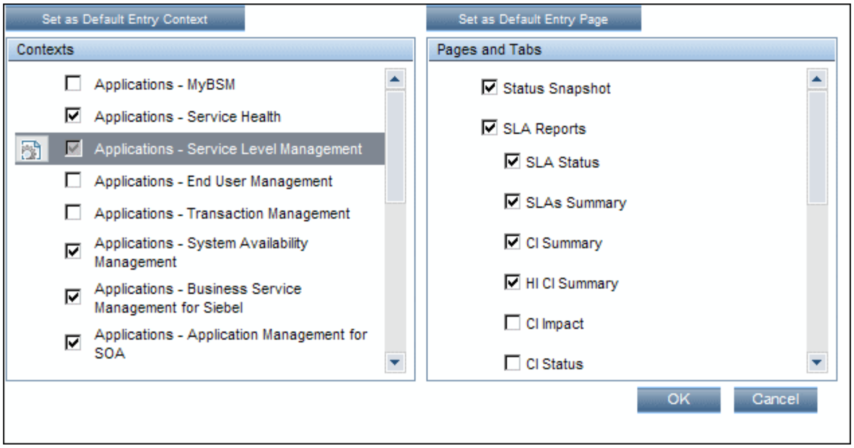
3 Assign a Default Entry Page

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:



Contexts

- ☐ Applications - MyBSM
- ☑ Applications - Service Health
- ☑ Applications - Service Level Management
- ☐ Applications - End User Management
- ☐ Applications - Transaction Management
- ☑ Applications - System Availability Management
- ☑ Applications - Business Service Management for Siebel
- ☑ Applications - Application Management for SOA

Pages and Tabs

- ☑ Status Snapshot
- ☑ SLA Reports
  - ☑ SLA Status
  - ☑ SLAs Summary
  - ☑ CI Summary
  - ☑ HI CI Summary
  - ☐ CI Impact
  - ☐ CI Status

How to Customize Your BSM Menus and Pages - Use-Case Scenario

This use-case scenario describes how to customize user menus for individual users.

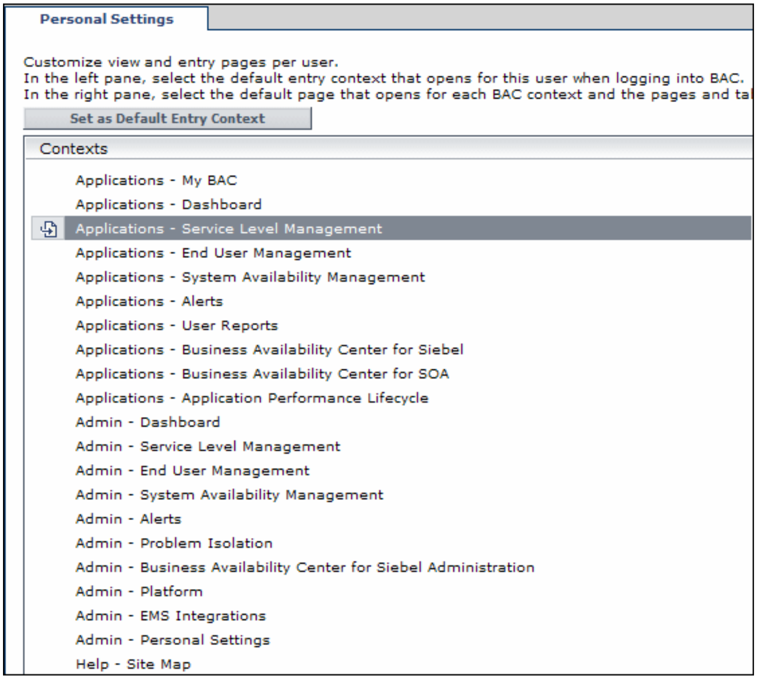
Note: For a task related to this scenario, see "How to Customize Your BSM Menus and Pages - Workflow" on page 382.

This task includes the following steps:

- ➤ "Assigning a Default Context" on page 385
- ➤ "Selecting Context Pages and Tabs" on page 386
- ➤ "Results" on page 387

1 Assigning a Default Context

John Smith is a registered HP Business Service Management user for the ABC Insurance Company. He wants to configure the Service Level Management application interface to be the default Business Service Management context that he sees when logging in. He navigates to the Personal Settings option by selecting **Admin** > **Personal Settings**, and selects **Menu Customization** to open the Menu Customization page. He selects **Applications - Service Level Management** in the Contexts pane and clicks **Set as Default Entry Context**. The Applications - Service Level Management option is indicated as the default entry context:



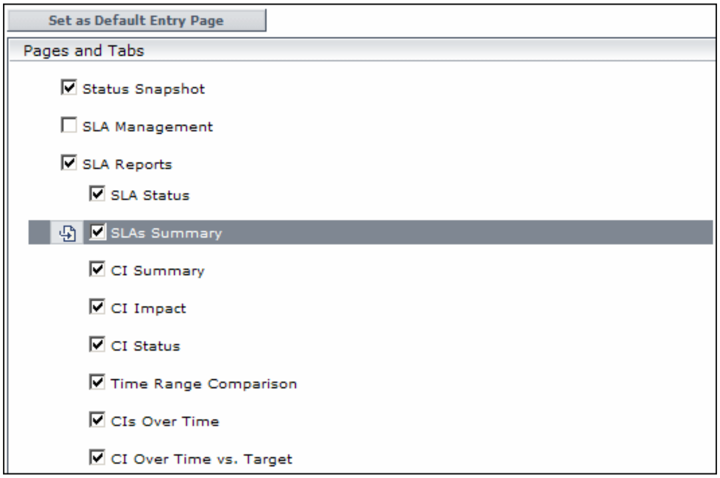
Customize view and entry pages per user.
In the left pane, select the default entry context that opens for this user when logging into BAC.
In the right pane, select the default page that opens for each BAC context and the pages and ta

Contexts

- Applications - My BAC
- Applications - Dashboard
- Applications - Service Level Management
- Applications - End User Management
- Applications - System Availability Management
- Applications - Alerts
- Applications - User Reports
- Applications - Business Availability Center for Siebel
- Applications - Business Availability Center for SOA
- Applications - Application Performance Lifecycle
- Admin - Dashboard
- Admin - Service Level Management
- Admin - End User Management
- Admin - System Availability Management
- Admin - Alerts
- Admin - Problem Isolation
- Admin - Business Availability Center for Siebel Administration
- Admin - Platform
- Admin - EMS Integrations
- Admin - Personal Settings
- Help - Site Map

2 Selecting Context Pages and Tabs

John wants to see only the pages and tabs that are relevant for his work, and wants to view the Service Level Agreements (SLAs) Summary report immediately upon logging in to HP Business Service Management. In the Pages and Tabs pane, he deselects the SLA Management option, as the information presented on this tab is not relevant to his work. He selects the **SLAs Summary** option and clicks **Set as Default Entry Page**. The SLAs Summary page is indicated as the default entry page that John sees when logging in to HP Business Service Management:

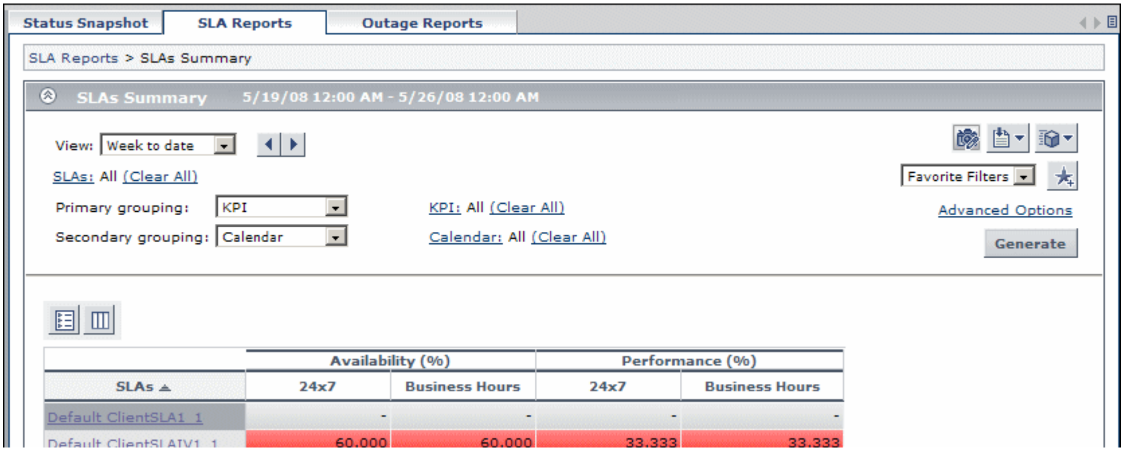


Pages and Tabs

- ☑ Status Snapshot
- ☐ SLA Management
- ☑ SLA Reports
  - ☑ SLA Status
  - ☑ SLAs Summary
  - ☑ CI Summary
  - ☑ CI Impact
  - ☑ CI Status
  - ☑ Time Range Comparison
  - ☑ CIs Over Time
  - ☑ CI Over Time vs. Target

3 Results

The context that opens when John Smith logs into HP Business Service Management is the **Service Level Management** context on the Applications menu. The **SLAs Summary Report** page is displayed on the SLA Reports tab:



SLAs Summary 5/19/08 12:00 AM - 5/26/08 12:00 AM

View: Week to date

SLAs: All (Clear All)

Primary grouping: KPI

Secondary grouping: Calendar

KPI: All (Clear All)

Calendar: All (Clear All)

	Availability (%)		Performance (%)	
SLAs ▲	24x7	Business Hours	24x7	Business Hours
Default ClientSLA1_1	-	-	-	-
Default ClientSLAIV1_1	60.000	60.000	33.333	33.333

Reference

Personal Settings User Interface

This section includes:

- User Account Page on page 388
- Menu Customization Page on page 390
- Recipient Tab on page 391

User Account Page

This page enables you to configure the user name, user mode, time zone, password, and refresh rate settings.

To access	Select **Admin** > **Personal Settings** > **User Account** **Note:** The Personal Settings tab can also be accessed by clicking **Change the default page** on the Site Map.
Important information	HP Business Service Management saves these settings per defined user. Any changes you make remain in effect for all future Web sessions for only that user.
See also	"User Account" on page 380

User interface elements are described below:

UI Elements (A-Z)	Description
Confirm Password	Re-enter the password specified in the **Password** field.
Login name	The name used to login to HP Business Service Management. **Note:** You cannot change the entry in this field.

UI Elements (A-Z)	Description
Password	Enter a password to be used when accessing HP Business Service Management.
Select auto-refresh rate	Select the rate at which you want HP Business Service Management 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.
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 Service Management 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. **Note:** For details on user modes, see "KPIs for User Modes" in *Using Service Health*.
User name	The 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

This page enables you to customize the view and entry pages per user. You can specify the default context that is displayed when logging into HP Business Service Management, specify the first page displayed in each of the different parts of HP Business Service Management, and specify the tabs and options available on pages throughout HP Business Service Management.

To access	Select **Admin** > **Personal Settings** > **Menu Customization** **Note:** The Personal Settings tab can also be accessed by clicking **Change the default page** on the Site Map.
Relevant tasks	"How to Customize Your BSM Menus and Pages - Workflow" on page 382
See also	"Personal Settings Overview" on page 380

User interface elements are described below:

UI Elements (A-Z)	Description
Contexts	Select an HP Business Service Management 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 Service Management.
Pages and Tabs	➤ Select the pages and tabs you want to be visible for the HP Business Service Management 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.

UI Elements (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 Service Management. 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.

Recipient Tab

This tab enables you to define recipients, their email, pager, and SMS information, and the template to use to send alert notices to those recipients.

For user interface details, see "New or Edit Recipient Dialog Box" on page 366.

16

Set Up the Authentication Strategies

This chapter includes:

Concepts

Reference

Concepts

Authentication Strategies - Overview

HP Business Service Management authentication is based on a concept of authentication strategies. Each strategy handles authentication against a specific authentication service. Only one authentication service can be configured with HP Business Service Management at any given time.

The default authentication strategy for logging into HP Business Service Management is the HP Business Service Management internal authentication service. You enter your HP Business Service Management user name and password from the login page, and your credentials are stored and verified by the HP Business Service Management database. For a description of the authentication process in HP Business Service Management, see "HP Business Service Management Login Flow" on page 27.

You can choose to configure authentication using the Lightweight Directory Access Protocol (LDAP). HP Business Service Management uses the LDAP server to verify a user's credentials. For details on LDAP, see "LDAP Authentication and Mapping" on page 431.

Authentication strategies are configured in the Authentication Management Wizard. For details on the Authentication Management Wizard, see "Authentication Wizard" on page 400.

Setting Up a Single Sign-On Authentication Strategy

Single Sign-On is a method of access control that enables a user to log in once and gain access to the resources of multiple software systems without being prompted to log in again. The applications inside the configured group of software systems 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 Service Management is Lightweight Single Sign-On (LW-SSO). LW-SSO is embedded in HP Business Service Management and does not require an external machine for authentication. For details on LW-SSO, see "Lightweight Single Sign-On (LW-SSO) Strategy - Overview" on page 418.

If the applications configured outside of HP Business Service Management do not support LW-SSO, or if you want a stronger Single Sign-On implementation, you can configure Identity Management Single Sign-On (IDM-SSO) using the Authentication Management Wizard. When enabled as a Single Sign-On strategy, IDM-SSO also serves as an authenticator. Users authenticated through IDM-SSO can log into HP Business Service Management, provided they fulfill the criteria defined in the **Users Filter** field of the LDAP Vendor Attributes dialog box. For details, see "LDAP Vendor Attributes Dialog Box" on page 411.

All requests to client applications are channeled through the SSO authentication. The supported applications need to know only the name of the authenticated user.

For details on the IDM-SSO authentication strategy, see "Identity Management Single Sign-On (IDM-SSO) - Overview" on page 428.

Setting Up an LDAP Authentication Strategy

The Lightweight Directory Access Protocol (LDAP) is an Internet protocol that email and other programs use to look up information from an external server. LDAP can be configured with HP Business Service Management in one of the following ways:

- As an authentication mechanism for users logging into HP Business Service Management.
- To map groups and synchronize HP Business Service Management users with users configured on the external LDAP server, thereby simplifying the process of managing users for HP Business Service Management administrators. For details, see "How to Map Groups and Synchronize Users" on page 437.

You enable and disable LDAP using the Authentication Management Wizard. For details, see "Authentication Wizard" on page 400.

Reference

Authentication Modes in HP Business Service Management

The following table displays the Authentication Strategy used by HP Business Service Management, as determined by both the Single Sign-On mode and the LDAP mode selected in the Authentication Management Wizard:

Single Sign-On Mode	LDAP Mode	Authenticator
Disabled	Disabled	HP Business Service Management Internal
	Enabled	LDAP
LW-SSO	Disabled	HP Business Service Management Internal
	Enabled	LDAP
IDM-SSO	Disabled	IDM-SSO
	Enabled	IDM-SSO

Authentication Strategy User Interface

This section includes (in alphabetical order):

- Authentication Strategy Page on page 398
- Authentication Wizard on page 400

Authentication Strategy Page

This page displays the current authentication strategy and Single Sign-on configurations for logging into HP Business Service Management.

To access	Select **Admin** > **Platform** > **Users and Permissions** > **Authentication Management**
Important information	Access to the Authentication Management page is dependent on the following permission levels: ➤ **View.** Enables viewing the Authentication Management Page. ➤ **Change.** Enables you to access the Authentication Management Wizard and change configurations. The **Configure** button is enabled. You configure permissions on the Users and Permissions interface. For details, see "How to Assign Permissions" on page 269.
See also	➤ "Authentication Strategies - Overview" on page 394 ➤ "Infrastructure Settings" on page 115

User interface elements are described below:

UI Elements (A-Z)	Description
Configure	Click to open the Authentication Wizard and configure an authentication strategy. For details on the Authentication Wizard, see "Authentication Wizard" on page 400. The parameters are configured for both the **Single Sign-On Configuration** and the **Lightweight Directory Access Protocol Configuration** using the same wizard accessed by clicking the **Configure** button. You can configure both sets of parameters at a time or you can configure them separately.
Lightweight Directory Access Protocol Configuration	The section displays: ➤ **Name.** The name of the **Lightweight Directory Access Protocol** parameter. ➤ **Value.** The value of the **Lightweight Directory Access Protocol** parameter as configured in the wizard.
Single Sign-On Configuration	The section displays: ➤ **Name.** The name of the **Single Sign-On** parameter. ➤ **Value.** The current value of the **Single Sign-On** parameter as configured in the wizard.

User interface elements are described below:

UI Elements (A-Z)	Description
Configure	Click to open the Authentication Wizard and configure an authentication strategy. For details on the Authentication Wizard, see "Authentication Wizard" on page 400.
Name	The name of the Single Sign-On or Lightweight Directory Access Protocol parameter.
Value	The value of the specified Single Sign-On or Lightweight Directory Access Protocol parameter.

Authentication Wizard

This wizard enables you to create an authentication strategy for logging into HP Business Service Management.

To access	Select **Admin** > **Platform** > **Users and Permissions** > **Authentication Management**, and click **Configure**.
Important information	If the User Interface does not respond properly after upgrading your version of HP Business Service Management (for example, the page does not load, or an error message is displayed), clean the java cache by following this procedure on your client PC: **1** Navigate to **Start** > **Control Panel** > **Java.** **2** In the Temporary Internet Files section, click **Settings**. **3** In the Temporary File Settings dialog box, click **Delete Files**.
Wizard map	This wizard contains: Introduction Page > Single Sign-On Page > (SAML2 Configuration Dialog Box) > LDAP General Configuration Page > (LDAP Vendor Attributes Dialog Box) > LDAP Users Synchronization Configuration Page > Summary Page

Introduction Page

This wizard page provides introductory information on the Authentication Wizard.

To access	Select **Admin** > **Platform** > **Users and Permissions** > **Authentication Management**, and click **Configure**.

Important information	General information about this wizard is available here: "Authentication Wizard" on page 400.
Wizard map	The Authentication Wizard contains: **Introduction Page** > Single Sign-On Page > (SAML2 Configuration Dialog Box) > LDAP General Configuration Page > (LDAP Vendor Attributes Dialog Box) > LDAP Users Synchronization Configuration Page > Summary Page

Single Sign-On Page

This wizard page enables you to configure a Single Sign-On strategy. The elements displayed on the Single Sign-On page are determined by the Single Sign-On mode you choose.

Important information	➤ General information about this wizard is available here: "Authentication Wizard" on page 400. ➤ If a value in one of the wizard fields is blank or invalid, an error icon ☒ is displayed on the field's cell. You can view a description of the error in one of the following ways: ➤ Hover over the error icon to display a tooltip with the error message. ➤ Access the log file **<HPBSM>/log/EJBContainer/login.log.**
Wizard map	The Authentication Wizard contains: Introduction Page > **Single Sign-On Page** > (SAML2 Configuration Dialog Box) > LDAP General Configuration Page > (LDAP Vendor Attributes Dialog Box) > LDAP Users Synchronization Configuration Page > Summary Page

User interface elements are described below:

UI Elements (A-Z)	Description
Disabled	Select to disable the Single Sign-On (SSO) authentication strategy.
IdentityManagement	Select to configure the Identity Management Single Sign-On (IDM-SSO) authentication strategy. For details on the elements displayed this page, see below. For details on this topic, see "Identity Management Single Sign-On (IDM-SSO) - Overview" on page 428. **Note:** If you have selected this option, LDAP can be configured only for group mapping and not for authentication.
Lightweight	Select to configure the Lightweight Single Sign-On (LW-SSO) authentication strategy. For details on the elements displayed on this page, see below. For details on this topic, see "Lightweight Single Sign-On (LW-SSO) Strategy - Overview" on page 418.

Identity Management Single Sign-On (IDM-SSO) Configuration

User interface elements are described below:

UI Elements (A-Z)	Description
☒	Indicates that the value in the specified field is empty or invalid. Hover over this icon to view a tooltip describing the error.

UI Elements (A-Z)	Description
Header Name	Enter the header name for the token name passed by the Identity Management Single Sign-On. **Example:** sso_user **Note:** Ens0ure that the Identity Management Single Sign-On strategy is securing HP Business Service Management resources before you enter this information.
Logout URL	Enter an alternate logout URL, to view a page other than the main login page when logging out of HP Business Service Management. **Example:** \<alternativeLogoutURL>.jsp **Note:** This field is optional.

Lightweight Single Sign-On (LW-SSO) Configuration

User interface elements are described below:

UI Elements	Description
☒	Indicates that the value in the specified field is empty or invalid. Hover over this icon to view a tooltip describing the error.
Add	Adds the host/domain to the list of protected hosts/domains.
HP Business Service Management Domain	Enter the relevant HP Business Service Management domain, to be used for token creation. This field is required for multi-domain support and normalized URLs when the domain cannot be parsed automatically, for example when using aliases. **Example:** devlab.ad
Token Creation Key (initString)	Enter an initString value, used for encryption and decryption of the LW-SSO token. If changing this value, remember to set initString to the same value in all HP products participating in LW-SSO integration. **Example:** Xy6stqZ

UI Elements	Description
Parse automatically	Click to parse the HP Business Service Management domain automatically.
Trusted Hosts/Domains	Displays the list of trusted hosts and domains that are participating in a LW-SSO integration. List of trusted hosts can contain DNS domain name (myDomain.com), NetBIOS name (myServer), IP address, or fully qualified domain name for the specific server (myServer.myDomain). To add a host or domain to the list of trusted hosts/domains, click the **Add** icon ✳, enter the name of the host or domain in the text box under **Trusted Hosts/Domains**, and select the type of host or domain name from the **Type** drop-down box. **Examples:** mercury.global, emea.hpqcorp.net, devlab.ad To remove a host or domain from the list of trusted hosts/domains, select it and click the **Remove** icon ❌.
Enable SAML2 authentication schema	Select to enable authentication using the Security Assertion Markup Language 2.0 protocol.
SAML2 Settings	Click to set parameters in the SAML2 Configuration Dialog Box.

SAML2 Configuration Dialog Box

This dialog box page enables you to modify the SAML authentication parameters for your Lightweight Single Sign-On configuration.

To access	In the Authentication Management Wizard, navigate to the Single Sign-On page, select **Lightweight**, and select the **Enable SAML2 authentication schema** check box. Click **SAML Settings** to open the SAML Configuration dialog box. The SAML Configuration dialog box consists of the following sections: ➤ **SAML2 Creation.** Modify the SAML2 Authentication parameters for sending SAML authentication requests from HP Business Service Management. ➤ **SAML2 Validation.** Modify the SAML2 Authetication parameters for decrypting SAML requests received by HP Business Service Management.
Important information	➤ General information about this wizard is available here: "Authentication Wizard" on page 400. ➤ HP Business Service Management comes with SAML enabled by default. If you want to disable SAML authentication, clear the **Enable SAML2 authentication schema** checkbox.
Wizard map	The Authentication Wizard contains: Introduction Page > Single Sign-On Page > (**SAML2 Configuration Dialog Box**) > LDAP General Configuration Page > (LDAP Vendor Attributes Dialog Box) > LDAP Users Synchronization Configuration Page > Summary Page

User interface elements are described below:

UI Elements	Description
Restore	Restores the SAML2 configuration attributes to their state upon logging into the current session of HP Business Service Management.

SAML2 Creation Section

User interface elements are described below:

UI Elements (A-Z)	Description
Look for keystore in classpath	Select for the Lightweight Single Sign-On framework to search for the keystore in the classpath. **Note:** When this option is selected, you enter only the name of the actual keystore file in the **Keystore filename** field.
Keystore filename	The filename of the keystore in HP Business Service Management. ➤ When **Look for keystore in classpath** is not selected, this value must be the full path of the keystore's location, for example: C:\mystore\java.keystore. ➤ When **Look for keystore in classpath** is selected, this value must be just the file name of the keystore, for example: java.keystore.
Keystore password	The password which enables access to the keystore containing the private key used for encryption during the SAML authentication request.
Private key alias	Indicates the alias of the private key used for encryption during the SAML authentication request.
Private key password	Indicates the password of the private key used for encryption during the SAML authentication request.

SAML2 Validation Section

User interface elements are described below:

UI Elements (A-Z)	Description
Look for keystore in classpath	Select for the Lightweight Single Sign-on framework to search for the keystore in the classpath. **Note:** When this option is selected, you enter only the name of the actual keystore file in the **Keystore filename** field.
Keystore filename	The filename of the keystore in HP Business Service Management. ➤ When **Look for keystore in classpath** is not selected, this value must be the full path of the keystore's location, for example: C:\mystore\java.keystore. ➤ When **Look for keystore in classpath** is selected, this value must be just the file name of the keystore, for example: java.keystore.
Keystore password	The password of the public key used for decryption during the SAML authentication request.

LDAP General Configuration Page

This wizard page enables you to use an external LDAP server to store authentication information (user names and passwords) and to enable user synchronization between LDAP users and HP Business Service Management users.

To access	Select **Admin** > **Platform** > **Users and Permissions** > **Authentication Management**, and click **Configure**. Navigate to the **LDAP General Configuration** page. The available LDAP modes are: ➤ **Enabled** ➤ **Disabled** **Note:** LDAP cannot be used for authentication when you choose **IdentityManagement** on the Single Sign-On Configuration page of the wizard.
Important information	➤ General information about this wizard is available here: "Authentication Wizard" on page 400. ➤ When configuring LDAP parameters, consult your LDAP Administrator for assistance.
Wizard map	The Authentication Wizard contains: Introduction Page > Single Sign-On Page > (SAML2 Configuration Dialog Box) > **LDAP General Configuration Page** > LDAP Users Synchronization Configuration Page > Summary Page

LDAP General Configuration Section

User interface elements are described below:

UI Elements (A-Z)	Description
☒	Indicates that the value in the specified field is empty or invalid. You can view a description of the error in one of the following ways: ➤ Hover over the error icon to display a tooltip with the error message. ➤ Access the log file <**HPBSM root directory**>**\log\EJBContainer\login.log.**
Advanced	Opens the LDAP Vendor Attributes dialog box enabling you to modify configurations for the selected LDAP vendor. For details, see "LDAP Vendor Attributes Dialog Box" on page 411.
Distinguished Name (DN) Resolution	Select to enable entering only the Unique User ID, instead of the full Distinguished Name (DN) when logging in. **Note:** ➤ Selecting this checkbox enables the various Distinguished Name (DN) Resolution elements. ➤ If you do not select this checkbox, you must use the full Distinguished Name (DN) to login to HP Business Service Management.
Distinguished Name of Search-Entitled User	Defines the Distinguished Name (DN) of a user with search privileges on the LDAP directory server. **Note:** Leave this entry blank for an anonymous user.

UI Elements (A-Z)	Description
LDAP server URL	Enter the URL of the LDAP server. The required format is: **ldap://machine_name:port/[??scope]** **Example:** ldap://my.ldap.server:389/ou=People,o=myOrg.com??sub ➤ Possible values of scope = **sub**, **one**, or **base**, and are case sensitive. ➤ Business Service Management ignores the attribute between the two question marks, if one exists. ➤ When the port number and scope value are empty, default values are used. ➤ **Default port number for regular communication:** 389 ➤ **Default port number for SSL communication:** 636 ➤ **Default scope vaule:** sub
LDAP vendor type	Enter the LDAP vendor you are using. Select from: ➤ Common LDAP ➤ Microsoft Active Directory ➤ Other **Note:** If you click **Advanced** and modify the LDAP Vendor Attribute settings, the value of this field automatically changes to **Other**.
Password of Search Entitled User	Defines the password of the user entitled to search the LDAP server entities for groups. **Note:** Leave this entry blank for an anonymous user.

Test DN Resolution Section

Enables you to verify that both the configured LDAP parameters and the credentials of a specified user are valid.

User interface elements are described below:

UI Elements (A-Z)	Description
Password	The password of the user whose credentials are entered in the **UUID** field. **Note:** This field is optional. If left empty, anonymous user is used.
Test	Tests the LDAP configuration and user credentials validity. A message is displayed indicating whether or not the validation was successful.
UUID	The actual login name (Unique User ID) of the LDAP user you want to verify.

LDAP Vendor Attributes Dialog Box

This dailog box page enables you modify the default LDAP settings that are specific to the selected vendor.

To access	Click **Advanced** on the **LDAP General Configuration Page** of the Authentication Management Wizard.
Important information	➤ General information about this wizard is available here: "Authentication Wizard" on page 400. ➤ If you modify the LDAP Vendor Attribute settings, the value of the **LDAP Vendor Type** field on the LDAP General Configuration page automatically changes to **Other**.
Wizard map	The Authentication Wizard contains: Introduction Page > Single Sign-On Page > (SAML2 Configuration Dialog Box) > LDAP General Configuration Page > (**LDAP Vendor Attributes Dialog Box**) > LDAP Users Synchronization Configuration Page > Summary Page

User interface elements are described below:

UI Elements (A-Z)	Description
Group class object	Defines which LDAP entities are to be considered groups on the LDAP server.
Groups member attribute	Defines the specific attribute that determines which of the LDAP group's entities are to be considered members of the LDAP group.
Restore Current	Restores the LDAP vendor attributes to their state upon logging into the current session of HP Business Service Management.
Users filter	Defines which LDAP users are enabled to log into HP Business Service Management.
Users object class	Defines which LDAP entities are to be considered users on the LDAP server.
Users unique ID attribute	The attribute you want to login to HP Business Service Management with, as it appears on the LDAP server. **Example:** uid, mail

LDAP Users Synchronization Configuration Page

This wizard page enables you configure the LDAP server to synchronize LDAP users with HP Business Service Management users.

To access	Select **Admin** > **Platform** > **Users and Permissions** > **Authentication Strategy**, and click **Configure**. Navigate to the **LDAP Users Synchronization Configuration** page.

Important information	➤ General information about this wizard is available here: "Authentication Wizard" on page 400. ➤ This page is enabled only if the LDAP General Configuration page has been configured correctly.
Wizard map	The Authentication Wizard contains: Introduction Page > Single Sign-On Page > (SAML2 Configuration Dialog Box) > LDAP General Configuration Page > (LDAP Vendor Attributes Dialog Box) > **LDAP Users Synchronization Configuration Page** > Summary Page

User interface elements are described below:

UI Elements (A-Z)	Description
☒	Indicates that the value entered in the specified field is invalid.
Enable User Synchronization	Select to enable User Synchronization upon logging into HP Business Service Management, to synchronize LDAP users with HP Business Service Management users. **Important:** Ensure that you have mapped LDAP groups to HP Business Service Management groups before selecting this checkbox. If you have not performed Group Mapping, all users are nested under the Root group and are assigned Viewer permissions. For details on mapping groups, see "How to Map Groups and Synchronize Users" on page 437.
Groups base DN	The Distinguished Name (DN) of the LDAP entity from which you want to start your groups search.
Groups search filter	Enter the relevant parameters to indicate which attributes are to be included in the groups search.
Root groups base DN	The Distinguished Name (DN) of the LDAP groups that are to be first on the hierarchical tree of mapped groups. This value must be a subset of the Groups base DN.

UI Elements (A-Z)	**Description**
Root groups filter	Enter the parameters to determine which LDAP entities are to be the hierarchical base for the LDAP groups. The specified entities are then available to be mapped to groups in HP Business Service Management.
Test	Verifies that the parameters entered to define the LDAP groups structure are valid.
Test Groups Configuration Pane	Displays the groups available for mapping with HP Business Service Management groups and the LDAP groups' hierarchical structure. The displayed groups are determined by the parameters entered into the fields on the LDAP Users Synchronization Configuration page.

Summary Page

This wizard page displays a summary of the authentication strategies configured in the Authentication Management Wizard.

To access	Select **Admin** > **Platform** > **Users and Permissions** > **Authentication Management**, and click **Configure**. Enter information in the Single Sign-On and LDAP pages, and navigate to the **Summary** page.
Important information	General information about this wizard is available here: "Authentication Wizard" on page 400.
Wizard map	The Authentication Wizard contains: Introduction Page > Single Sign-On Page > (SAML2 Configuration Dialog Box) > LDAP General Configuration Page > (LDAP Vendor Attributes Dialog Box) > LDAP Users Synchronization Configuration Page > **Summary Page**

User interface elements are described below:

UI Elements (A-Z)	Description
LDAP General Configuration	Displays the LDAP General Configuration parameters, as configured on the LDAP General Configuration page of the wizard.
LDAP Users Synchronization Configuration	Displays the LDAP Users Synchronization Configuration parameters, as configured on the LDAP Users Synchronization Configuration page of the wizard.
Single Sign-On Configuration	Displays the Single Sign-On parameters, as configured in the wizard.

17

Lightweight Single Sign-On Strategy

This chapter includes:

Concepts

Tasks

Reference

Concepts

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

The default single sign-on authentication strategy for HP Business Service Management is Lightweight Single Sign-On (LW-SSO). LW-SSO is embedded in HP Business Service Management and does not require an external machine for authentication. HP Business Service Management currently uses version 2.2 of LW-SSO.

For an overview of Single Sign-On strategies, see "Setting Up a Single Sign-On Authentication Strategy" on page 395.

You configure LW-SSO in HP Business Service Management using the Authentication Wizard. For details on the Authentication Wizard, see "Authentication Wizard" on page 400.

LW-SSO can be configured via the JMX console to accept client-side authentication certificates. Once a certificate is recognized, LW-SSO creates the token to be used by other applications. For details, see “How to Configure LW-SSO to Work with Client-Side Authentication Certificates” on page 422.

For details on limitations of working with LW-SSO, see "LW-SSO Authentication – General Reference" on page 445.

Note: Demonstration mode enables LW-SSO to be used between applications that are not in the same domain and without having to use the FQDN. This option should be used for demonstration and testing purposes only. Cookies can be passed to machines and applications that are not in the same domain, making this mode unsecure. This option is not supported for use in product environments. You can enable this option using the JMX console. For details, see "How to Modify LW-SSO Parameters Using the JMX Console" on page 421.

Tasks

How to Configure Unknown User Handling Mode

This task describes how to handle unknown users trying to login to HP Business Service Management -- users that were authenticated by the hosting application but do not exist in the HP Business Service Management users repository:

To configure unknown user handling mode:

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 - Lightweight (LW-SSO) field, and select one of the following options:

- **Integration User.** A user with the User name **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 Service Management 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 Service Management, and is directed to the login page.

The changes take effect immediately.

Note: When User Synchronization is enabled between HP Business Service Management and the LDAP server, unknown users are always denied entry into HP Business Service Management.

How to Modify LW-SSO Parameters Using the JMX Console

This task describes how to modify options and parameters used with LW-SSO in the JMX console. These options include the ability to enable demonstration mode (beginning with LW-SSO version 2.2).

You can also use the JMX console if you are locked out of HP Business Service Management and must change SSO parameters to gain access.

To modify 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.

Note: To enable demonstration mode, change the property **LwSsoFrameworkDemoMode** from its default value of **False** to **True**.

The changes take effect immediately.

How to Configure LW-SSO to Work with Client-Side Authentication Certificates

This task describes how to configure the Lightweight Single Sign-On authentication strategy to accept client-side authentication certificates, using the JMX console.

To configure LW-SSO to work with client-side authentication certificates:

1 Enter the URL of the JMX console (**http://<Gateway or Data Processing 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:

- Domain name: **Topaz**
- Service: **LW-SSO Configuration**

4 To enable client-side authentication, set the attribute **ClientCertificateInboundHandlerEnabled** to **true**.

Note: It is strongly recommended to enable client-side authentication only when this is required, and otherwise to explicitly set the value to **false**.

5 To define the field that contains the User Identifier, locate the attribute **ClientCertificateUserIdentifierRetrieveField**, and enter the name of the authentication certificate field in which the User Identifier is located, for example **SubjectDN** or **SubjectAlternativeName**.

6 To define how to retrieve the User Identifier from the field, locate the attribute **ClientCertificateUserIdentifierRetrieveMode**, and enter the appropriate User Identifier retrieve mode -- either **EntireField** or **FieldPart**.

7 To define the part of the User Identifier Retrieve field that contains the User Identifier, locate the attribute attribute **ClientCertificateUserIdentifierRetrieveFieldPart**, and enter the name of the part of the User Identifier Retrieve field in which the User Identifier is located, for example **EMAILADDRESS**.

Note: If userIdentifierRetrieveMode is set as **FieldPart**, or if userIdentifierRetrieveField is set as **SubjectAlternativeName**, the attribute ClientCertificateUserIdentifierRetrieveFieldPart must be specified. Otherwise, it may be left empty.

---

8 Click **Apply Changes**.

Reference

Troubleshooting and Limitations

This section describes troubleshooting and limitations for Lightweight Single Sign-On.

This section includes:

- "Unable to Access HP Business Service Management Due to Changes in LW-SSO Parameters" on page 424
- "Synchronizing Users When Using LW-SSO" on page 425

Unable to Access HP Business Service Management Due to Changes in LW-SSO Parameters

If you are locked out of HP Business Service Management, you can update selected Lightweight Single Sign-On (LW-SSO) parameters remotely using the JMX console on the application server that is embedded in HP Business Service Management.

For details on how to change LW-SSO parameters outside the HP Business Service Management interface, see "How to Modify LW-SSO Parameters Using the JMX Console" on page 421.

Synchronizing Users When Using LW-SSO

LW-SSO does not ensure user synchronization between integrated applications. Therefore, you must enable LDAP and configure group mapping for the integrated application to monitor users. Failure to map groups and synchronize users may cause security breaches and negative application behavior. For details on mapping users between applications, see "How to Map Groups and Synchronize Users" on page 437.

18

Identity Management Single Sign-On Authentication

This chapter includes:

Concepts

Reference

Concepts

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

You implement IDM-SSO if you want a more secure connection than that offered by LW-SSO, or if the applications configured outside of HP Business Service Management do not support LW-SSO. The IDM server is monitored by a single center Policy Server, and consists of a User Repository, 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. For details, see your IDM vendor's documentation.

HP Business Service Management requires the IDM vendor to store user information to render it available as a header on http requests. You configure both the Header name and the IDM-SSO strategy in the Authentication Wizard. For details, see "Authentication Wizard" on page 400.

Reference

Securing BSM Resources Under IDM-SSO

The following HP Business Service Management resources should be secured when using IDM-SSO as a Single Sign-On strategy:

Resource	Authentication Scheme
/ext/*	basic
/filters/*	form
/hpbsm/*	form
/mam/*	basic
/mam-collectors/*	basic
/mam-images/*	form
/mcrs/*	form
/MercuryAM/*	form
/odb/*	form
/opal/*	form
/opr-admin-server/*	form
/opr-console/*	form
/opr-gateway/*	form
/ovpm /*	form
/topaz/*	form
/topaz/rfw/directAccess.do	basic
/topaz/sitescope/*	basic
/topaz/topaz_api/*	basic
/topazSettings/*	form

Resource	Authentication Scheme
/tv/*	form
/tvb/*	form
/ucmdb-ui/*	form
/uim/*	form
/utility_portlets/*	form
/webinfra/*	form

Additionally, the following resources should be unprotected:

- **/topaz/images**
- **/topaz/Imgs/chartTemp**
- **/topaz/js**
- **/topaz/static**
- **/topaz/rfw/static**
- **/topaz/stylesheets**
- **/topaz/services/technical/time**
- **/topaz/Charts**
- **/ucmdb-api**

If you are using a Load Balancer, you should also unprotect the following resources:

- **/topaz/topaz_api/loadBalancerVerify_core.jsp**
- **/topaz/topaz_api/loadBalancerVerify_centers.jsp**

19

LDAP Authentication and Mapping

This chapter includes:

Concepts

Tasks

Reference

Concepts

LDAP Authentication - Overview

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

Authentication is performed by the LDAP server, and authorization is handled by the HP Business Service Management server.

You configure the LDAP server for authentication and user synchronization using the Authentication Wizard. For details on the Authentication Wizard, see "Authentication Wizard" on page 400.

For details on securing communication between an LDAP server and your HP Business Service Management server over SSL, see "Securing Communication Between an LDAP Server and BSM Server Over SSL" in the *HP Business Service Management Hardening Guide* PDF.

Mapping Groups

You map groups to enable user synchronization between LDAP users and HP Business Service Management users. The Group Mapping feature is accessible through the Users and Permissions interface, by clicking the **LDAP Synchronization** button and selecting **Group Mappings**. This button is enabled only if the following conditions are met:

- The **LDAP mode** on the Authentication Strategy page is configured to **Enabled**.
- The user has administrator permissions.

Once user synchronization is enabled, the User Management interface has the following limitations:

- You cannot create a user.
- The User name and Login name fields for individual users are disabled.
- The Password field is invisible.
- You cannot nest users in groups via the Hierarchy tab.

You can optionally map an LDAP group to multiple HP Business Service Management groups, or multiple LDAP groups to an HP Business Service Management group.

When enabling the Group Mapping feature, you can log into HP Business Service Management with any unique user attribute that exists on the LDAP server (for example, an email address). For details, see "How to Modify the Attribute Used to Log into HP Business Service Management" on page 441.

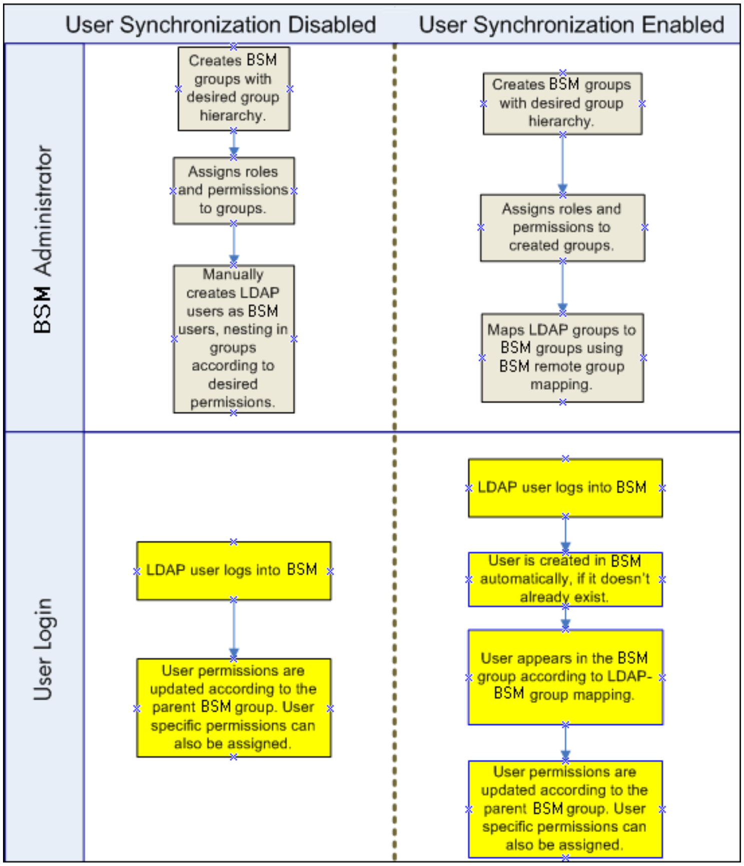
Synchronizing Users

The user synchronization feature maps users on an LDAP server to users in HP Business Service Management. This simplifies the process of managing users for HP Business Service Management administrators, as all of the user management functions are done through the LDAP server. It is recommended to grant permissions on the group level in HP Business Service Management, and then nest users into groups according to their desired permission level. If users are moved between LDAP groups, they are moved between their corresponding mapped groups on the HP Business Service Management server after logging into HP Business Service Management.

An LDAP user that does not exist in HP Business Service Management who logs into HP Business Service Management is created as an HP Business Service Management user. Their status is determined as follows:

- If the user belongs to a mapped LDAP group, they are automatically assigned to the HP Business Service Management group that is mapped to their LDAP group.
- If their group is not mapped to an HP Business Service Management group, or if they do not belong to an LDAP group, they are nested under the **Root** group and created as an HP Business Service Management user with **System Viewer** permissions. Their permissions and user hierarchy can be modified on the User Management interface.

The following flowchart displays the process of User Management when LDAP is enabled, as performed by the HP Business Service Management administrator and HP Business Service Management itself when the user logs in:


User Synchronization Disabled
User Synchronization Enabled
BSM Administrator
User Login
Creates BSM groups with desired group hierarchy.
Assigns roles and permissions to groups.
Manually creates LDAP users as BSM users, nesting in groups according to desired permissions.
Creates BSM groups with desired group hierarchy.
Assigns roles and permissions to created groups.
Maps LDAP groups to BSM groups using BSM remote group mapping.
LDAP user logs into BSM
User permissions are updated according to the parent BSM group. User specific permissions can also be assigned.
LDAP user logs into BSM
User is created in BSM automatically, if it doesn't already exist.
User appears in the BSM group according to LDAP-BSM group mapping.
User permissions are updated according to the parent BSM group. User specific permissions can also be assigned.

For an LDAP user to log into HP Business Service Management, they must match the criteria defined in the **Users filter** field on the LDAP Advanced General Configuration dialog box in the Authentication Wizard. For details on the LDAP General Configuration page, see "LDAP Vendor Attributes Dialog Box" on page 411.

Users that have been removed from the LDAP server are still displayed as HP Business Service Management users, even though they are no longer registered as LDAP users and cannot log into HP Business Service Management. These users are called **Obsolete Users**. For details on removing Obsolete Users from HP Business Service Management, see "How to Delete Obsolete Users" on page 441.

For details on synchronizing LDAP users with HP Business Service Management users, see "How to Map Groups and Synchronize Users" on page 437.

For details on synchronizing groups after upgrading from a previous version of HP Business Service Management, see "Synchronizing Users After Upgrading from a Previous Version of HP Business Service Management" on page 436.

Synchronizing Users After Upgrading from a Previous Version of HP Business Service Management

When upgrading from a previous version of HP Business Service Management, the **Enable User Synchronization** setting in Infrastructure Settings is set to **False** by default. This enables you to map the LDAP groups to groups in HP Business Service Management using the **LDAP Configuration** button on the Users and Permissions interface. If you do not map the groups at this time, all HP Business Service Management groups are nested under the Root directory.

Once the LDAP and HP Business Service Management 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 Service Management.

For details on performing this task, see "How to Synchronize Users After Upgrading from a Previous Version of BSM" on page 440.

Tasks

How to Map Groups and Synchronize Users

This task describes how to map LDAP groups to HP Business Service Management groups, and how to synchronize LDAP users with HP Business Service Management users:

This task includes the following steps:

- "Configure the LDAP Server for Mapping Groups" on page 437
- "Create HP Business Service Management Groups and Hierarchy" on page 437
- "Map LDAP Groups to HP Business Service Management Groups" on page 437
- "Enable User Synchronization" on page 439

1 Configure the LDAP Server for Mapping Groups

You enable the LDAP server for Group Mapping, using the Authentication Wizard. For task details, see "Authentication Wizard" on page 400.

2 Create HP Business Service Management Groups and Hierarchy

You create local groups in HP Business Service Management with the appropriate roles to nest users into, and users adopt the permission level of the group they are nested in. For task details, see "Groups/Users Pane" on page 351.

3 Map LDAP Groups to HP Business Service Management Groups

You map user groups on the LDAP server to groups in HP Business Service Management.

Caution: Administrators must do one of the following, to avoid being locked out of HP Business Service Management when logging out after enabling the LDAP server but before configuring group mapping and user synchronization:

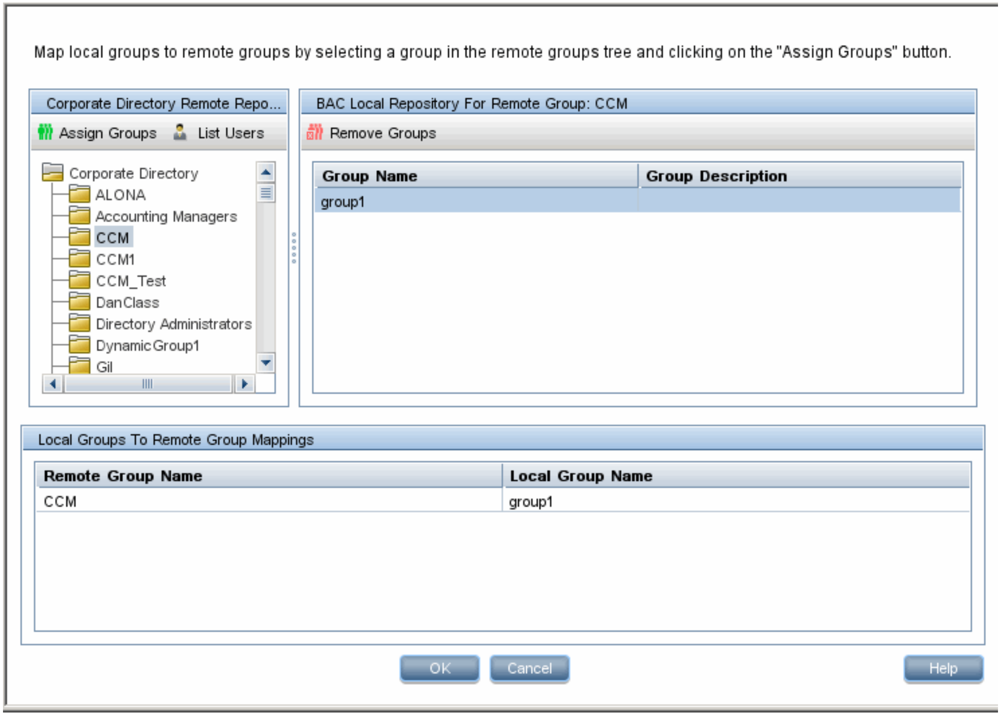
- Ensure that they have mapped their own group, to enable logging into HP Business Service Management after enabling User Synchronization.
- Create an account in HP Business Service Management with superuser permissions.

a On the Users and Permissions interface, navigate to the Groups/Users pane, click the **LDAP Configuration** 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 Service Management groups mapped to the selected LDAP group are displayed in the **BSM Local Repository for Remote Group:** <**group name**> pane.

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



Map local groups to remote groups by selecting a group in the remote groups tree and clicking on the "Assign Groups" button.

Corporate Directory Remote Repo...

BAC Local Repository For Remote Group: CCM

Group Name	Group Description
group1	

Local Groups To Remote Group Mappings

Remote Group Name	Local Group Name
CCM	group1

4 Enable User Synchronization

You enable synchronization of user groups on the LDAP server with user groups in HP Business Service Management by configuring the relevant settings on the LDAP Users Synchronization Configuration page in the Authentication Wizard.

Note:

- Before enabling user synchronization, ensure that you have either created a superuser account in HP Business Service Management that matches your own LDAP user login, or mapped an appropriate LDAP group to an HP Business Service Management group that has the **superuser** role assigned to it. If you have not done so, and log out of HP Business Service Management after enabling LDAP but before group mapping is completed and user synchronization is enabled, the designated HP Business Service Management superuser account will be locked out of HP Business Service Management.
- To disable user synchronization and enable management of users through the User Management interface in HP Business Service Management, clear the **Enable User Synchronization** checkbox on the **LDAP Users Synchronization Configuration** page in the Authentication Wizard.

For details on synchronizing users through the Authentication Wizard, see "LDAP Users Synchronization Configuration Page" on page 412.

How to Modify the Attribute Used to Log into HP Business Service Management

This task describes how to modify the LDAP attribute with which you want to log into HP Business Service Management.

To modify the LDAP attribute with which you want to log into HP Business Service Management:

1. Navigate to **Admin** > **Platform** > **Users and Permissions** > **Authentication Strategy**.
2. Click the **Configure** button to activate the Authentication Strategy Wizard.
3. Navigate to the **LDAP General Configuration** page, and click the **Advanced** button.
4. Modify the **User unique ID** attribute to the attribute you want to log in with, as it appears on the LDAP server.

How to Delete Obsolete Users

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

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

- The **Remote user repository mode** on the Authentication Strategy page is set to **Enabled**.
- The user has **Delete** permissions.

To delete obsolete users:

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

2 Select the user you want to delete.

Reference

Troubleshooting and Limitations

This section describes troubleshooting and limitations for Lightweight Directory Access Protocol (LDAP) Authentication.

- If you have configured HP Business Service Management to use LDAP Authentication and are unable to log into HP Business Service Management, see the HP Software Self-solve knowledge base (http://h20230.www2.hp.com/selfsolve/document/39499). To enter the knowledge base, you must log in with your HP Passport ID.

20

LW-SSO Authentication – General Reference

This chapter includes:

Concepts

Reference

Concepts

LW-SSO Authentication Overview

LW-SSO is a method of access control that enables a user to log on once and gain access to the resources of multiple software systems without being prompted to log on again. The applications inside the configured group of software systems trust the authentication, and there is no need for further authentication when moving from one application to another.

The information in this section applies to LW-SSO version 2.2 and 2.3.

This section includes the following topics:

- “LW-SSO Token Expiration” on page 446
- “Recommended Configuration of the LW-SSO Token Expiration” on page 446
- “GMT Time” on page 447
- “Multi-domain Functionality” on page 447
- “Get SecurityToken for URL Functionality” on page 447

LW-SSO Token Expiration

The LW-SSO Token's expiration value determines the application's session validity. Therefore, its expiration value should be at least the same value as that of the application session expiration value.

Recommended Configuration of the LW-SSO Token Expiration

Each application using LW-SSO should configure token expiration. The recommended value is 60 minutes. For an application that does not require a high level of security, it is possible to configure a value of 300 minutes.

GMT Time

All applications participating in an LW-SSO integration must use the same GMT time with a maximum difference of 15 minutes.

Multi-domain Functionality

Multi-domain functionality requires that all applications participating in LW-SSO integration configure the trustedHosts settings (or the **protectedDomains** settings), if they are required to integrate with applications in different DNS domains. In addition, they must also add the correct domain in the **lwsso** element of the configuration.

Get SecurityToken for URL Functionality

To receive information sent as a **SecurityToken for URL** from other applications, the host application should configure the correct domain in the **lwsso** element of the configuration.

Reference

LW-SSO System Requirements

The following table lists LW-SSO configuration requirements:

Application	Version	Comments
Java	1.5 and higher	
HTTP Sevlets API	2.1 and higher	
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
JBoss Authentications	JBoss 4.0.3 JBoss 4.3.0	
Tomcat Authentications	Standalone Tomcat 5.0.28 Standalone Tomcat 5.5.20	
Acegi Authentications	Acegi 0.9.0 Acegi 1.0.4	
Spring Security Authentication	Spring Security 2.0.4	
Web Services Engines	Axis 1 - 1.4 Axis 2 - 1.2 JAX-WS-RI 2.1.1	

LW-SSO Security Warnings

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

- **Confidential InitString parameter in LW-SSO.** LW-SSO uses Symmetric Encryption to validate and create a LW-SSO 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.

  Caution:

  - It is not possible to use LW-SSO without setting the **initString** parameter.
  - The **initString** parameter is confidential information and should be treated as such in terms of publishing, transporting, and persistency.
  - The **initString** parameter should be shared only between applications integrating with each other using LW-SSO.
  - The **initString** parameter should have a minimum length of 12 characters.

- **Enable LW-SSO only if required.** LW-SSO should be disabled unless it is specifically required.
- **Level of authentication security.** The application that uses the weakest authentication framework and issues a LW-SSO token that is trusted by other integrated applications determines the level of authentication security for all the applications.

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

- **Symmetric encryption implications.** 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** parameter. This potential risk is relevant when an application sharing an initString either resides on, or is accessible from, 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. We recommend 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. For example, the same user name may be assigned to different real users in the various applications.

  In addition, in cases where a user logs onto an application (AppA) and then accesses a second application (AppB) that uses container or application authentication, the failure to map the user will force the user to manually log on to AppB and enter a user name. If the user enters a different user name than was used to log on to AppA, the following behavior can arise: If the user subsequently accesses a third application (AppC) from AppA or AppB, then they will access it using the user names that were used to log on to AppA or AppB respectively.
- **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 file.
- **LW-SSO Demo mode**.
  - The Demo mode should be used for demonstrative purposes only.
  - The Demo mode should be used in unsecured networks only.
  - The Demo mode must not be used in production. Any combination of the Demo mode with the production mode should not be used.

Troubleshooting and Limitations

Known Issues

This section describes known issues for LW-SSO authentication.

- **Security context.** The LW-SSO security context supports only one attribute value per attribute name.

  Therefore, when the SAML2 token sends more than one value for the same attribute name, only one value is accepted by the LW-SSO framework.

  Similarly, if the IdM token is configured to send more than one value for the same attribute name, only one value is accepted by the LW-SSO framework.

- **Multi-domain logout functionality when using Internet Explorer 7**. Multi-domain logout functionality may fail when the browser used is Internet Explorer 7 and the application is invoking more than three consecutive HTTP 302 redirect verbs in the logout procedure.

  In this case, Internet Explorer 7 may mishandle the HTTP 302 redirect response and display an **Internet Explorer cannot display the webpage** error page instead.

  As a workaround, it is recommended to reduce, if possible, the number of application redirect commands in the logout sequence.

Limitations

Note the following limitations when working with LW-SSO authentication:

- **Client access to the application**.

  If a domain is defined in the LW-SSO configuration:

  - The application clients must access the application with a Fully Qualified Domain Name (FQDN) in the login URL, for example, http://myserver.**companydomain**.com/WebApp.
  - LW-SSO cannot support URLs with an IP address, for example, http://192.168.12.13/WebApp.

  - LW-SSO cannot support URLs without a domain, for example, http://myserver/WebApp.

  If a domain is not defined in the LW-SSO configuration: The client can access the application without a FQDN in the login URL. In this case a LW-SSO session cookie is created specifically for a single machine without any domain information. Therefore, the cookie is not delegated by the browser to another, and does not pass to other computers located in the same DNS domain. This means that LW-SSO does not work in the same domain.

- **LW-SSO framework integration.** Applications can leverage and use LW-SSO capabilities only if integrated within the LW-SSO framework in advance.
- **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.
  - 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 in 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 referrer 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 cookie 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 *.mydomain.com) to the Intranet/Trusted zone on your computer (in Microsoft Internet Explorer, select **Menu** > **Tools** > **Internet Options** > **Security** > **Local Intranet** > **Sites** > **Advanced**), which causes the cookies to be accepted.

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

- **SAML2 token.**
  - Logout functionality is not supported when the SAML2 token is used.

    Therefore, if the SAML2 token is used to access a second application, a user who logs out of the first application is not logged out of the second application.

  - The SAML2 token's expiration is not reflected in the application's session management.

    Therefore, if the SAML2 token is used to access a second application, each application's session management is handled independently.

- **JAAS Realm.** The JAAS Realm in Tomcat is not supported.
- **Using spaces in Tomcat directories.** 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.
- **Demo mode**. In Demo mode, LW-SSO supports links from one application to another but does not support typing a URL into a browser window, due to an HTTP referrer header absence in this case.

Part V

Report and Alert Admin

21

Report Schedule Manager

This chapter includes:

Concepts

Reference

Concepts

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, through email, at regularly defined intervals. For details on scheduling User reports, see "How to Create and Manage User Reports Using the Report Manager" in *Reports*.

Reference

Report Schedule Manager User Interface

This section includes:

- Report Schedule Manager Main Page on page 459

Report Schedule Manager Main Page

This page 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 cannot create a new schedule from the Report Schedule Manager main page. For details on creating schedules, see "How to Create and Manage User Reports Using the Report Manager" in *Reports*.
Relevant tasks	"How to Create and Manage User Reports Using the Report Manager" in *Reports*.

User interface elements are described below:

UI Elements (A–Z)	**Description**
✎	Opens the Edit Schedule for the <Report Name> dialog box enabling you to 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 "How to Create and Manage User Reports Using the Report Manager" in *Reports*.
✖	Deletes the selected schedule.
▷	Resumes the selected schedule.
⏸	Pauses the selected schedule.
⟳	Refreshes the Report Schedule Manager page.
☰	Resets the width of the columns to the default setting.
▥	Enables you to select columns to be visible in the table.
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 for which the schedule is configured.

UI Elements (A–Z)	Description
Report Type	The type of report for which the schedule is configured.
Status	The status of the schedule. Possible values are: ➤ Active ➤ Paused

22

Setting Up an Alert Delivery System

This chapter includes:

Concepts

Tasks

Reference

Concepts

Alerts Overview

HP Business Service Management alerts proactively inform you when predefined performance limits are breached, by triggering alerts.

For task details, see "How to Set Up an Alert Delivery System" on page 469.

This section includes the following topics:

- "Alert Recipients" on page 464
- "Notification Template" on page 464
- "Alert Schemes" on page 464
- "Open Events in OM" on page 465
- "Alert History" on page 466
- "Delivery of Alerts" on page 466

Alert Recipients

Alerts can be configured to send notification to specified recipients. For task details on configuring recipients, see "Recipient Management" on page 357.

Notification Template

For each recipient, you can specify the notification method (any combination of email, pager, and/or SMS) and the template to use for alert notices. You can also create a notification schedule for the alerts. For details, see "How to Configure EUM Alerts Notification Templates" on page 488.

Alert Schemes

In each alert scheme, you define a unique set of alert properties. After you create an alert scheme, you view and edit it in the appropriate Alerts user interface. For detailed tips and guidelines, see "Tips for Creating Effective Alert Schemes" on page 468.

You can configure alerts and assign recipients to the alerts for:

- **CIs in a view.** CI Status alerts are triggered by a pre-defined status change for the selected configuration item (CI) detected by the Business Logic Engine. For details, see "CI Status Alerts Administration Overview" in *Using Service Health*.

  HP Service Manager automatically opens incidents when a CI Status alert is triggered in Business Service Management. For details, see "How to Integrate HP Service Manager with Business Service Management Components" in *Solutions and Integrations*.

- **SLAs.** SLA status alerts are triggered by changes to an SLA's key performance indicator status. For details, see "SLA Alerts Overview" in *Using Service Level Management*.
- **EUM alerts.** EUM alerts are triggered when pre-defined conditions, such as transaction response time, availability, success or failure, or completion time, are reached. For details, see "EUM Alerts Administration Overview" in *Using End User Management*.

Open Events in OM

You can automatically open events in OM, when a CI Status alert, an SLA alert, or an EUM alerts alert is triggered in Business Service Management. For details, see "Generating Events in HP Operations Manager when BSM Alert is Triggered Overview" in *Solutions and Integrations*.

Alert History

You can view the history of the alerts in the following:

- **CI Status Alerts Report tab.** Enables you to list all of the CI Status alert triggers that occurred during the specified time range. For details, see "Configuration Item Status Alerts Report" in *Using Service Health*.
- **SLA Alerts Report tab.** Enables you to list all of the Service Level Management alert triggers that occurred during the specified time range. For details, see "Alerts Log Report" in *Using Service Level Management*.
- **EUM Alerts Report tab.** Enables you to access the following reports:
  - **Alert Log report.** Enables you to track all alert details for EUM alerts alerts sent by HP Business Service Management during the specified time range. For details, see "Alerts Log Report" in *Using End User Management*.
  - **Alert Count Over Time report.** Enables you to display an overview of the frequency of alerts. For details, see "Alerts Count Over Time Report" in *Using End User Management*.

Delivery of Alerts

If the online components are experiencing downtime, the Alerts application makes sure that the data is stored in the bus for one hour by default. After the components are back online, the Alerts engine generates alerts from data in the bus.

Alerts and Downtime

When you configure a CI Status alert, downtime can affect the CIs and skew the CI's data.

When you configure an EUM alert scheme for CIs whose status is based on data from Business Process Monitor or SiteScope data sources, downtime can affect the CIs and skew the CI's data.

You may decide to trigger a CI Status alert or an EUM alert during downtime or not. For concept details about downtime, see "Downtime Management - Overview" in *Platform Administration*.

To specify how to handle the CI Status alerts and the EUM alerts during downtime, select **Admin** > **Platform** > **Downtime**, and select one of the following options:

- **Take no action**
- **Suppress events, alerts & notifications (continue monitoring, calculating and displaying data)**
- **Enforce downtime on KPI calculations; suppress events, alerts & notifications (continue monitoring)**
- **Enforce downtime on Reports and KPI calculations; suppress events, alerts & notifications (continue monitoring)**
- **Stop active monitoring (BPM & SiteScope); enforce downtime on Reports & KPI calculations, suppress events, alerts & notifications**

CI Status or EUM alerts for CIs that are in a scheduled downtime are not sent for all the options listed above apart from **Take no action**.

The CI alert is sent even if one of the options listed above is selected (apart from Take no action), if you configured the alert to be triggered when the status of the CI changes to the **Downtime** status. For user interface details, see "General Page" in *Using Service Health*.

For task details, see "How to Set Up an Alert Delivery System" on page 469.

For user interface details, see "Downtime Management Page" in *Platform Administration*.

Tips for Creating Effective Alert Schemes

Before creating alert schemes, you should consider how to most effectively alert users to performance issues. The information described below can assist you with effective alert planning.

Note: HP Professional Services offers best practice consulting on this subject. For information on how to obtain this service, contact your HP representative.

- When creating alert schemes, categorize alerts by severity. Create critical alerts for events that require immediate corrective action (for example, transaction failure, or excessive response times for critical transactions). Create non-critical alerts for events that require early notification (for example, slow response times).
- Determine the users that receive the different types of alerts, and consider the alert delivery method that best suits the alert type. For example, pager delivery as opposed to email delivery might be more effective for critical alerts. When determining the delivery method, take the time of day into account as well. For example, email alerts might not be effective during non-business hours.
- Set HP Business Service Management to alert you to a recurring problem, not one-time events. Recurring alerts are the most accurate indicator of problems with your application. For example, as a rule, you should compare the number of recurring events to the number of Business Process Monitor locations from which you are monitoring. For example, if you had three failures, but you were monitoring from 100 locations, it would not be as critical as if you had five failures in all five locations.

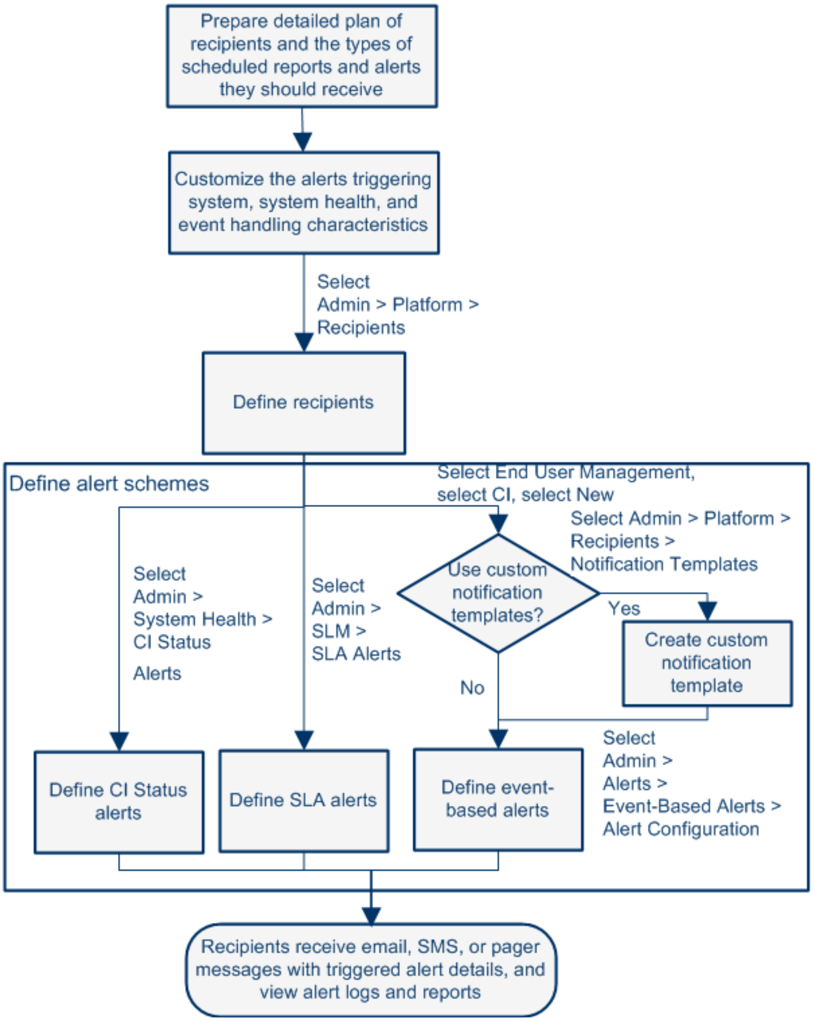
Tasks

How to Set Up an Alert Delivery System

This task and the associated flowchart describe how to set up a system for delivering alerts to recipients.

This task includes the following steps:

- "Plan the alert recipient requirements" on page 471
- "Specify the appropriate user permissions" on page 472
- "Specify how alerts are triggered during downtime" on page 473
- "Customize the alerts triggering system, alerts system health, and event handling characteristics – optional" on page 473
- "Define recipients" on page 473
- "Create custom notification templates – optional" on page 474
- "Set up to open an event in OM when an alert is triggered in BSM" on page 474
- "Result - define the alerts schemes" on page 474


Prepare detailed plan of recipients and the types of scheduled reports and alerts they should receive
Customize the alerts triggering system, system health, and event handling characteristics
Select Admin > Platform > Recipients
Define recipients
Define alert schemes
Select End User Management, select CI, select New
Select Admin > Platform > Recipients > Notification Templates
Select Admin > System Health > CI Status Alerts
Select Admin > SLM > SLA Alerts
Use custom notification templates?
Yes
Create custom notification template
No
Select Admin > Alerts > Event-Based Alerts > Alert Configuration
Define CI Status alerts
Define SLA alerts
Define event-based alerts
Recipients receive email, SMS, or pager messages with triggered alert details, and view alert logs and reports

1 Plan the alert recipient requirements

It is recommended to:

- List the required recipients of alerts, including contact information and required delivery method to the recipient (email, SMS, pager). For suggestions on how to proceed, see "Tips for Creating Effective Alert Schemes" on page 468.
- Map out the types of alerts you plan to deliver. For details on the types of alerts, see "Result - define the alerts schemes" on page 474.

2 Specify the appropriate user permissions

Specify the appropriate user permissions for:

- **The EUM alerts.**
  - You can specify that a user can have a **View** or **Full Control** permission per application. Select **Admin** > **Platform** > **Users and Permissions** > **User Management**, create/edit a user, and click **Permissions**, in the **End User Management** context, select **Business Service Management** > **Applications** > <Application> > **Alerts** context.
  - You must also specify the permission for the CEM event template. Select **Admin** > **Platform** > **Users and Permissions** > **User Management**, create/edit a user, and click **Permissions**, in the **End User Managemen**t context, select **Alert - Notification template**.
- **The CI Status alerts.** You can specify that a user can have a **Change**, **View, Delete,** or **Full Control** permission per view. Select **Admin** > **Platform** > **Users and Permissions** > **User Management**, create/edit a user, and click **Permissions**, in the **ODB** context, select **Business Service Management** > **Views** > <view_name> context.
- **The SLA alerts.** You can specify that a user can have an **Add, Change**, **View, Delete,** or **Full Control** permission per SLA. Select **Admin** > **Platform** > **Users and Permissions** > **User Management**, create/edit a user, and click **Permissions**, in the **Service Level Management** context, select **Business Service Management** > **SLAs** > <sla_name> context.
- **The alert external actions** (**Run executable**, **Send SNMP trap**, or **Log to Event Viewer**). You can specify that a user can have a **Change** or **Full Control** permission at the global level. Select **Admin** > **Platform** > **Users and Permissions** > **User Management**, create/edit a user, and click **Permissions**, in the **Platform** context, select **Business Service Management** > **Run executable**, **Send SNMP trap**, or **Log to Event Viewer** contexts separately.

- **The notification template you can specify for the alerts.** You can specify that a user can have an **Add, Change, View, Delete**, or **Full Control** permission for the template. To do so, select **Admin** > **Platform** > **Users and Permissions** > **User Management**, create/edit a user, and click **Permissions**. In the **End User Management** context, select **Business Service Management** > **System Recipient Template** context. These permissions are defined at the global level.

  For user interface details, see "Operations" in *Platform Administration*.

3 Specify how alerts are triggered during downtime

When you configure a CI Status alert or an EUM alert scheme for CIs whose status is based on data from Business Process Monitor or SiteScope data sources, downtime can affect the CIs and skew the CI's data.

You may decide to trigger a CI Status alert or an EUM alert during downtime or not. To specify how to handle the CI Status alerts and the EUM alerts during downtime, select **Admin** > **Platform** > **Downtime**, and select one of the available options.

For concept details, see "Alerts and Downtime" on page 467.

For user interface details, see "Downtime Management Page" in *Platform Administration*.

4 Customize the alerts triggering system, alerts system health, and event handling characteristics – optional

Customize the alerts triggering system, system health, and event handling characteristics. For more information, see "How to Customize Alerts" on page 475.

5 Define recipients

On the Recipients page, you define system recipients for alerts (except SiteScope alerts). You can specify email, SMS, or pager delivery methods. If required, enter specific alert delivery schedules (for example, recipients who receive alerts during business hours as opposed to evenings and weekends). For more information, see "Recipient Tab (User Management)" on page 341.

6 Create custom notification templates – optional

If required, when defining EUM alerts, you have the option to create custom notification templates that customize the format and information included in alert emails. For more information, see "How to Configure EUM Alerts Notification Templates" on page 488.

7 Set up to open an event in OM when an alert is triggered in BSM

You can set up to open events in OM when an alert is triggered in Business Service Management. For concept details, see "How to Configure BSM Alerts to Forward an Event When the Alert is Triggered" in *Solutions and Integrations*. For task details, see "How to Configure BSM Alerts to Forward an Event When the Alert is Triggered" in *Solutions and Integrations*.

8 Result - define the alerts schemes

You have planned the alert schemes, set up the relevant recipients, customized the alerts general settings and customized the notification templates. You can now define the alert schemes you require:

- **CI Status Alerts.** Define CI Status alerts as required to alert recipients to KPI status changes for specific CIs and KPIs being monitored in Service Health. For more information, For more information, see "How to Create a CI Status Alert Scheme and Attach it to a CI" in *Using Service Health*.
- **SLA Alerts.** Define SLA alerts as required to alert recipients to changes in the current and forecasted status for service agreements. For more information, see "How to Define an SLA Alert Scheme" in *Using Service Level Management*.
- **EUM Alerts.** Define EUM alerts as required to alert recipients to performance variance of Real User Monitor entities or Business Process Monitor transactions. For more information, see "How to Create EUM Alert Schemes" in *Using End User Management*.

How to Customize Alerts

Note: All the steps in the task are optional and can be performed in any order.

This task describes the customization you can perform for CI Status, SLM, and EUM alerts.

- "Modify the way events are handled" on page 475
- "Modify the Alerting System Health parameters" on page 476
- "Modify the alerts triggering defaults" on page 477

Modify the way events are handled

To modify the way events are handled, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**:

- Select **Foundations**.
- Select **Alerting**.
- In the **Alerting - Event handling** table, locate and modify the following parameters:

Purpose	Parameter	Description
Specify the default delay for alerts	**Acceptable event delay (minutes)**	Modify the default delay (60 minutes) after which alerts are discarded.
Enable/disable calculation persistency	**Calculation persistency**	When calculation persistency is enabled, the calculated data, which existed before the system goes down, is taken into consideration in data calculations after the system goes up. Select **false** to disable calculation persistency and **true** to enable calculation persistency.

Modify the Alerting System Health parameters

Note: This is not applicable for BSM 9.00

To modify the way events are handled, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**:

- Select **Foundations**.
- Select **Alerting**.
- In the **Alerting - System Health** table, locate and modify the following parameters:

Purpose	Parameter	Description
Specify when notification queue status changes to error	**Error threshold for the notification queue monitor**	Enter the maximum number of messages waiting in the alert queue of the notification queue monitor after which the notification queue monitor status changes to **error**.
Specify when notification queue status changes to warning	**Warning threshold for the notification queue monitor**	Enter the maximum number of messages waiting in the alert queue of the notification queue monitor after which the notification queue monitor status changes to **warning**.
Specify when alert queue status changes to error	**Error threshold for the alert queue monitor**	Enter the maximum number of messages waiting in the alert queue of the alert queue monitor after which the alert queue monitor status changes to **error**.
Specify when alert queue status changes to warning	**Warning threshold for the alert queue monitor**	Enter the maximum number of messages waiting in the alert queue of the alert queue monitor after which the alert queue monitor status changes to **warning**.

Modify the alerts triggering defaults

To modify the way events are handled, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**:

- Select **Foundations**.
- Select **Alerting**.
- In the **Alerting - Triggered alerts** table, locate and modify the following parameters:
    - **Add year to notification message.** Used to add the year information to notification messages. Select:
        - **true** to add the year to the date in Email notifications.
        - **false** to add the year to the date in Email notifications.
    - **Email sender.** Used to modify the default sender used in emails

      Limitation: The following characters are invalid:
      ‘ ~ ! # $ % ^ * _ - + = { } \ | / ? . ’ <space>
    - **Alerts email sender address.** Used to modify the default sender email address used in emails. Use the parameter to modify the default value (**HP_BSM_Alert_Manager**) that appears in the **From** field when HP Business Service Management sends alerts is set when you install the Data Processing Server.
    - **SMTP server, SMTP server port, and Alternate SMTP server.** Used to modify the primary and alternate SMTP server. Both the primary and alternate SMTP server can be defined as either:
        - **A designated server with a defined port number.** Enter a server name for sending SMTP emails as the value in the **SMTP server** or **Alternate SMTP server** field and enter a port number for the server in the **SMTP server port** or **Alternate SMTP server** field.
        - **Microsoft’s SMTP services.** Enter <SMTPSVC> as the value in the **SMTP server** or **Alternate SMTP server** field.

      Limitation: The following characters are invalid: _ . -

- **Command line execution timeout (seconds).** Modify the default timeout for an action. Use the parameter to modify the default timeout (30 seconds) after which a command line alert action is not executed.
- **Default SNMP Target Address or Default SNMP Port.** Used to modify the default SNMP Trap host address. Modify the default SNMP trap host address, by entering the IP address or server name in the **Default SNMP Target Address** parameter, and the port number in the **Default SNMP Port** parameter.

Note: You can specify only one SNMP target address. The default host address of the SNMP trap appears automatically in the **Enter host destination** box in the Create New/Edit SNMP Trap dialog box. For details, see "Create New/Edit SNMP Trap Dialog Box" in *Using Service Health* or "Create SNMP Trap/Edit SNMP Trap Dialog Box" in *Using Service Level Management*. If, when you create or edit an SNMP trap, you select the default host address and then modify it afterwards in the Infrastructure Settings, the address in all the SNMP trap you created are updated to the new default. Any alert that is sent causes the SNMP trap to be sent to the new default address.

Note to HP Software-as-a-Service customers: You can set the default host address per customer by selecting a customer when you log in. The updated host address is defined only for the specific customer. You can also define a global host address.

- **Enable alert timer reset.** Used to reset the notification frequency timer. Select:
  - **false.** (Default) An alert is triggered by a specific condition, then the condition that triggered the alert does not exist any more. If the condition that triggered the alert occurs again before the end of time period specified in the **Acceptable events delay** parameter ends, the alert is not sent.
  - **true.** An alert is triggered by a specific condition, then the condition that triggered the alert does not exist any more. If the condition that triggered the alert occurs again before the end of time period specified in the **Acceptable events delay** parameter ends, the alert is sent because the trigger condition has reset the notification frequency timer.
- **Enable cross profile alert dependencies.** Use to enable alert dependencies between profiles. Select:
  - **false.** (Default) Alert dependencies are not allowed between profiles.
  - **true.** Alert dependencies are allowed between profiles.
- **Enable logging to DB.** Enable logging alerts and notifications in the Profile database. This customization is available only for EUM alerts. Select:
  - **true.** (Default) Alerts and notifications are logged in the Profile database.
  - **false.** Alerts and notifications are not logged in the Profile database.
- **Enable notifications and actions.** Enable the alert engine to perform actions and send notifications. This customization is available only for EUM alerts. Select:
  - **true**. (Default) Actions are performed and notifications are sent by the alert engine.
  - **false.** Actions are not performed and notifications are not sent to the user.

- **Notification execution retries.** Use to specify the number of retries of a notification. This customization is available only for EUM alerts. By default, a notification is sent once. Change the default using the **Notification execution retries** parameter. The number of retries that is performed equals the number you specify plus one.
- **Email alerts charset, SMS alert charset, Pager alert charset.** When an alert is triggered, recipients for the generated alert can be notified by email, SMS, or pager messages. You can select one of the following character sets for emails, SMS, or pager messages separately:
  - **UTF-8.** The default character set.
  - **ISO-2022-JP**.

Note to HP Software-as-a-Service customers: The settings described in this section are per customer.

- **SMTP server socket connection timeout (seconds) (Windows).** Use the parameter to modify the default timeout (60 seconds) after which an SMTP server socket is disconnected.

  Note: This is for Windows operating systems only.

- **SMTP trap max length (bytes).** Use the parameter to modify the default maximum length of an SNMP trap (in bytes).
- **Wait interval between retries (seconds).** Use the parameter to modify the default waiting interval between notification retries.

Reference

Setting Up an Alert Delivery System User Interface

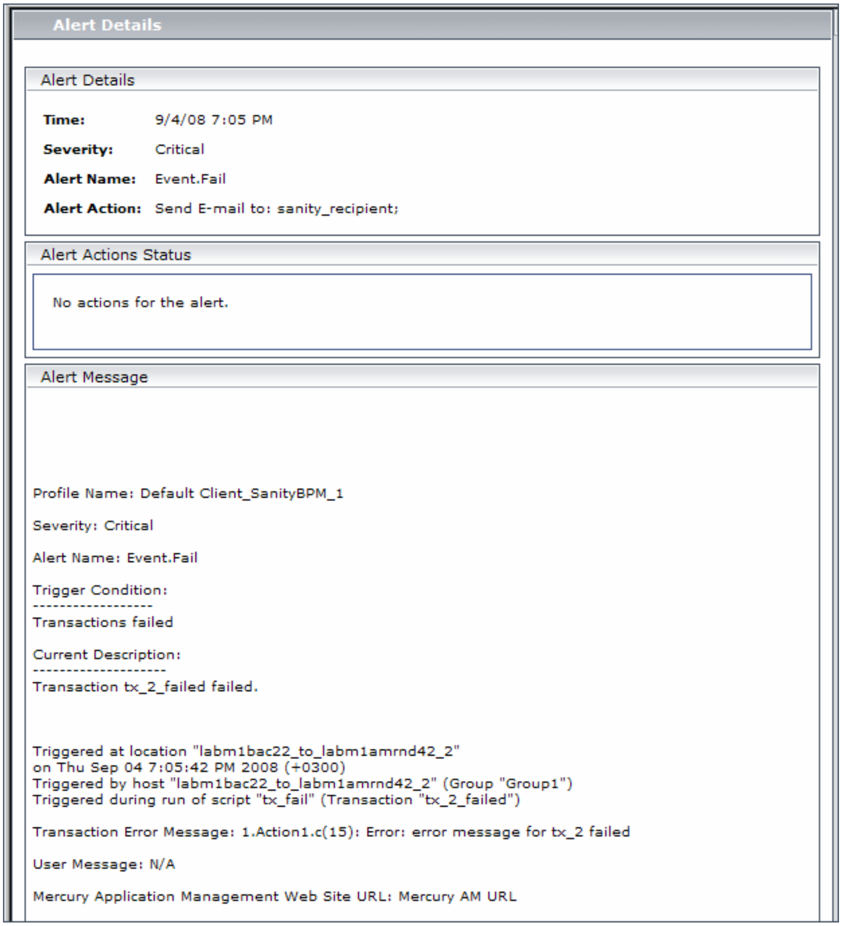
This section includes:

➤ Alert Details Report on page 482

Alert Details Report

This report displays the triggering information that is available for the alert, including the actual conditions at the time of the alert.

The following is an example of the Alert Details report.



Alert Details

Alert Details

Time: 9/4/08 7:05 PM

Severity: Critical

Alert Name: Event.Fail

Alert Action: Send E-mail to: sanity_recipient;

Alert Actions Status

No actions for the alert.

Alert Message

```
Profile Name: Default Client_SanityBPM_1

Severity: Critical

Alert Name: Event.Fail

Trigger Condition:
------------------
Transactions failed

Current Description:
--------------------
Transaction tx_2_failed failed.


Triggered at location "labm1bac22_to_labm1amrnd42_2"
on Thu Sep 04 7:05:42 PM 2008 (+0300)
Triggered by host "labm1bac22_to_labm1amrnd42_2" (Group "Group1")
Triggered during run of script "tx_fail" (Transaction "tx_2_failed")

Transaction Error Message: 1.Action1.c(15): Error: error message for tx_2 failed

User Message: N/A

Mercury Application Management Web Site URL: Mercury AM URL
```

To access	Click 📋 in the Configuration Item Status Alerts page, SLA Status Alerts page, or Alerts Log reports.
Important information	For CI Status Alerts, see details about the Alert Details page in "Configuration Item Status Alert Notifications Report" in *Using Service Health*. For SLA Status Alerts, see details about the Alert Details page in "Alert Details" in *Using Service Level Management*. For EUM alerts, see details about the Alert Details page in "Alert Details" in *Using End User Management*.

23

Configure EUM Alerts Notification Templates

This chapter includes:

Concepts

Tasks

Reference

Concepts

EUM Alerts Notification Templates

To determine the contents and appearance of the EUM alert notices, you can select predefined templates or configure your own template for notifications.

Alerts notification templates specify the information that Business Service Management includes when it sends various types of alert notices. The available default templates are pre-configured with selected parameters for each section of the alert notice. For details on the information included in the default templates, see "Notification Templates Page" on page 497.

You can also create custom templates. For example, you can create different templates for different alert notice delivery methods (email, pager, SMS), or for different recipients. A custom template is defined in the Notification Template Properties page. Each section of the alert notice includes a list of parameters that you can select. For details on the information that can be included in a custom template, see "Notification Templates Page" on page 497.

Note for HP Software-as-a-Service customers: Your list of notification templates includes the default notification templates, the notification templates created for your use by HP Software-as-a-Service representatives and those created by your organization.

Clear Alert Notification Templates

When configuring alert schemes, you can set up an alert scheme to automatically send a clear alert notification. For details on selecting this option while creating your alert scheme, see "How to Create EUM Alert Schemes" on page 522.

The default template for clear alert notifications is automatically used by BSM. If you do not want BSM to use the default template, you can create your own clear alert template. The clear alert template must be based on an existing notification template. BSM uses the clear alert notification template that you create under the following circumstances:

- An alert has been triggered.
- Notification is sent to a recipient based on an existing template (default or user-defined).
- The alert scheme has been configured to send a clear alert.

  For details on configuring a clear alert notification template, see "How to Configure a Template for Clear Alert Notifications" on page 489.

Tasks

How to Configure EUM Alerts Notification Templates

You can select predefined templates, modify existing templates, or create your own notification templates to determine the contents and appearance of the alert notices. For details on notification templates, see "EUM Alerts Notification Templates" on page 486.

This task includes the following steps:

➤ "Create custom templates" on page 488

➤ "Manage existing templates" on page 488

1 Create custom templates

BSM gives you the flexibility to create different notification templates for the different alert schemes and recipients that are defined for your platform.

Every template is divided into sections. You specify the information that you want to appear in each section. For details, see "Notification Template Properties Dialog Box" on page 490.

2 Manage existing templates

Over time, you may find it necessary to make changes to notification templates that you create, because of organizational changes, changes in notification policies, changes to service level monitoring contracts, and so on. You use the Notification Templates page to edit, clone, and delete notification templates defined in BSM. For details, see "Notification Templates Page" on page 497.

How to Configure a Template for Clear Alert Notifications

You can select predefined clear alert notification templates, modify existing templates, or create your own clear alert notification templates to determine the contents and appearance of the clear alert notices. For details on notification templates, see "Clear Alert Notification Templates" on page 487.

Note: The notification template selected for the recipient has a clear alert template based on the notification template's name. For details on naming a clear alert template, see "Notification Template Properties Dialog Box" on page 490. For details on clear alerts, see "Advanced Settings Tab" in *Using End User Management*.

To create, modify, or manage clear alerts notification templates, see "Notification Templates Page" on page 497.

Reference

EUM Alerts Notification Templates User Interface

This section describes:

- Notification Template Properties Dialog Box on page 490
- Notification Templates Page on page 497

Notification Template Properties Dialog Box

This dialog box enables you to define a new alerts notification template.

To access	➤ To create a new template: in the Notification Templates page, click the **New Template** button. ➤ To edit an existing template: in the Notification Templates page, select an existing template, and click ✎.

Important information	**Clear alert notifications:** To set up a clear alert notification, select the notification template to use as the basis for your clear alert template and clone it. Make you determination based on the notification templates that was selected for users likely to receive a clear alert notification. Change the name of the template by deleting Copy of and adding _FOLLOWUP (all caps, one word). Edit the template details as required. It is recommended that you include in the Subject of a clear alert email, the Header, the Alert Specific Information, or both. **Example:** If you are creating a clear alert template based on the LONG default template, you would call the clear alert template LONG_FOLLOWUP. If the clear alert template is based on a user-defined template called MyTemplate, name the clear alert template MyTemplate_FOLLOWUP. **Default:** The _FOLLOWUP string is the default string recognized by Business Service Management as the template name for a clear alert message. **Customization:** You can customize the _FOLLOWUP string. For details, see "How to Configure a Template for Clear Alert Notifications" on page 489.
Relevant tasks	"How to Configure a Template for Clear Alert Notifications" on page 489

General Information Area

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description
<**Insert**>	Select a parameter to add to the section. Repeat to add as many text parameters as you want from the list. Add free text before or after the text parameters. The text parameters available for this section are: ➤ **Alert Name.** The name of the alert, as defined in the alert scheme. ➤ **Severity.** The severity label assigned to the alert in the alert scheme. ➤ **HP BSM URL.** The URL of the Business Service Management Web site. ➤ **Entity Name.** The name of the CI attached to the alert. ➤ **Entity Type.** The type of the CI attached to the alert. ➤ **Alert User Description.** The description you specified in the alert scheme. ➤ **Actions Result.** A description of the results of the alert actions specified in the alert scheme.
Message format	Select the format for the message: **Text** or **HTML**.
Name	Enter a name for the template. If possible, use a descriptive name that includes information on the type of alert (email, pager, SMS) for which you plan to use the template, or the recipients who receive alerts using this template.
Subject	Specify the information that you want HP Business Service Management to include in the subject of the email, pager message, or SMS message. Use the <**insert list for Subject** / **Header** / **Footer**> to add parameters and free text to create a customized subject. Use as many parameters as you want from the list.

Header Area

Use this area to specify the information that you want to appear at the top of the alert notice. Select parameters from the **<Insert>** list and free text to create a customized header. Use as many parameters as you want from the list.

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description
<**Insert**>	Select a parameter to add to the section. Repeat to add as many text parameters as you want from the list. Add free text before or after the text parameters. The text parameters available for this section are: ➤ **Alert Name.** The name of the alert, as defined in the alert scheme. ➤ **Severity.** The severity label assigned to the alert in the alert scheme. ➤ **HP BSM URL.** The URL of the Business Service Management Web site. ➤ **Entity Name.** The name of the CI attached to the alert. ➤ **Entity Type.** The type of the CI attached to the alert. ➤ **Alert User Description.** The description you specified in the alert scheme. ➤ **Actions Result.** A description of the results of the alert actions specified in the alert scheme.

Alert Specific Information Area

Use this area to add alert information to the notification.

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description
<insert list for Alert Specific Information>	Select a text parameter to add to the section. Repeat to add as many text parameters as you want from the list. ➤ **Trigger Cause.** A description of the alert trigger conditions, as specified in the alert scheme. ➤ **Actual Details.** A description of the actual conditions at the time of the alert.

Transaction Area

Use this area to specify the BMP transaction details relevant only for the BPM alert type.

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description
<Insert>	Select a parameter to add to the section. Repeat to add as many text parameters as you want from the list. Add free text before or after the text parameters. The text parameters available for this section are: ➤ **Data Collector Name.** The name of the data collector running the transaction related to the alert. ➤ **Script Name.** The name of the script containing the transaction related to the alert. ➤ **Transaction Time.** The date and time of the alert. ➤ **Transaction Description.** A description of the transaction, if it has been defined in System Availability Management. ➤ **Transaction Name.** The name of the transaction related to the alert. ➤ **Transaction Error.** The error message generated by the data collector for the transaction, if a transaction error occurred at the time of the alert. ➤ **Location Name.** The location of the data collector running the transaction related to the alert.

Footer Area

Use this area to specify the information that you want to appear at the bottom of the alert notice. Select parameters from the **<Insert>** list and free text to create a customized footer. Use as many parameters as you want from the list.

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description
<Insert>	Select a parameter to add to the section. Repeat to add as many text parameters as you want from the list. Add free text before or after the text parameters. The text parameters available for this section are: ➤ **Alert Name.** The name of the alert, as defined in the alert scheme. ➤ **Severity.** The severity label assigned to the alert in the alert scheme. ➤ **HP BSM URL.** The URL of the Business Service Management Web site. ➤ **Entity Name.** The name of the CI attached to the alert. ➤ **Entity Type.** The type of the CI attached to the alert. ➤ **Alert User Description.** The description you specified in the alert scheme. ➤ **Actions Result.** A description of the results of the alert actions specified in the alert scheme.

Notification Templates Page

This page lists the default templates and any custom template that has been defined. It enables you to manage default and custom templates and to create new templates, or to edit clear alert notification templates.

To access	**Admin** > **Platform** > **Recipients** > **EUM Notification Templates**
Important information	When configuring alert schemes, you can instruct BSM to automatically follow up the alert by sending a clear alert notification. For details on selecting this option while creating your alert scheme, see "How to Configure a Template for Clear Alert Notifications" on page 489. The default template for clear alert notifications is automatically used by BSM. If you do not want to use that default template, you can create your own clear alert template. It is recommended to clone an existing notifications template and then to modify the cloned template. HP Business Service Management uses the clear alert notification template that you create under the following circumstances: ➤ An alert has been triggered. ➤ Notification is sent to a recipient based on an existing template (default or user-defined). ➤ The alert scheme has been configured to send a clear alert. ➤ The notification template (DEFAULT_POSITIVE_FORMAT) selected for the recipient has a clear alert template based on the notification template's name.
Relevant tasks	"How to Configure EUM Alerts Notification Templates" on page 488

User interface elements are described below:

UI Element (A-Z)	Description
⧉	**Click to duplicate notification template.** Clones the selected notification template. The Notification Template Properties dialog box opens where you can edit the cloded notification. For details, see "Notification Template Properties Dialog Box" on page 490.
✎	**Click to modify notification template properties.** Click to edit the selected template. For details, see "Notification Template Properties Dialog Box" on page 490.
☒	**Click to delete notification template.** Delete the selected templates simultaneously. To delete multiple templates simultaneously, select their check boxes, and click the ☒ button located at the bottom of the templates list.
New Template	Click the **New Template** button to open the Notification Template Properties dialog box. For details, see "Notification Template Properties Dialog Box" on page 490.

UI Element (A-Z)	Description
Notification Template Name	Lists the default templates and the custom templates. The default templates are: ➤ **DEFAULT_LOG_FORMAT.** Includes all the elements needed to create a default long format notification for reports. ➤ **DEFAULT_POSITIVE_FORMAT.** Includes all the elements needed to create a default long format notification for positive or clear alerts. For details on clear alerts, see "How to Configure a Template for Clear Alert Notifications" on page 489. ➤ **LONG.** Includes all the elements needed to create a default long format notification. ➤ **SHORT.** Includes all the elements needed to create a default short format notification. **Note:** For details on the parameters displayed in each template, see "Notification Template Properties Dialog Box" on page 490.

Index