

HP Business Service Management

for the Windows and Linux operating systems

Software Version: 9.13

Platform Administration

Document Release Date: May 2012

Software Release Date: May 2012



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

© Copyright 2005 - 2012 Hewlett-Packard Development Company, L.P.

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.

iPod is a trademark of Apple Computer, Inc.

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

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

Welcome to This Guide	15
How This Guide Is Organized	15
Who Should Read This Guide	16
How Do I Find the Information That I Need?	17
Additional Online Resources.....	19
Documentation Updates	20

PART I: ACCESSING AND NAVIGATING HP BUSINESS SERVICE MANAGEMENT

Chapter 1: BSM Administration	23
How to Start and Stop BSM	24
How to View the Status of Processes and Services	25
Start Menu in Windows	27
Chapter 2: Logging Into HP Business Service Management.....	29
Logging In and Out — Overview	30
Logging into BSM with LW-SSO	31
Advanced Login Options.....	32
Linking to a Specific Page.....	32
Using the JMX Console.....	34
BSM Login Flow.....	35
How to Log In and Out	37
How to Use Advanced Login Options.....	38
How to Change the JMX Password	42
How to Create a Keystore Certificate	42
How to Track Login Attempts and Logged In Users	43
Security Notes and Precautions.....	44
Logging Into BSM User Interface	45
Troubleshooting and Limitations	47

Chapter 3: Navigating and Using Business Service Management	53
Navigating BSM	54
User Interface Enhancements	58
How to Customize the Masthead Title and Logo	60
Client Requirements for Viewing BSM	61
Menus and Options.....	63

PART II: SETUP AND MAINTENANCE

Chapter 4: Downloads	71
Downloads Overview	72
How to Download Components.....	73
Downloads User Interface	74
Chapter 5: Licenses	77
License Management Overview	78
Licenses User Interface	79
Troubleshooting and Limitations	82
Chapter 6: Server Deployment	83
Server Deployment Overview.....	84
How to Update Your BSM Licenses, Applications, or Deployment Scope	86
Server Deployment User Interface	89
Troubleshooting and Limitations	93
Chapter 7: Database Administration	95
Database Management — Overview	96
Partitioning and Purging Historical Data from Databases.....	98
Removing Unwanted Data from the Profile Database.....	102
How to Configure a Profile Database on a Microsoft SQL Server	103
How to Configure a User Schema on an Oracle Server.....	104
How to Work with the Purging Manager.....	106
How to Enable the Re-aggregation-Only Option	108
How to Determine the Events Per Minute for Data Arriving in BSM	109
How to Customize Data Marking Utility Configurations.....	110
Database Administration User Interface	111
Troubleshooting and Limitations	123

Chapter 8: Infrastructure Settings	127
Infrastructure Settings Manager — Overview	128
How to Modify Infrastructure Settings Using the Infrastructure Settings Manager.....	130
How to Modify the Ping Time Interval.....	130
How to Modify the Location and Expiration of Temporary Image Files.....	131
Infrastructure Settings User Interface.....	141
Chapter 9: BSM Server Time Synchronization	143
BSM Server Time Synchronization - Overview	144
How to View the BSM Server Time	145
Chapter 10: System Health	147
System Health — Overview	148
System Health Setup Wizard – Overview	150
System Health Displays	151
Understanding the Monitors Table	158
Understanding Service Reassignment	159
Adding Additional Monitors to System Health	161
How to Deploy and Access System Health.....	162
How to Ensure the Health of Your System	171
How to Add Additional Monitors to System Health Using a Template	175
BSM Components.....	178
BSM Processes	179
System Health Monitors.....	181
Component and Monitor Status Indicators.....	249
System Health User Interface	250
Troubleshooting and Limitations	287
Chapter 11: Audit Log	289
Audit Log — Overview	290
How to Use the Audit Log.....	293
How to Customize a Log File for Audit Log.....	294
Audit Log User Interface.....	295

Chapter 12: Working in Non-English Locales	299
Installation and Deployment Issues.....	300
Database Environment Issues	302
Administration Issues	303
Service Health Issues	304
Service Level Management Issues.....	305
Report Issues.....	305
Business Process Monitor Issues.....	305
SiteScope Issues	306
Real User Monitor Issues	306
End User Management Administration Issues.....	307
Data Flow Management Issues.....	307
Multilingual Issues	307
Multilingual User (MLU) Interface Support.....	308
Chapter 13: HP Business Service Management Logs	313
BSM Logs — Overview	314
Log File Locations.....	314
Log Severity Levels	315
Log File Size and Automatic Archiving.....	316
JBoss and Tomcat Logs.....	316
How to Change Log Levels.....	318
Chapter 14: Port Usage	319
How to Change Ports Manually.....	320
Incoming HP Business Service Management Traffic.....	323
Outgoing HP Business Service Management Traffic	325
Local HP Business Service Management Traffic.....	326
Chapter 15: File Backup Recommendations	331
Configuration and Data File Backup.....	332

PART III: DATA ENRICHMENT

Chapter 16: Location Manager	337
Location Manager Overview	338
Populating the Location Manager.....	339
Creating and Working with the XML File	341
How to Populate the Location Manager	344
How to Update Locations Using Mass Upload	345
Location Manager User Interface	348

Chapter 17: Content Packs	363
Content Packs Manager.....	364
How to Create and Manage Content Packs	375
Content Pack Content Types	378
Content Pack Manager Command-Line Interface	381
Content Packs Manager User Interface	386
Troubleshooting and Limitations	403
Chapter 18: Downtime Management	405
Downtime Management — Overview.....	406
How to Create and Manage Downtimes for CIs	409
Downtime REST Service	412
Downtime Management User Interface.....	416
Troubleshooting and Limitations	431

PART IV: USERS, PERMISSIONS, AND RECIPIENTS

Chapter 19: User Management	441
User Management — Overview.....	443
Permissions Overview.....	445
Group and User Hierarchy	451
Customizing User Menus	453
How to Configure Users and Permissions — Workflow	454
How to Configure Users and Permissions — Use-Case Scenario	456
How to Assign Permissions	466
How to Configure Group and User Hierarchy	468
How to Remove Security Officer Status Using the JMX Console	470
How to Customize User Menus.....	471
How to Customize User Menus — Use-Case Scenario	473
How to Add a Custom Pager or SMS Service Provider	477
User Management Roles Applied Across BSM.....	480
User Management Roles Applied to Specific Contexts	519
User Management Operations.....	525
User Management User Interface	553
Chapter 20: Recipient Management	577
Recipient Management Overview	578
How to Configure and Manage Recipients	579
How to Add a Custom Pager or SMS Service Provider	579
Recipient Management User Interface	582

Chapter 21: Personal Settings	599
Personal Settings Overview	600
How to Customize Your BSM Menus and Pages — Workflow	602
How to Customize Your BSM Menus and Pages — Use-Case Scenario.....	604
Personal Settings User Interface	608
Chapter 22: Set Up the Authentication Strategies	613
Authentication Strategies — Overview	614
Setting Up an SSO Authentication Strategy.....	614
Setting Up LDAP Authentication	615
Authentication Modes in BSM	616
Authentication Strategy User Interface	617
Chapter 23: Lightweight Single Sign-On Strategy	635
LW-SSO Strategy — Overview	636
LW-SSO Configuration for Multi-Domain and Nested Domain Installations	636
How to Configure Unknown User Handling Mode.....	638
How to Modify LW-SSO Parameters Using the JMX Console	639
How to Secure User Access to BSM Using Client-Side Authentication Certificates.....	640
How to Secure User Access to BSM Using an External Authentication Point	641
Troubleshooting and Limitations	643
Chapter 24: Identity Management Single Sign-On Authentication	645
IDM-SSO — Overview	646
Securing BSM Resources Under IDM-SSO	647
Troubleshooting and Limitations	649
Chapter 25: LDAP Authentication and Mapping	651
LDAP Authentication — Overview	652
Mapping Groups.....	652
Synchronizing Users.....	654
Achieving Finer Control over Default User Permission Assignments	657
How to Map Groups and Synchronize Users	659
How to Synchronize Users After Upgrading from a Previous Version of BSM.....	662
How to Modify the Attribute Used to Log into BSM	663
How to Delete Obsolete Users	663
Troubleshooting and Limitations	664

Chapter 26: LW-SSO Authentication – General Reference	665
LW-SSO Authentication Overview	666
LW-SSO System Requirements	668
LW-SSO Security Warnings	669
Troubleshooting and Limitations	671

PART V: REPORT AND ALERT ADMIN

Chapter 27: Report Schedule Manager	677
Report Schedule Manager — Overview	678
Report Schedule Manager User Interface	679
Chapter 28: Setting Up an Alert Delivery System	683
Alerts Overview	684
Alerts and Downtime	687
Planning for Effective Alert Schemes	688
How to Set Up an Alert Delivery System.....	689
How to Customize Alerts.....	694
Alert Logs	706
Alert Details Report	708
Troubleshooting and Limitations	709
Chapter 29: Configure EUM Alerts Notification Templates	711
EUM Alerts Notification Templates	712
Clear Alert Notification Templates	713
How to Configure EUM Alerts Notification Templates	714
How to Configure a Template for Clear Alert Notifications.....	715
EUM Alerts Notification Templates User Interface	716

PART VI: TROUBLESHOOTING

Chapter 30: Platform Administration Troubleshooting	729
Troubleshooting and Limitations	729
Index	739

Table of Contents

Welcome to This Guide

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

This chapter includes:

- ▶ How This Guide Is Organized on page 15
- ▶ Who Should Read This Guide on page 16
- ▶ How Do I Find the Information That I Need? on page 17
- ▶ Additional Online Resources on page 19
- ▶ Documentation Updates on page 20

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 BSM 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 BSM 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.

Part VI Troubleshooting

Describes common problems that you may encounter when working in the Platform Administration area of BSM.

Who Should Read This Guide

This guide is intended for the following users of BSM:

- BSM administrators
- BSM platform administrators

Readers of this guide should be knowledgeable about enterprise system administration and highly knowledgeable about BSM.

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 BSM documentation.

You can access the Documentation Library by doing the following:



- In BSM, select **Help > Documentation Library**.
- From a BSM 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 	<p>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.</p> <p>Task steps can be with or without numbering:</p> <ul style="list-style-type: none"> ▶ 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. 	<ul style="list-style-type: none"> ▶ 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.
	<p>Use-case Scenario Tasks. Examples of how to perform a task for a specific situation.</p>	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/hpssoftwaresupport.

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

BSM Administration

This chapter includes:

Tasks

- How to Start and Stop BSM on page 24
- How to View the Status of Processes and Services on page 25

Reference

- Start Menu in Windows on page 27

Tasks

How to Start and Stop BSM

To start or stop BSM in Windows:

Select **Start > Programs > HP Business Service Management > Administration > Enable | Disable Business Service Management**. When enabling a distributed environment, first enable the Data Processing Server and then enable the Gateway Server.

To start or stop BSM in Linux:

```
/opt/HP/BSM/scripts/run_hpbsm start | stop
```

To start, stop, or restart BSM using a daemon script:

```
/etc/init.d/hpbsmd {start| stop | restart}
```

Note: When you stop BSM, the BSM service is not removed from Microsoft's Services window. The BSM service is removed from the Services window only after you uninstall BSM.

How to View the Status of Processes and Services

You can view the status of the processes and services run by the HP Business Service Management service and High Availability Controller on the HP Business Service Management server status HTML page.

To view the status of the processes and services, perform the appropriate procedure:

- Windows: Select **Start > Programs > HP Business Service Management > Administration > HP Business Service Management Status**
- Linux: Run
opt/HP/BSM/AppServer/webapps/myStatus.war/myStatus.html
- From a remote computer: Enter the URL **http://<server-name>:8080/myStatus/myStatus.html** in a web browser.

Limitation: This page is only available remotely once the JBoss application server is up.

If a security warning appears above the HP Software title bar, right-click on it, select **Allow Blocked Content**, and click **Yes** in the dialog box that opens.

The line below the HP Software title bar indicates whether all the HP Business Service Management services are running (Server is READY) or some are down (Server is NOT READY).

To view a list of all the processes and their statuses, click the **Nanny Status** title bar.

To view a list of all the High Availability Controller services and their statuses, click the **HAC Status** title bar.

The screenshot shows the HP Software interface with a green status bar indicating "Server is READY". Below this, there are two expandable sections: "Nanny Status" and "HAC Status".

Nanny Status

ServiceName	ProcessName	Status	ExecutionOrder
domain_manager	DomainManager	STARTED	2
message_broker	MessageBroker	STARTED	4
mercuryAS	MercuryAS	STARTED	6
tmu	TMU	STARTED	10
online_engine	mercury_online_engine	STARTED	16
db_loader	mercury_db_loader	STARTED	18
wde	mercury_wde	STARTED	20
ldap	slapd	STARTED	22
offline_engine	mercury_offline_engine	STARTED	24
email_reports	EmailReportsMdrv	STARTED	26
pmanager	mercury_pm	STARTED	28

HAC Status

Service	Process	Ping	State - [Since] - [Duration]
CDM	mercury_as	10s	RUNNING - [29/Jul/2007 11:25:59] - [1d:1h:4m]
CMDB	mercury_as	10s	RUNNING - [29/Jul/2007 11:17:27] - [1d:1h:13m]
MAMVIEWSYS	mercury_as	10s	RUNNING - [29/Jul/2007 11:18:03] - [1d:1h:12m]
VERTICALS	mercury_as	10s	RUNNING - [29/Jul/2007 11:25:54] - [1d:1h:4m]
MAMPACKAGER	mercury_as	10s	RUNNING - [29/Jul/2007 11:25:37] - [1d:1h:5m]
MAMBASIC	mercury_as	10s	RUNNING - [29/Jul/2007 11:17:43] - [1d:1h:12m]
MAMDISCOVERY	mercury_as	10s	RUNNING - [29/Jul/2007 11:18:03] - [1d:1h:12m]
KPI_ENRICHMENT	mercury_as	10s	RUNNING - [29/Jul/2007 11:25:55] - [1d:1h:4m]
MAMIMPACT	mercury_as	10s	RUNNING - [29/Jul/2007 11:18:03] - [1d:1h:12m]
MAMREPORT	mercury_as	10s	RUNNING - [29/Jul/2007 11:18:03] - [1d:1h:12m]
MAMCONFIG	mercury_as	10s	RUNNING - [29/Jul/2007 11:18:03] - [1d:1h:12m]
EMS_HOST	mercury_as	10s	RUNNING - [29/Jul/2007 11:25:57] - [1d:1h:4m]
NCA	mercury_offline_engine	2s	RUNNING - [29/Jul/2007 11:18:11] - [1d:1h:11m]

Last updated: 14:30:38

Reference

Start Menu in Windows

During the installation of BSM in a Windows environment, a menu for BSM is added to the Start Menu of the machine on which BSM was installed.

To access the BSM menu, select **Start > Programs > HP Business Service Management**. The menu includes the following options:

- "Administration" on page 27
- "Documentation" on page 28
- "Open HP Business Service Management" on page 28

Administration

The Administration menu option includes the following sub-options:

Sub-option	Description
Configure HP Business Service Management	Runs the Setup and Database Configuration utility, which enables you to create and connect to management, RTSM, RTSM history, and application databases/user schemas on Microsoft SQL Server or Oracle Server. For details, see "Server Deployment and Setting Database Parameters" in the <i>HP Business Service Management Deployment Guide</i> PDF.
Disable HP Business Service Management	Stops BSM on the specific machine, and disables it from being run automatically when the machine is started.

Sub-option	Description
Enable HP Business Service Management	Starts BSM on the specific machine, and sets it to be run automatically whenever the machine is started.
HP Business Service Management Server Status	Enables you to view the status of the processes and services run by the BSM service and High Availability Controller. For details on this HTML page, see "How to View the Status of Processes and Services".

Documentation

The Documentation menu option, available on the Gateway Server only, includes the following sub-options:

Sub-option	Description
HP Business Service Management Documentation Library	Opens the BSM Documentation Library home page in your Web browser.
HP Business Service Management Deployment Guide	Opens the <i>HP Business Service Management Deployment Guide</i> PDF.

Open HP Business Service Management

Selecting this option opens the BSM application login page in a Web browser.

2

Logging Into HP Business Service Management

This chapter includes:

Concepts

- ▶ Logging In and Out — Overview on page 30
- ▶ Logging into BSM with LW-SSO on page 31
- ▶ Advanced Login Options on page 32
- ▶ Linking to a Specific Page on page 32
- ▶ Using the JMX Console on page 34
- ▶ BSM Login Flow on page 35

Tasks

- ▶ How to Log In and Out on page 37
- ▶ How to Use Advanced Login Options on page 38
- ▶ How to Change the JMX Password on page 42
- ▶ How to Create a Keystore Certificate on page 42
- ▶ How to Track Login Attempts and Logged In Users on page 43

Reference

- ▶ Security Notes and Precautions on page 44
- ▶ Logging Into BSM User Interface on page 45

Troubleshooting and Limitations on page 47

Concepts

Logging In and Out — Overview

You access BSM using a supported Web browser, from any computer with a network connection (intranet or Internet) to the BSM 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 466.

BSM is by default configured with Lightweight Single Sign-On (LW-SSO). LW-SSO enables you to log into BSM and automatically have access to other configured applications, without needing to log into those applications. For details on how LW-SSO affects logging into BSM, see "Logging into BSM with LW-SSO" on page 31.

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

Note: HP Software-as-a-Service customers access BSM using the HP Software-as-a-Service support Web site (portal.saas.hp.com).

Logging into BSM with LW-SSO

When Lightweight Single Sign-On (LW-SSO) Authentication Support 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 BSM, 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 619.
- ▶ **The JMX console.** For details on disabling LW-SSO through the JMX console, see "Resetting LDAP/SSO Settings Using the JMX Console" on page 52.

Once LW-SSO is disabled, the default BSM 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 BSM 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 619.

For details on the requirements for logging into BSM, see "How to Log In and Out" on page 37.

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 BSM.

Advanced login options include:

- ▶ **Automatic login.** You can configure BSM 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 40.
- ▶ **Direct login capabilities.** You can guide another user to a specific target page in BSM. For details, see "Use the Link to This Page Option to Open a Specific Page" on page 41.
- ▶ **Limiting login access.** You can limit the number of machines accessing BSM using the same login name. For details, see "Limit Access by Different Machines Using the Same Login Name" on page 41.
- ▶ **Linking to specific pages.** You can guide another user to a specific target page in BSM 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 32.

Linking to a Specific Page

You can guide another user to a specific target page in BSM 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 BSM 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 BSM 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.

To view Service Health or MyBSM pages in a third-party portal, select the **Embedded link** checkbox in the **Link to this page** window. The generated URL can be used in a third-party portal, so that only the specific page is displayed, and not the entire BSM application with menus.

Note: In a third-party portal, only one Service Health or MyBSM page can be embedded in each portal page. If you need to see more information, create a page which uses tabbed components. For details, see "How to Create Your MyBSM Workspace" in *Using MyBSM*.

For details on the user interface for the **Link to this page** option, see "Link to This Page Window" on page 46.

Creating a Direct Link in the RTSM

You can create a link to a specific target page in the Run-time Service Model (RTSM) using the Direct Links feature. For details on Direct Links, see "Generate a Direct Link – Overview" in *Modeling*.

Using the JMX Console

The JMX console comes embedded in BSM, and enables you to:

- ▶ Perform management operations
- ▶ View performance of processes
- ▶ Troubleshoot problematic areas of BSM

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 BSM 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 42.

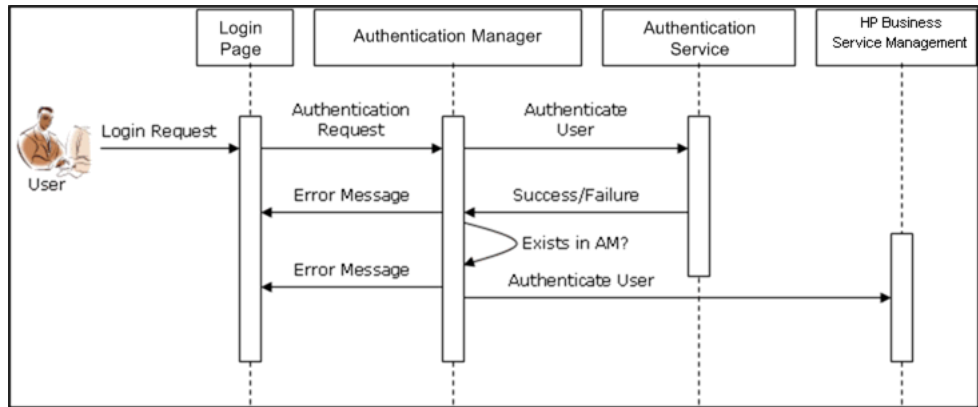
Note: The login name cannot be changed.

You can monitor the availability of your BSM system on the HP Business Service Management server status HTML page. For details, see "How to View the Status of Processes and Services" on page 25.

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.

BSM Login Flow

This section describes the general authentication flow in BSM:



- 1** 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**).
- 2** The request is transferred to the BSM 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 619.
- 3** The Authentication Manager reads the strategy name and dispatches the request to the relevant authentication strategy to validate the user.
- 4** The relevant authentication strategy accepts the request and tries to authenticate the user against the authentication service in question.
- 5** If authentication is approved, BSM verifies the user according to the selected strategy.

Note: When creating users in BSM, make sure that user names match the user names in the relevant strategy database. A user cannot log into BSM if the name does not match.

- 6 If the user passes the previous steps, they are considered an authenticated user. The BSM 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 BSM from the login page.

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

To access the BSM 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 BSM 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 BSM 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 BSM 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 administrator user name ("admin") and password specified in the Setup and Database Configuration utility.

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 557.
 - The login name cannot be changed.
-

For details on the user interface for creating users in the BSM system, see "Create User Dialog Box" on page 554.

For details on login authentication strategies that can be used in BSM, see "Set Up the Authentication Strategies" on page 613.

For login troubleshooting information, see "Troubleshooting and Limitations" on page 47.

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

To log out of BSM:

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 BSM. For details, see "Advanced Login Options" on page 32.

This section also includes:

- ▶ "Enable Automatic Login in the Login Page" on page 39
- ▶ "Modify Automatic Login Settings — Optional" on page 39
- ▶ "Use the Automatic Login URL Mechanism" on page 40
- ▶ "Use the Link to This Page Option to Open a Specific Page" on page 41
- ▶ "Limit Access by Different Machines Using the Same Login Name" on page 41

- "Open an Application Page Using a URL" on page 42

Enable Automatic Login in the Login Page

This task describes how to enable automatic login to BSM.

- 1** On the BSM login page, select **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 BSM.

Note: When automatic login is enabled from the login page and the user enters the URL to access BSM:

- 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**).
- ▶ Prevent 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 BSM 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 141.

Use the Automatic Login URL Mechanism

You can use a special URL, containing several parameters (including login name and password), to access BSM 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 BSM 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 BSM.

To enable direct entry to BSM, bookmark the Automatic Login 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 BSM. **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 BSM login page because the URL supplies the user name and password information. For details, see "Link to This Page Window" on page 46.

Limit Access by Different Machines Using the Same Login Name

BSM can be accessed using the same login name from different machines. The number of machines accessing BSM 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:

- 1** Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
- 2** Choose **Foundations**.
- 3** Select **Security**.
- 4** Locate the **Maximum machines per login name** entry, and modify the value to the number of machines you want to enable to access BSM 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 BSM, 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 51.

Open an Application Page Using a URL

You can open a specific BSM page directly in your browser by using a URL. For details, see "Linking to a Specific Page" on page 32.

How to Change the JMX Password

This task describes how to change the JMX password.

- 1 Stop the BSM Gateway or Data Processing Server.
- 2 Run the file `<HPBSM root directory>\tools\jmx\changeCredentials.bat` on either the Gateway or Data Processing Server.

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 BSM.

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 Run `cmd.exe` to open a Command Prompt 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 BSM.

How to Track Login Attempts and Logged In Users

To track who has attempted to log into the system:

View `<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 34.)
- 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 BSM:

- ▶ 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 BSM 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 BSM.

Logging Into BSM User Interface

This section includes (in alphabetical order):

- BSM Login Page on page 45
- Link to This Page Window on page 46

BSM Login Page

This page enables you to log into BSM.

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 BSM 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 37
See also	"Logging into BSM with LW-SSO" on page 31

User interface elements are described below:

UI Element (A-Z)	Description
Login Name	Enter the relevant login name to access BSM.
Password	Enter the relevant password to access BSM.
Remember my login name and password for 14 days	Select to enable BSM 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 BSM.

To access	Select Admin > Link to this page .
Relevant tasks	"How to Use Advanced Login Options" on page 38
See also	"Advanced Login Options" on page 32 "Generate a Direct Link User Interface" in <i>Modeling</i> .

User interface elements are described below:

UI Element (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 BSM page. Note: If you select this option after selecting No Credentials or Use credentials (to use credentials other than your own) and you want to invoke the login URL on the same local machine you created it on, you must first log out of BSM.
Confirm password	Re-enter the password entered in the Password field.
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 <code>about:config</code> in the browser's search window, locate the signed.applets.codebase_principal_support option, and set it to true .
Embedded link	Displayed in Service Health and MyBSM only. Select this checkbox to create a URL which can be used in a third-party portal, so that only the specific page is displayed, and not the entire BSM application with menus.

UI Element (A-Z)	Description
Generate HTML	Generates an HTML page for the specified BSM page. Note: If you select this option after selecting No Credentials or Use credentials (to use credentials other than your own) and you want to log in using the generated HTML page on the same local machine you created it on, you must first log out of BSM.
Link	The URL that the receiver uses to access the specified BSM 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 BSM.

This section includes the following topics:

- ▶ "Login Troubleshooting" on page 48
- ▶ "Limiting Access by Different Machines Using the Same Login Name Limitation" on page 51
- ▶ "Configuring the JMX Console to Work with SSL Limitations" on page 52
- ▶ "Resetting LDAP/SSO Settings Using the JMX Console" on page 52

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	<p>BSM failed to connect to the JBoss application server running on the Gateway Server. This may be due to:</p> <ul style="list-style-type: none"> ▶ the JBoss server being down ▶ problems with the BSM service ▶ the port required by the application server being used by another application 	<p>Solution 1: Close all applications on the Gateway Server machine and restart the machine.</p> <p>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).</p>
LI002	The JBoss application server running on the Gateway Server is not responding or is not installed correctly.	Restart the BSM 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 BSM administrator to create a new user for you.
LI004	The connection between the Tomcat servlet engine and the JBoss application server failed due to a Remote Method Invocation (RMI) exception. This may be due to problems in RMI calls to JBoss.	<p>Ensure that none of the JBoss ports are in use by another process. Also, ensure that the RMI ports are bound.</p> <p>For details on ports, see "Port Usage" on page 319.</p>

Error No.	Problem/Possible Cause(s)	Solution(s)
LI005	<p>The BSM login fails or hangs. This may be due to:</p> <ul style="list-style-type: none"> ▶ 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 	<p>Solution 1: Ensure that you or the user enters a correct login name/password combination.</p> <p>Solution 2: Ensure that the connection to the management database is healthy. To do so:</p> <ol style="list-style-type: none"> 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 Setup and Database Configuration utility. <p><i>...cont'd</i></p>

Error No.	Problem/Possible Cause(s)	Solution(s)
LI005 (cont'd)	The BSM login fails or hangs.	<p>Solution 3: Ensure that the user has appropriate permissions to access BSM. For details on user permissions, see "Permissions Overview" on page 445.</p> <p>Solution 4: Verify that an authentication strategy has been configured correctly. For details on authentication strategies, see "Set Up the Authentication Strategies" on page 613.</p>
LI006	<p>The BSM login fails. This may be due to:</p> <ul style="list-style-type: none"> ▶ Incorrect cookie settings in the Web browser ▶ An unsupported character in the names of the machines running the BSM servers 	<p>Solution 1: Ensure that the client Web browser is set to accept cookies from BSM servers.</p> <p>Solution 2: Ensure that there are no underscore characters (_) in the names of the machines running the BSM servers. If there are, either rename the server or use the server's IP address when accessing the machine. For example, to access BSM, use <code>http://111.222.33.44/<HPBSM root directory></code> instead of <code>http://my_server/<HPBSM root directory></code></p>

Error No.	Problem/Possible Cause(s)	Solution(s)
LI007	The BSM login fails. This is because the maximum number has been reached of concurrent logins from different machines that access BSM using the same login name.	<p>Solution 1: Log out of the instances of BSM 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.</p> <p>Solution 2: Log in using a different login name, if available.</p> <p>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.</p>

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 address resolved to BSM is that of the Gateway or Proxy server and not the IP address of the client. As a result, BSM treats each client as coming from the same IP address. Since the number of logins from the same machine (IP address) is not limited, all of the clients can log into BSM.

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 BSM.

Resetting LDAP/SSO Settings Using the JMX Console

If your LDAP or SSO settings have not been configured properly, you may be prevented from accessing BSM. If this happens, you must reset your LDAP or SSO settings remotely using the JMX console in the Application server that comes with BSM.

To reset LDAP/SSO settings using 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**

3

Navigating and Using Business Service Management

This chapter includes:

Concepts

- ▶ Navigating BSM on page 54
- ▶ User Interface Enhancements on page 58

Tasks

- ▶ How to Customize the Masthead Title and Logo on page 60

Reference

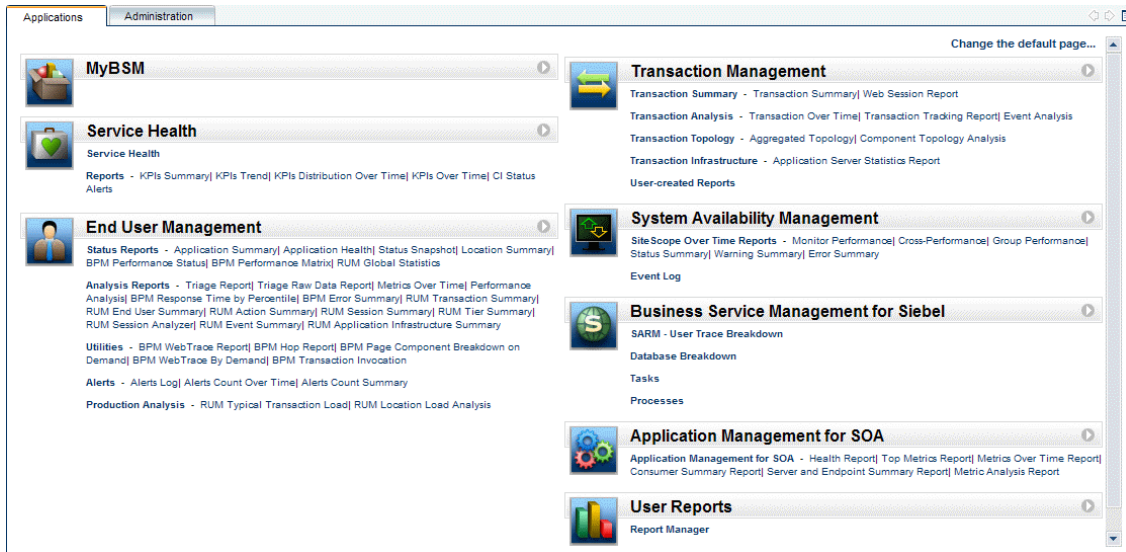
- ▶ Client Requirements for Viewing BSM on page 61
- ▶ Menus and Options on page 63

Concepts

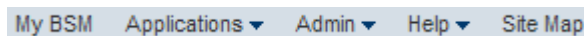
Navigating BSM

BSM runs in a Web browser. You move around BSM 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 BSM. 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.



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

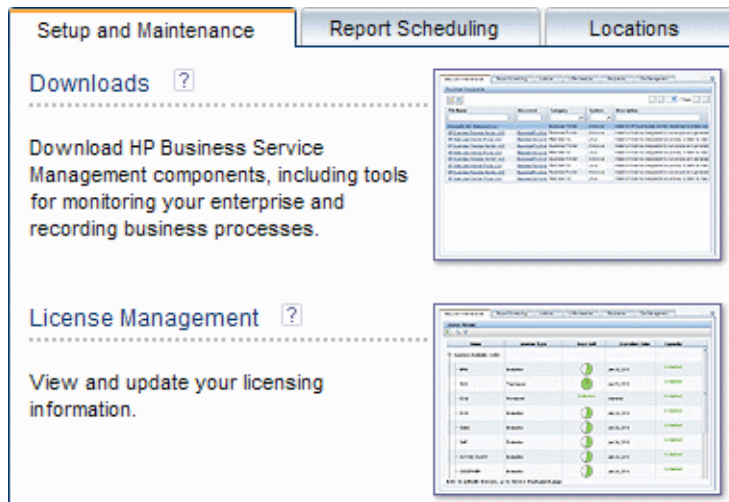


You can click the **Full Screen View** link to display the current page over the full screen. When selecting **Full Screen View**, the Task Assistant (if displayed), Menu Bar, Breadcrumbs, and Tabs are hidden. To return to the standard view of the page, click **Standard View** or press **Esc** on your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

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



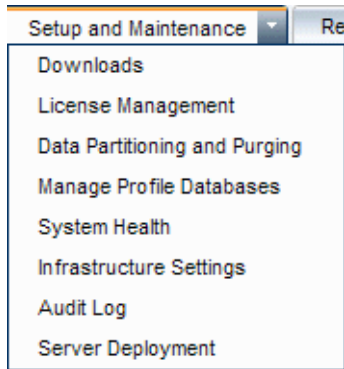
- ▶ **Tabs.** Enable navigation to various contexts within a particular area of BSM, such as to different types of reports within an application, views within a report, or administrative functions within the Administration Console. In certain contexts, tabs are used to distinguish between functions;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



- ▶ **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 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 BSM 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.

Tip: 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.

Tip: The Web browser **Back** function is not supported in BSM. 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 BSM or the breadcrumb function.

User Interface Enhancements


The BSM interface includes many features to enhance the user experience. These include:



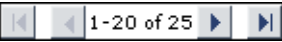



- ▶ **Section 508 compliance.** BSM is compliant with the accessibility and usability standards for people with disabilities set by the US Federal Electronic and Information Technology Accessibility and Compliance Act ("Section 508"), and supports the JAWS® screen reader.

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 BSM 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  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 .

For details about table functionality in reports, see "Common Report and Page Elements" on page 320.

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 BSM window. This change is made on the server side and affects all users accessing BSM. For details, see "How to Customize the Masthead Title and Logo" on page 60.
- **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:

- 1** Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
- 2** Select the **Foundations** context.
- 3** Select **Business Service Management Interface** from the list.
- 4** 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	<ul style="list-style-type: none"> ▶ Minimum: Color palette setting of at least 256 colors ▶ Recommended: Color palette setting of 32,000 colors <p>Note: This requirement is only necessary for the Gateway Server machine.</p>
Resolution	<ul style="list-style-type: none"> ▶ 1280x1024 or higher (recommended) ▶ 1024x768 ▶ 1280x800
Supported Browsers	<ul style="list-style-type: none"> ▶ Microsoft Internet Explorer (IE) 8.0 ▶ Microsoft Internet Explorer (IE) 7.0 <p>Note: The browser must be set to accept all cookies.</p>
Flash Player	Acrobat Flash 10.0 or later

<p>Java Plug-in (to view applets)</p>	<p>Recommended: Version 6 update 20</p> <p>Supported: Version 6 update 18 and higher</p> <p>Note: You may not be able to view all BSM 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.</p> <p>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.</p>
<p>Viewing the Documentation Library</p>	<ul style="list-style-type: none"> ▶ 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.

Tip 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 63
- ▶ "Business User Applications" on page 64
- ▶ "Administration Console" on page 65
- ▶ "Help Menu" on page 67

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

BSM 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 <i>Using Service Health</i> .
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 <i>Using Service Level Management</i> .
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 <i>Using End User Management</i> .
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 <i>Operations Management</i> .
Transaction Management	Displays transaction topology and infrastructure for data collection and report viewing. For details, see <i>Using Transaction Management</i> .

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 <i>Using System Availability Management</i> .
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 <i>Reports</i> .

Administration Console

Administrators use the Administration Console to administer the BSM 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 <i>Using Service Health</i> .
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 <i>Using Service Level Management</i> .
Operations Management	Opens the Operations Management Administration pages. For details, see <i>Operations Management</i> .

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 <i>Using End User Management</i> .
System Availability Management	Opens the System Availability Management Administration pages, where you configure and administer the SiteScope data collector. For details, see <i>Using System Availability Management</i> .
RTSM Administration	Opens the RTSM Administration pages, where you build and manage a model of your IT universe in the Run-time Service Model (RTSM). From RTSM Administration, you use Data Flow Management 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 BSM applications. You can also manually create CIs to add to the model. For details, see <i>Modeling</i> .
Business Service Management for Siebel Administration	Opens the Application Management for Siebel Administration page.
Platform	Opens the Platform Administration pages, which provide complete platform administration and configuration functionality. .
Integrations	Opens the EMS Integrations application, where you access out-of-the-box integrations (HP Service Manager, 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 BSM. For details, see <i>Solutions and Integrations</i> .

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 BSM. For details, see "Link to This Page Window" on page 46.
Personal Settings	Select to access the Personal Settings tab, which enables personalization of various aspects of BSM, including menus and passwords. Note that Personal Settings are available to all users. For details, see "Personal Settings" on page 599.

Help Menu

You access the following online resources from the BSM 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 BSM.
Troubleshooting & Knowledge Base	Opens the HP Software Support Web Site directly to the troubleshooting landing page (required HP Passport login). The URL for this Web site is http://h20230.www2.hp.com/troubleshooting.jsp
HP Software Support	Opens the HP Software Support Web Site. This site enables you to browse the knowledge base and add your own articles, post to and search user discussion forums, submit support requests, download patches and updated documentation, and more. The URL for this Web site is http://www.hp.com/go/hpsupport

Menu Option	Description
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	<p>Opens the site map, which enables quick access to all top-level contexts in the Applications menu or the Administration Console.</p> <p>Note: The Site Map is the default entry page when you log into BSM. 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 599.</p>
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

4

Downloads

This chapter includes:

Concepts

- ▶ Downloads Overview on page 72

Tasks

- ▶ How to Download Components on page 73

Reference

- ▶ Downloads User Interface on page 74

Concepts

Downloads Overview

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

Note: Products available on the Downloads page may not be the latest version; It is recommended that you check the Software Patches page in the HP Software Support Web site for the latest version (<http://support.openview.hp.com/downloads.jsp>).

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 74


Download Components Page

This page lists the BSM 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	<ul style="list-style-type: none"> ▶ 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 72

User interface elements are described below:

UI Element (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 Element (A-Z)	Description
	<p>Divides the table of data into pages. You move from page to page by clicking the relevant button:</p> <ul style="list-style-type: none"> ▶ To view more reports, click Next page or Last page. ▶ To view previous reports in the list, click Previous page or First page.
<p>Category</p>	<p>The downloadable component's category. Available categories are:</p> <ul style="list-style-type: none"> ▶ Business Process Insight. Downloadable files that enable you to install and run Business Process Insight components on BSM. ▶ Business Process Monitor. Downloadable files that enable you to install and run Business Process Monitor components on BSM. ▶ Data Flow Probe. The Data Flow Probe downloadable file that enables you to install and run the Data Flow Probe component on BSM. ▶ Diagnostics. Downloadable files that enable you to install and run Diagnostics components. ▶ 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 your operating system. ▶ 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.
<p>Description</p>	<p>An explanation of the specific downloadable file.</p>

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

Note: Products available on the Downloads page may not be the latest version; It is recommended that you check the Software Patches page in the HP Software Support Web site for the latest version (<http://support.openview.hp.com/downloads.jsp>).

5

Licenses

This chapter includes:

Concepts

- ▶ License Management Overview on page 78

Reference

- ▶ Licenses User Interface on page 79

Troubleshooting and Limitations on page 82

Concepts

License Management Overview

You must have a valid license to run monitors and transactions, and to use various integral applications in BSM.

The BSM 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.

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

A number of BSM applications require additional licensing. To use these applications, you must obtain a license from HP and then upload the license file in BSM. For more information, see "License Manager Page" on page 79. For specific information on the Operations Manager *i* (OMi) licensing structure, see "Licensing" in *Using Operations Management*.

Reference

Licenses User Interface

This section includes:


- ▶ License Manager Page on page 79

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 86
See also	<ul style="list-style-type: none"> ▶ "License Management Overview" on page 78 ▶ "Server Deployment Overview" on page 84

User interface elements are described below:

UI Element	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 Element	Description
<p>License Type</p>	<p>There are three types of licenses:</p> <ul style="list-style-type: none"> ▶ 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.
<p>Days Left</p>	<p>Displays the number of days that 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.</p> <p>When green, expiry time is pending; when red, the license is expired.</p>
<p>Expiration Date</p>	<p>Displays the license's fixed expiration date.</p> <p>This date is displayed only for time-based licenses.</p>
<p>Capacity</p>	<p>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.</p> <p>Available when:</p> <p>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.</p>

UI Element	Description
Capacity Details	<p>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.</p> <p>Available when:</p> <p>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.</p>
Server Deployment Link	<p>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.</p> <p>For user interface details, see "Server Deployment User Interface" on page 89.</p> <p>For concept details, see "Server Deployment Overview" on page 84.</p>

Troubleshooting and Limitations

This section describes troubleshooting and limitations for licence management and activation.

Manual License Activation

Some licenses are not automatically activated upon installation. These licenses must be activated for specific use and do not run at all times. To activate such a license, click the **Server Deployment** link at the bottom of the License Manager pane.

Installed Licenses and Server Deployment

Although a particular license is installed, you may find that not all features offered by the license are available to you. This can be a result of how these features are configured in BSM. You can configure these on the BSM Server Deployment page, available by clicking the **Server Deployment** link at the bottom of the License Manager pane, or by running the BSM Setup and Database Configuration Utility. For details, see "Server Deployment and Setting Database Parameters" in the *HP Business Service Management Deployment Guide* PDF.

Tip: Make sure that the enabled application always matches the installed licenses.

6

Server Deployment

This chapter includes:

Concepts

- ▶ Server Deployment Overview on page 84

Tasks

- ▶ How to Update Your BSM Licenses, Applications, or Deployment Scope on page 86

Reference

- ▶ Server Deployment User Interface on page 89

Troubleshooting and Limitations on page 93

Concepts

Server Deployment Overview

BSM 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 86
- "Add a new license — optional" on page 87
- "Update the deployment in the Server Deployment page" on page 87
- "Restart BSM" on page 88
- "Results" on page 88

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 85.

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.

Alternatively, you can 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 90.

4 Restart BSM

After you click **Save** in the Server 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 menu. 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 90

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	<ul style="list-style-type: none"> ▶ It is recommended to use this page in conjunction with the capacity calculator. For details, see "Capacity Calculator" on page 85. ▶ 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 86
See also	"Server Deployment Overview" on page 84

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

UI Element	Description
<Capacity Calculator file name>	<p>Use the Browse button to locate and upload your saved capacity calculator Excel file.</p> <p>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).</p> <p>For concept details, see "Capacity Calculator" on page 85 and for the task, see "Use the capacity calculator to determine the required capacity of your deployment change" on page 86.</p>

UI Element	Description
<Capacity table>	<p>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.</p> <p>You can change capacity level of your deployment for:</p> <ul style="list-style-type: none"> ➤ Users. Number of logged in users. ➤ Model. The number of configuration items in your model determines whether your model is small, medium, large, or extra-large. ➤ Metric Data. The number of monitored applications, transactions, locations, and hosts determines whether your metric data load is small, medium, or large. <p>You can also enable/disable applications and features, and change their capacity levels.</p> <ul style="list-style-type: none"> ➤ End User Management ➤ TransactionVision ➤ Diagnostics ➤ Business Process Insight ➤ OMi. <ul style="list-style-type: none"> ➤ TBEC. Topology-Based Event Correlation used to correlate events with OMi. ➤ Custom Rules. Used to customize event processing. For example, to customize event enrichment, or to provide custom actions in the event browser. If you are unsure whether users will be using custom rules, select to enable this feature if OMi is enabled. ➤ System Availability Management ➤ Service Level Management <p>After you click Save and restart BSM:</p> <ul style="list-style-type: none"> ➤ If you selected an application that was previously not selected, the application is available in BSM and applicable menus. ➤ If you cleared an application that was previously selected, the application is no longer accessible.

UI Element	Description
<Server status table>	<p>The lower table lists all the servers running BSM including:</p> <ul style="list-style-type: none"> ▶ 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. <p>If the Required memory is higher than the memory in the Detected column, you must either:</p> <ul style="list-style-type: none"> ▶ 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.
To disable machine	<p>Link to page on which you can disable server machines whose installed BSM components are no longer relevant to the ongoing operation of the system. Non-operational servers can also be enabled from this page. The page is not intended for high availability tasks. Before disabling a machine, verify that it is no longer an operational part of the BSM server architecture.</p>

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.

7

Database Administration

This chapter includes:

Concepts

- ▶ Database Management — Overview on page 96
- ▶ Partitioning and Purging Historical Data from Databases on page 98
- ▶ Removing Unwanted Data from the Profile Database on page 102

Tasks

- ▶ How to Configure a Profile Database on a Microsoft SQL Server on page 103
- ▶ How to Configure a User Schema on an Oracle Server on page 104
- ▶ How to Work with the Purging Manager on page 106
- ▶ How to Enable the Re-aggregation-Only Option on page 108
- ▶ How to Determine the Events Per Minute for Data Arriving in BSM on page 109
- ▶ How to Customize Data Marking Utility Configurations on page 110

Reference

- ▶ Database Administration User Interface on page 111

Troubleshooting and Limitations on page 123

Concepts

Database Management — Overview

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

You can maintain and administer the databases BSM 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.

BSM 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 103.
- ▶ **Oracle server.** This database runs on any BSM 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 104.

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.** BSM 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 BSM 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.** BSM 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.** BSM 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.

Note: BSM data collectors collect performance data and transmit it to the Gateway Server, which submits the data to profile databases using the loader mechanism. Data is inserted into the database along with a timestamp. BSM components synchronize their time clocks with that of the database server machine hosting the BSM database. Thus, the timestamp attached to each measurement inserted into the database is that of the database server clock at the time the measurement was collected.

Partitioning and Purging Historical Data from Databases

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

You use the Partition and Purging Manager to instruct the platform to automatically partition historical data for later removal from profile and Service Health Analyzer (SHA) databases.

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

BSM'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 BSM reports. After no more than two hours, that partition is purged from the profile database.

The Partition and Purging Manager is activated for each profile or SHA database and handles partitioning and later purging of historical data according to the time period listed for the database table. The size of each profile database partition is determined by the EPM (events per minute) value displayed on the Purging Manager Page. To access, select **Admin > Platform > Setup and Maintenance > Data Partitioning and Purging**.

Note: The Purging Manager Page is used for profile database configuration, and not relevant for SHA databases.

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.

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 121.

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 101.

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 BSM.

If a particular set of 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 will only be 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\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.

Removing Unwanted Data from the Profile Database

This section is not relevant to HP Software-as-a-Service customers.

The Data Marking utility enables BSM users with superuser security privileges to mark specific sets of data in profile databases as unwanted. This filters out unwanted data and enables BSM to display only the most relevant data for the specified time period. After the utility marks the specified data as unavailable, BSM automatically re-aggregates the remaining raw data for the selected time period.

The Data Marking utility also enables removal of unwanted Business Process Monitor and SiteScope data.

After you mark a specific set of data from a given time period as unwanted, BSM reruns the aggregation process on remaining raw data for the relevant time period so that the marked data is not displayed. The Data Marking utility also enables you to re-aggregate a defined set of data without marking it as unavailable. For details, see "How to Enable the Re-aggregation-Only Option" on page 108.

During installation, BSM installs the Data Marking utility on the Gateway Server. While the utility does not physically remove marked data from the database, it renders it unusable in reports and applications by assigning the marked data a status of **unavailable** in the database.

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

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 103
- "Add a Database" on page 104

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

- Access the Database Management page, located at **Admin > Platform > Setup and Maintenance > Manage Profile Databases**.
- Select **MS SQL** from the dropdown list, and click **Add**.
- 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 116.

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 104
- ▶ "Gather Connection Parameters" on page 105
- ▶ "Add a User Schema" on page 105

1 Prerequisites

Before you begin, make sure that:

- You have created a dedicated default tablespace for profile user schemas (and a dedicated temporary tablespace, if required).
- You are using a secure network connection if you do not want to submit database administrator connection parameters over a non-secure connection. If you do not want to submit database administrator connection parameters using 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 BSM 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 118.

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 106
- ▶ "Change the Database Template" on page 106
- ▶ "Change Settings for Multiple Databases" on page 107
- ▶ "Change Settings for Individual Databases" on page 108

1 Prerequisites

Ensure that you have at least one profile database configured in your BSM 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 103.

For details on configuring a user schema on an Oracle server, see "How to Configure a User Schema on an Oracle Server" on page 104.

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 check box 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 Enable the Re-aggregation-Only Option

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

To enable the re-aggregation-only option:

- 1** Open the file `<Gateway Server root directory>\tools\dataMarking\dataMarking.bat` in a text editor.
- 2** Add the **DadvanceMode** property with a value of **true** to the **SET SERVICE_MANAGER_OPTS** line. For example:

```
SET SERVICE_MANAGER_OPTS=-  
DhacProcessName=%PROCESS_NAME % -DadvancedMode=true
```

- 3 Save the file. The next time you open the Data Marking utility, the **Advanced** button appears.

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

To run data re-aggregation only:

- 1 Define the set of data you want to re-aggregate, as described in "Removing Unwanted Data from the Profile Database" on page 102.
- 2 Click the **Advanced** button. The Advanced window opens.
- 3 Select the **Run re-aggregation only** check box.
- 4 Select the categories of data for the re-aggregation and click **OK** to confirm selection.
- 5 Click **Start**.

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 BSM. 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.

How to Customize Data Marking Utility Configurations

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

To configure the maximum duration:

- 1** Open the <Gateway Server root directory>\tools\dataMarking\dataMarking.bat file in a text editor.
- 2** Add the **DmaximumDuration** property, with a value of the maximum duration in hours, to the **SET SERVICE_MANAGER_OPTS** line.

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

```
SET SERVICE_MANAGER_OPTS=  
-DhacProcessName=%PROCESS_NAME%  
-Dlog.folder.path.output=%PROCESS_NAME% -DmaximumDuration=24
```

- 3** Save and close the file.

Reference

Database Administration User Interface

This section includes (in alphabetical order):


- Database Management Page on page 111
- Data Marking Utility Page on page 112
- Profile Database Properties — MS SQL Server Page on page 116
- Profile User Schema Properties — Oracle Server Page on page 118
- Purging Manager Page on page 121

Database Management Page

This page enables you to maintain and administer the databases BSM 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 Element (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.
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.

Data Marking Utility Page

This page enables you to select sets of data for removal by application or by location for Business Process Monitor data, and by SiteScope target machine for SiteScope data.

To access	On the Gateway Server, double-click the <HPBSM Gateway Server root directory>\tools\dataMarking\dataMarking.bat file. A Command Prompt window opens, followed by the Data Marking utility login dialog box. Enter the user name and password of a BSM user with superuser privileges.
------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Important information	<ul style="list-style-type: none"> ▶ Do not run more than one instance of the Data Marking utility at a time, as this can affect the re-aggregation process. ▶ Do not mark data sets for time periods that include purged data (data that has been removed using the Partition and Purging Manager) as this can affect the re-aggregation process.
See also	<ul style="list-style-type: none"> ▶ "Removing Unwanted Data from the Profile Database" on page 102 ▶ "Data Marking Utility Limitations" on page 124

User interface elements are described below:

UI Element (A-Z)	Description
Applications	List of applications you can mark as obsolete.
Business Transaction Flows	List of business transaction flows you can mark as obsolete. Note: This field is visible only in the Applications view (i.e., if you chose Applications in the View by dropdown).
Duration	Select the period of time, starting from the specified start time, for the utility to mark data as unavailable. Note: You can set a maximum duration of up to 6 hours and 59 minutes for each data marking run. For details on customizing this value, see "How to Customize Data Marking Utility Configurations" on page 110.
Get Info	Click before running the Data Marking utility to view the number of data rows to be marked. For details, see "Data Marking Information Window" on page 115.
Locations	List of locations you can mark as obsolete.
Mark data as obsolete	Marks the filtered criteria (i.e., Applications, Business Transaction Flows, Transactions, Locations, or SiteScope Targets) as obsolete.

UI Element (A-Z)	Description
Mark data as valid (undo mark as obsolete)	Makes selected data available again after having been marked as obsolete.
Progress	Displays the progress of the data marking process and re-aggregation process.
SiteScope Targets	List of SiteScope target machines (i.e., machines being monitored by SiteScope) you can mark as obsolete. Note: This field is visible only in the SiteScope view (i.e., if you chose SiteScope View in the View by dropdown).
Start	Activates the Data Marking utility and marks data as obsolete.
Start Time	Select a starting data and time for data to be marked as unavailable.
Transactions	List of transactions you can mark as obsolete. Note: This field is visible only in the Applications view (i.e., if you chose Applications in the View by dropdown).
View by	Select the type of view to be visible in the Data Marking utility: <ul style="list-style-type: none"> ➤ Applications ➤ Locations ➤ SiteScope Targets

Data Marking Information Window

This window displays the data to be marked as obsolete by the Data Marking utility.

To access	Click the Get Info button on the Data Marking utility page.
Important information	The lower portion of the Data Marking Information window displays the SLAs affected by the marked data. You can recalculate the affected SLAs on the Agreements Manager tab under Admin > Service Level Management . For details, see "Working with the Service Level Management Application" in <i>Using Service Level Management</i> .
See also	<ul style="list-style-type: none"> ➤ "Removing Unwanted Data from the Profile Database" on page 102 ➤ "Data Marking Utility Limitations" on page 124

User interface elements are described below:

UI Element (A-Z)	Description
Application Name	The name of the application to be marked as obsolete.
Number of Rows to Update	The number of data rows to be marked as obsolete.
Total Rows to Update	The total number of rows available to be marked as obsolete. This number can differ from the value of the Number of Rows to Update field. For details, see "Data Marking Utility Limitations" on page 124.


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	<ul style="list-style-type: none"> ▶ 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 <i>HP Business Service Management Database Guide</i> PDF. ▶ Database creation can take several minutes.
Relevant tasks	"How to Configure a Profile Database on a Microsoft SQL Server" on page 103
See also	"Database Management — Overview" on page 96

User interface elements are described below:

UI Element (A-Z)	Description
Create database and/or tables	Select or clear as required. <ul style="list-style-type: none"> ▶ 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	<ul style="list-style-type: none"> ▶ 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.

UI Element (A-Z)	Description
Disconnect	<p>Disconnects the database from BSM.</p> <p>Note: This button appears only after you have clicked the Disconnect Database button  on the Database Management page.</p>
Make this my default profile database (required for custom data types)	<p>Select or clear as required.</p> <p>Note:</p> <ul style="list-style-type: none"> ▶ 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	<ul style="list-style-type: none"> ▶ Should remain empty if you are using Windows authentication. Make sure BSM 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.
Port	<p>Enter the port number if:</p> <ul style="list-style-type: none"> ▶ 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	<p>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></p>
SQL server authentication	<p>Select if the Microsoft SQL server is using SQL server authentication.</p>


UI Element (A-Z)	Description
User name	<ul style="list-style-type: none"> ▶ 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	<ul style="list-style-type: none"> ▶ 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 <i>HP Business Service Management Database Guide</i> 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 104
See also	"Database Management — Overview" on page 96

User interface elements are described below:

UI Element (A-Z)	Description
Create database and/or tables	<p>Select or clear as required.</p> <ul style="list-style-type: none"> ▶ 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. <p>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.</p>
Database administrator password	<p>Enter the password of a user with administrative permissions on Oracle server.</p> <p>Note: This field is enabled only if you selected the Create database and/or tables check box.</p>
Database administrator user name	<p>Enter the user name and password of a user with administrative permissions on Oracle server.</p> <p>Note: This field is enabled only if you selected the Create database and/or tables check box.</p>
Default tablespace	<p>Enter the name of the default tablespace designated for use with profile user schemas.</p> <p>Default Value: users</p>
Disconnect	<p>Disconnects the user schema from BSM.</p> <p>Note: This button appears only after you have clicked the Disconnect Database button  on the Database Management page.</p>
Host name	<p>Enter the name of the machine on which the Oracle server is installed.</p>

UI Element (A-Z)	Description
Make this my default profile database (required for custom data types)	Select or clear as required. Note: <ul style="list-style-type: none"> ▶ 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	<ul style="list-style-type: none"> ▶ 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	<ul style="list-style-type: none"> ▶ 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 BSM on the Oracle server.

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.

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 <i>HP Business Service Management Database Guide</i> PDF.
See also	"Partitioning and Purging Historical Data from Databases" on page 98

User interface elements are described below:

UI Element (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 109.
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 Element (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 109.
Keep Data for	<p>The time range for keeping data in the database tables whose check box is selected. This element appears as follows:</p> <ul style="list-style-type: none"> ➤ 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. <p>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.</p>
Name of Table in Database	<p>The name of the table in the database.</p> <p>Database tables are listed by the data collector from which the data was gathered. The following data types are available:</p> <ul style="list-style-type: none"> ➤ Alerts ➤ BPI ➤ Business Logic Engine ➤ Business Process Monitor ➤ Diagnostics ➤ Real User Monitor ➤ SOA ➤ Service Level Management ➤ SiteScope ➤ TV ➤ UDX (custom data) ➤ WebTrace

UI Element (A-Z)	Description
Select a profile database	<p>Select a profile database for which you want to modify time range configurations for purging data.</p> <p>Note: This field is visible only on the Database Specific tab.</p>
Template and Multiple Databases	<p>Select this tab to:</p> <ul style="list-style-type: none"> ▶ 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. <p>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.</p>

Troubleshooting and Limitations

This section describes troubleshooting and limitations for database administration.

This section includes:

- ▶ "Troubleshooting Data Marking Utility Errors" on page 124
- ▶ "Data Marking Utility Limitations" on page 124

Troubleshooting Data Marking Utility Errors

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

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

Reasons for which the utility might display this error include:

- ▶ failure to connect to the database server or profile database.
- ▶ failure to complete the data marking process, for example, due to a communication error between the Aggregation server and database.
- ▶ failure of BSM to successfully re-aggregate raw data for the defined data set.

In case of error, check the <HPBSM Gateway Server root directory>\log\datamarking.log file for error information.

Data Marking Utility Limitations

Following are limitations associated with the Data Marking utility:

- ▶ The utility does not support the removal of late arriving data.
For example, if a set of data for a specific time period is marked for removal and BSM later receives data from that time period (which arrived late due to a Business Process Monitor temporarily being unable to connect to the Gateway Server), the late arriving data is not available for use in reports. Use the **Get Info** button to check for late arriving data. If any value other than zero rows are displayed, run the utility again, if required, to remove the data that arrived late.
- ▶ The utility does not support removal of data arriving during the data marking process.

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

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

8

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 on page 128

Tasks

- ▶ How to Modify Infrastructure Settings Using the Infrastructure Settings Manager on page 130
- ▶ How to Modify the Ping Time Interval on page 130
- ▶ How to Modify the Location and Expiration of Temporary Image Files on page 131

Reference

- ▶ Infrastructure Settings User Interface on page 141

Concepts

Infrastructure Settings Manager — Overview

You can configure BSM settings to meet your organization's specifications for the platform and its applications. You configure most infrastructure settings directly within the Administration Console.

BSM enables you to modify the value of many settings that determine how BSM and its applications run.

Caution: Modifying certain settings can adversely affect the performance of BSM. 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 BSM 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 BSM foundation run. Contexts such as RTSM (Runtime Service Model) and LDAP Configuration are listed.

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

For details on configuring most infrastructure settings, see "How to Modify Infrastructure Settings Using the Infrastructure Settings Manager" on page 130.

Some infrastructure settings are configured outside the Infrastructure Settings Manager. For details, see "How to Modify the Ping Time Interval" on page 130, and "How to Modify the Location and Expiration of Temporary Image Files" on page 131.

Tasks

How to Modify Infrastructure Settings Using the Infrastructure Settings Manager

This task describes how to use the Infrastructure Settings Manager to modify infrastructure settings.

To modify infrastructure settings using the Infrastructure Settings Manager:

- 1** Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
- 2** Choose to view a group of contexts: **Applications, Foundations, or All**.
- 3** Select a specific context from the drop-down box.
- 4** All configurable infrastructure settings relating to that context are displayed, along with descriptions and the current values of each setting. Click the **Edit Setting** button and modify the value of a specific setting.

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 BSM 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, and it is recommended that it be less than a third, of the value specified for the session timeout period (the `user.session.timeout` parameter).
- 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: This 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 132.
- ▶ **The configuration of a shared location for temporary image files**
For details, see "Access Temp Directory with Multiple Gateway Server Machines" on page 133.
- ▶ **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 136.

► **The directories from which temporary images are removed**

For details, see "Specify the Directories from Which Temporary Image Files Are Removed" on page 139.

Modify the Directory in Which Temporary Image Files Are Stored

You can modify the path to the directory where BSM stores generated images used in scheduled reports. 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.

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 BSM 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 BSM reports are accessing the Gateway Server machine using a virtual IP, the load balancer could send requests to any of the Gateway Server machines. Thus, the image files need to be in a common location that is configured on all the Gateway Server machines and shared among them. This is typical when there are multiple Gateway Server machines running behind a load balancer in the BSM architecture.

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.

If you set a custom path to temporary images, as defined in the **images.save.directory.offline** parameter (for details, see "Modify the Directory in Which Temporary Image Files Are Stored" on page 132), 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, as defined in the **images.save.directory.offline** parameter (for details, see "Modify the Directory in Which Temporary Image Files Are Stored" on page 132). 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 BSM 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, as defined in the **images.save.directory.offline** parameter (for details, see "Modify the Directory in Which Temporary Image Files Are Stored" on page 132).

4 Save the file.

5 Restart BSM 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 (before the line **NameTrans fn=document-root root="\$docroot"**, and before the line **NameTrans fn="pfx2dir" from="/Imgs" dir="ProductDir/Site Imgs/"**, if it exists):

```
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, as defined in the **images.save.directory.offline** parameter (for details, see "Modify the Directory in Which Temporary Image Files Are Stored" on page 132).

- 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 BSM 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 <HPBSM 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 reports
remove.files.1.path=../../AppServer/webapps/site.war/Imgs/chartTemp/online	Path to images created when generating reports in BSM 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 BSM 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 BSM 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 BSM 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, BSM first removes expired files. BSM 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, BSM 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 BSM 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 BSM to use only the expiration time criterion.

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

Specifies the additional amount by which BSM 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. BSM deletes the oldest files first.

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

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

Specifies how often BSM runs the mechanism that performs the defined work.

Example:

BSM is instructed to perform the following work once every 30 minutes: BSM first checks whether there are files older than 1 hour and, if so, deletes them. Then BSM 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, BSM reduces the total directory size by 50% by removing the oldest files. As a result, BSM 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
```

Tip: 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 <HPBSM Gateway Server root directory>\conf\topaz.config in a text editor.
- 2** 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.
- 3** Modify the settings as required.
- 4** Save the **topaz.config** file.
- 5** Restart BSM 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 BSM to remove temporary image files from the subdirectories of the specified path.

To configure BSM 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 BSM 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 141





Infrastructure Settings Manager Page

This page enables you to define the value of many settings that determine how BSM 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 BSM. 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 128

User interface elements are described below:

UI Element (A-Z)	Description
All	Select to view all the settings for both Applications and Foundations.
Applications	Select to edit one of the BSM Applications.

UI Element (A-Z)	Description
Description	<p>Describes the specific infrastructure setting.</p> <p>Note: This field is visible on both the Infrastructure Settings Manager page, and the Edit Setting dialog box after clicking the Edit Setting button  next to the relevant setting.</p>
Foundations	<p>Select to edit one of the BSM Foundations.</p>
Name	<p>The name of the setting.</p> <p>Note: This field is visible on both the Infrastructure Settings Manager page, and the Edit Setting dialog box after clicking the Edit Setting button  next to the relevant setting.</p>
Restore Default	<p>Restores the default value of the setting.</p> <p>Note: This button is visible on the Edit Setting dialog box after clicking the Edit Setting button  next to the relevant setting.</p>
Value	<p>The current value of the given setting.</p> <p>Note: This field is visible on both the Infrastructure Settings Manager page, and the Edit Setting dialog box after clicking the Edit Setting button  next to the relevant setting.</p>

9

BSM Server Time Synchronization

This chapter includes:

Concepts

- ▶ BSM Server Time Synchronization - Overview on page 144

Tasks

- ▶ How to View the BSM Server Time on page 145

Concepts

BSM Server Time Synchronization - Overview

In order to ensure that the BSM server clocks are accurate and synchronized, the BSM servers check their system clocks against an NTP server every twenty minutes by default. Several NTP servers are configured by default, but you can manually add one in the configuration file `<BSM_HOME>\conf\settings\mtime\mtime.xml`.

If no NTP server is reachable, the database clock is used for synchronization instead.

Tasks

How to View the BSM Server Time

You can view the current BSM server time via the following URLs:

To view Unix time in plain text:

```
http://<machine>/topaz/services/technical/time?alt=text/plain
```

Example results:

```
1314089070858
```

To view the current time in XML format:

```
http://<machine>/topaz/services/technical/time
```

Example results:

```
<entry xmlns="http://www.w3.org/2005/Atom">
  <id>timeService:1</id>
  <title type="text" xml:lang="en">Time service.</title>
  <summary type="text" xml:lang="en">The time is 2011-08-23 08:44:30,858</summary>
  <published>2011-08-23T11:44:31.382+03:00</published>
  <content type="text">1314089070858</content>
</entry>
```

To view the log for this feature, see `<BSM_HOME>\logs\topaz_all.ejb.log`

10

System Health

This chapter includes:

Concepts

- ▶ System Health — Overview on page 148
- ▶ System Health Setup Wizard – Overview on page 150
- ▶ System Health Displays on page 151
- ▶ Understanding the Monitors Table on page 158
- ▶ Understanding Service Reassignment on page 159
- ▶ Adding Additional Monitors to System Health on page 161

Tasks

- ▶ How to Deploy and Access System Health on page 162
- ▶ How to Ensure the Health of Your System on page 171
- ▶ How to Add Additional Monitors to System Health Using a Template on page 175

Reference

- ▶ BSM Components on page 178
- ▶ BSM Processes on page 179
- ▶ System Health Monitors on page 181
- ▶ Component and Monitor Status Indicators on page 249
- ▶ System Health User Interface on page 250

Troubleshooting and Limitations on page 287

Concepts

System Health — Overview

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

You use System Health to:

- ▶ Measure performance by viewing the output from monitors running on the various system components.
- ▶ Monitor areas of the databases that influence performance.
- ▶ Display problematic areas of the servers, databases, and data collectors.
- ▶ Perform operations on your environment, such as:
 - ▶ **Move Backend Services.** You can move backend services from one server to another of the same type, in case the server machine is not functioning properly or requires downtime for servicing. For details on the user interface for performing this task, see "Service Manager Dialog Box" on page 281.
 - ▶ **Configure Backup Servers.** You can define a backup server in case the server machine is not functioning properly or requires downtime for servicing. For details on the user interface for performing this task, see "Backup Server Setup Window" on page 283.
 - ▶ **Manage BSM Processes.** You can start or stop various BSM processes. For details on the user interface for performing this task, see "Process Manager Dialog Box" on page 284.
- ▶ View log files on specific components in a variety of formats.
- ▶ View information on components and monitors in .csv format (displaying current status) and Quick Report format (displaying status of the past 24 hours).

BSM Server Deployment

BSM servers can be deployed through either of the following configurations:

Recommended Deployment

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

You can also deploy a separate Business Process Insight (BPI) server (BPI Full), to enable BPI Instance Tracking for full BPI functionality. For details on the BPI Application, see *Using Business Process Insight*, in the BSM Documentation Library.

Legacy Deployment

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

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

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

You can reassign the BSM services from one server to another. For details, see "Understanding Service Reassignment" on page 159.

For details on the BSM deployment configurations, see "Deployment Configurations" in the *HP Business Service Management Deployment Guide* PDF in the BSM Documentation Library.

System Health Setup Wizard – Overview

The System Health Setup Wizard enables you to create remote connections to the servers which System Health monitors. If remote connections are not created, only the monitors that do not require credential authorization to access the System Health servers will provide data.

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

For details on configuring the System Health Setup Wizard, see "How to Ensure the Health of Your System" on page 171.

For details on the pages and elements contained in the System Health Setup Wizard, see "System Health Setup Wizard" on page 269.

This section contains the following topics:

- ▶ "Synchronizing System Health in the Setup Wizard" on page 150
- ▶ "Accessing the System Health Setup Wizard" on page 151

Synchronizing System Health in the Setup Wizard



You can also access the System Health Setup Wizard by performing either **Full Model Synchronization** or **Soft Synchronization**. Soft Synchronization updates System Health with any changes to the System Health model. Full Model Synchronization resets the configuration of the selected component, including resetting of all monitors and their status. If no specific component is selected, the entire System Health configuration is reset, and the System Health Setup Wizard is generated, where you must reconfigure the connection of all system monitors to the servers.

When you perform a Soft Synchronization, System Health applies to BSM with the synchronization request. BSM receives the request and builds an up-to-date model of the BSM system and sends that model back to System Health.

- If there are new components that do not exist in System Health's current model of the BSM system, System Health adds the components to the model and deploys the appropriate monitors on those added components.
- If there is a component that was in System Health but is missing from the updated model that BSM sent to System Health, System Health does not remove the component or its monitors.

Accessing the System Health Setup Wizard

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

- The first time you access the System Health application on the machine running BSM.
- 
 ➤ Clicking the **Soft Synchronization** button on the System Health Dashboard toolbar or the Inventory tab toolbar. Soft Synchronization opens the wizard only if changes were made to the System Health model.
- 
 ➤ Clicking the **Full Model Synchronization** button on the System Health Dashboard toolbar or the Inventory tab toolbar, when no specific component is selected.

Note: Clicking the **Soft Synchronization** button displays only the portion of the wizard relevant to changes made in the system. If no changes were made, the System Health Setup Wizard does not appear.

System Health Displays

You can view the status of the BSM components using the following:

- System Health Dashboard. For details, see "System Health Dashboard" on page 152.
- Inventory Tab. For details, see "Inventory Tab" on page 155.
- Log Manager Tab. For details, see "Log Manager Tab" on page 156.

System Health Dashboard

Displays a map of all components. The color of the component box outline, as well as the status icon's color in the **Monitors** table, determines the component status. For details on the components' outline colors, see "Component Status and Description" on page 263. For details on the status icon colors, see "Component and Monitor Status Indicators" on page 249.



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



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

You can perform actions on the components by clicking the various icons on the System Health Dashboard toolbar. For details on the System Health Dashboard toolbar, see "Toolbar" on page 276.

You can also retrieve information on BSM servers using the **General** table, and information on the server's components on the **Monitors** table in the System Health Dashboard right pane. The displayed monitors run on the selected component in the System Health Dashboard left pane. For details, see "Understanding the Monitors Table" on page 158.

The monitors table is displayed as follows:

Last Update Time: 08/07/08 15:26:43

labm1mam11 - Database server

Monitors

Monitor/Group Name	Status	Last Up...
Ping	●	08/07/0...
Virtual Memory	●	08/07/0...
CPU	●	08/07/0...
cmdbhist8	○	
fnd8	○	
cmdb8	○	

Monitor Details:

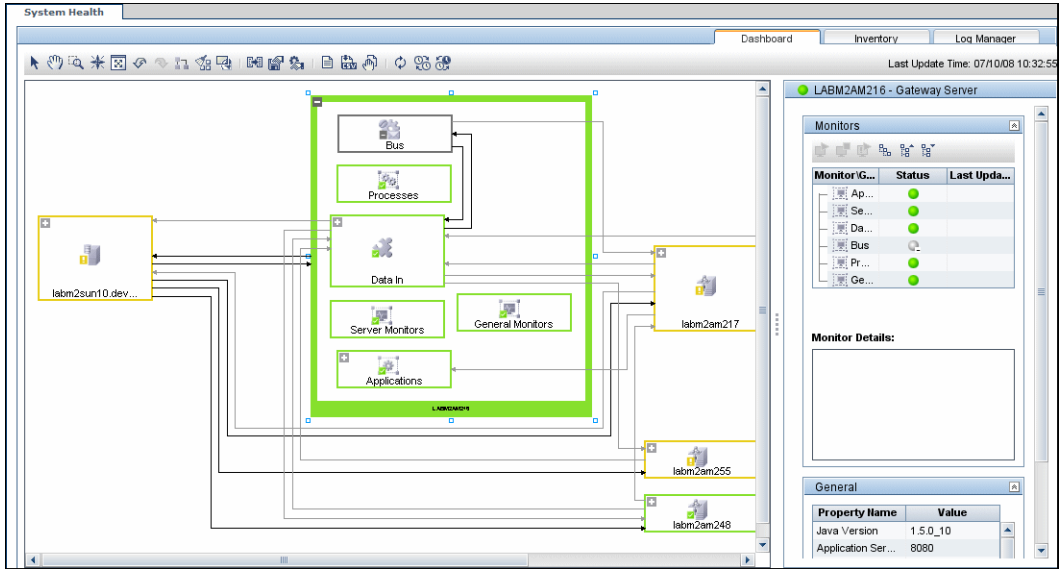
Description:
Checks the availability of the host via the network

Additional Information:
0.01 sec

General

Property Name	Value
OS Type	IBMPC/MIN_NT-8.1.0
Encoding	Cp1252
Database Type	ORACLE
IP	16.59.60.53
Name	labm1mam11
Version	Oracle Database 10g

The Dashboard tab is displayed as follows:



Inventory Tab

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

The Inventory tab is divided into the following tables:

- ▶ **Gateway Machines.** Displays the status of the various components running on the BSM Gateway machines.
- ▶ **Processing Machines.** Displays the status of the various components running on the BSM Data Processing machines.
- ▶ **<Subcomponent Name> Details.** Displays information about the selected component's monitors. The **Monitor Details** area provides additional information on the subcomponent's monitors, if applicable.

Note: The **<Subcomponent Name> Details** table is displayed only when a specific component is selected on either on the Gateway Machines or Processing Machines table on the Inventory tab.

The Inventory tab is displayed as follows:

The screenshot shows the 'System Health' application window with the 'Inventory' tab selected. The window title bar includes 'Dashboard', 'Inventory', and 'Log Manager'. The date and time '16/2/2011 16:56:08' are displayed in the top right corner. The main content area is divided into two sections: 'Gateway Machines' and 'Processing Machines'.

Gateway Machines Table:

Name	Type	Status	Server Monitors	Applications							Data In			Bus	General Monitors	Proce...	
				OPR (Console)	Portal	SAM	BPI	SLM	TVB	Dashboard App	Loader	Web Data	OPR (Gateway)				
VMAM...	Gatewa...	⊗	⦿	⦿	⦿	⦿	⦿	⦿	⦿	⦿	⦿	⦿	⦿	⦿	⦿	⦿	⦿
VMAM...	Gatewa...	⊗	⦿	⦿	⦿	⦿	⦿	⦿	⦿	⦿	⦿	⦿	⦿	⦿	⦿	⦿	⦿

Processing Machines Table:

Name	Type	Status
labm3am268	Processing Server	⊗
labm3am267	Processing Server	⊗

The component and monitor status is indicated on both the monitors table in the System Health Dashboard, and in the Inventory tab tables as a colored icon. For details on the colored icons, see "Component and Monitor Status Indicators" on page 249.

Log Manager Tab

The Log Manager tab displays the various log files associated with the components that System Health is monitoring. Logs are arranged hierarchically in **log bundles**. Nested under the log bundles are the machines in the BSM deployment that contain the individual log files.

The entities that can be seen in the **Log Bundle** pane tree are:

- ▶ **Log Bundles.** Can contain any or all of the following:
 - ▶ Other log bundles
 - ▶ Machines
 - ▶ Logs (if there is no model configured on the System Health Dashboard), arranged by category.
- ▶ **Machines.** Contains a group of logs arranged by the machine they are located on. Machines are nested under the log bundles in the hierarchical tree.
- ▶ **Individual Logs.** The individual log files monitoring the behavior of the monitored components. Logs are nested either under the log bundles, or the specific machines on which they are running.

You configure a time frame for which you want data to be retrieved in the **Time Frame** pane, and then select one or more of the components in the **Log Bundles** pane. You can then perform one of the following actions:



- ▶ Download and save the selected logs by clicking the **Save Output** button in the **Log Bundles** pane.



- ▶ Retrieve and view the selected logs by clicking the **Retrieve Logs** button. The logs are displayed in the **Main** pane, where you can also save the displayed output by clicking the **Save Output** button.



You can select any combination of log bundles, machines, and log files.

Understanding the Monitors Table

The Monitors table displays information about the monitors running on the component selected in the System Health Dashboard.

Once you have drilled down to a specific monitor in the Monitors table, you can:

- enable the monitor
- disable the monitor
- run the monitor immediately, instead of waiting for it to run according to its schedule

The monitor groups correspond to the components contained in the highlighted component in the System Health Dashboard left pane. Additional information on the individual monitors is displayed in the **Monitor Details** pane.

You can double-click a group in the Monitors table to open the monitor's parent component on the System Health Dashboard.

For details on the System Health monitors that are run by the SiteScope application, click the **SiteScope** link at the top left corner of the System Health interface.

For details on the Monitors table user interface, see "Monitors Table" on page 258.

Understanding Service Reassignment

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

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

BSM servers can be deployed either through the recommended deployment configuration or legacy deployment configuration. For details, see "BSM Server Deployment" on page 149.

When reassigning services, the secondary machine must also be a Data Processing Server.

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

For details on reassigning services, see "Service Manager Dialog Box" on page 281.

Service Reassignment Flow Table

There are several theoretical scenarios for reassigning services among machines, depending on the type of deployment with which BSM servers are configured. For details on BSM server deployment, see "BSM Server Deployment" on page 149.

The table below illustrates these scenarios by indicating the paths along which services can be reassigned.

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

Adding Additional Monitors to System Health

You can add additional monitors to System Health and view the overall health of the BSM system in one place. You can do this by creating a new template, and adding monitors and alerts to the template. You also need to add the template to the `<SiteScope root directory>/conf/sh/templates.xml` file to avoid the newly-created monitors being deleted after a Full Model Synchronization.

Note:

- ▶ It is not recommended to modify the original System Health templates, since this may lead to issues if you need to upgrade System Health.
- ▶ It is recommended to create templates outside of the System Health template container to avoid losing these changes should you need to redeploy the template.

For task details, see "How to Add Additional Monitors to System Health Using a Template" on page 175.

Tasks

How to Deploy and Access System Health

You deploy System Health in one of the following ways:

- ▶ On a standalone machine with access to BSM (recommended so that System Health continues to run if BSM servers are down).
- ▶ On any BSM Gateway server (should be done only if a standalone machine is not available).

This section contains the following topics:

- ▶ "Deploying System Health" on page 162
- ▶ "Accessing System Health" on page 168
- ▶ "Deploying System Health in a Secured Environment" on page 170

Deploying System Health

You must ensure that the Gateway server and the Management database are up and running before deploying System Health. System Health must be deployed in the same domain as BSM, and any firewalls must be open.

To deploy System Health:

- 1** Insert the SiteScope installation disk into your machine.
- 2** Run the SiteScope installation and System Health path according to your operating system.

For Windows:

- a** Enter the location from which you are installing SiteScope according to your operating system and architecture, followed by:
HPSiteScope_11.10_setup.exe.
For example, to install SiteScope on a Windows 32-bit operating system, run <DVD_ROOT>\Windows_Setup\32bit\HPSiteScope_11.10_setup.exe
- b** Run the System Health patch executable.

For Linux:

- a** Log into the server as user **root**.
 - b** Move to the directory of the DVD drive where the installation files can be found according to your operating system and architecture.
 - c** Run the script **./HPSiteScope_11.10_setup.bin -i console**
 - d** Choose to install **HP SiteScope**
Note: At this step, no System Health configuration is performed.
 - e** Copy Zip file to your local Linux server.
 - f** Extract Zip file: **unzip <name>.zip**
 - g** Edit execute permissions to all files in folder: **chmod 777 -R ***
 - h** Install 11.10 Patch for System Health: **./SIS_patch.sh**
- 3** The Choose Locale screen is displayed. Click **OK** to continue with the installation. The Initialization screen is displayed.
- 4** If the Installer detects any anti-virus program running on your system, it prompts you to examine the warnings before you continue with the installation. Read the warnings, if any, that appear in the **Application requirement** check warnings screen and follow the instructions as described in the screen.
- Click **Continue** to continue with the installation.
- 5** In the Introduction (Install) screen that opens, click **Next**.
- 6** The license agreement screen opens. Read the SiteScope License Agreement.

To install System Health, you must accept the terms of the license agreement by clicking **Next**.

- 7** In the Product Customization screen, select the **HP System Health** setup type. Click **Next** to continue.
- 8** The Feature Selection screen opens, displaying the application selected. Click **Next** to continue.
- 9** The Install Checks screen opens and runs verification checks. Click **Next** after the free disk space verification is completed successfully.

If the free disk space verification is not successful, do the following:

- Free disk space, for example by using the Windows Disk Cleanup utility.
- Repeat steps 8 and 9.

- 10** In the Pre-Install Summary screen, click **Install**.

The Installer selects and installs the required SiteScope software components. Each software component and its installation progress is displayed on your screen during installation.

- 11** After installing the SiteScope components, the Introduction screen of the SiteScope Configuration Wizard opens. Click **Next**.

12 The Settings screen of the SiteScope Configuration Wizard opens.

Settings

Enter values for the following deployment settings:

Basic settings

Port

BSM server

HP BSM Server machine

License

License file

SiteScope service settings

Service name

Use local system account

Use this account:

Password:

Confirm Password:

Enter the required configuration information and click **Next**:

- **Port.** The SiteScope port number. Accept the default port number of 18080, or choose another port that is free. If the port number is already in use (an error message is displayed).
- **HP Business Service Management server machine.** The name of the BSM Gateway server.

Note: If you are connecting System Health to an environment with a Load Balancer, enter the hostname of the BSM Gateway server, not the Load Balancer.

- ▶ **Service name.** The name of the SiteScope service. If the machine has a previous version of SiteScope installed, enter another name for the SiteScope service. The default service name is SiteScope.
 - ▶ **Use local system account.** By default, SiteScope is installed to run as a Local System account. This account has extensive privileges on the local computer, and has access to most system objects. When SiteScope is running under a Local Systems account, it attempts to connect to remote servers using the name of the server.
 - ▶ **Use this account.** Select to change the user account of the SiteScope service. You can set the SiteScope service to log on as a user with domain administration privileges. This gives SiteScope access privileges to monitor server data within the domain. Enter an account and password (and confirm the password) that can access the remote servers. If SiteScope is installed to run as a custom user account, the account used must have **Log on as a service** rights.
- 13** The Import Configuration screen opens, enabling you to import existing SiteScope configuration data to the new SiteScope installation.

Import Configuration
Import configuration data from an existing configuration file or SiteScope installation

Do not import configuration

Use existing exported configuration file

File

Import from the following SiteScope installation

Folder

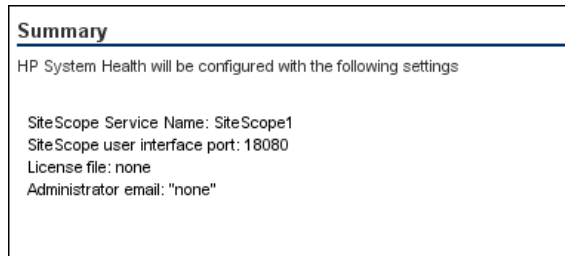
Include log files

Select one of the following options and click **Next**:

- ▶ **Do not import configuration data.**
- ▶ **Use existing exported configuration file.** Enables you to use SiteScope data from an existing exported configuration file. SiteScope data is exported using the Configuration Tool, and is saved in ZIP format. Click the **Select** button and navigate to the user data file that you want to import.

- **Import from the following SiteScope installation.** Click the **Select** button and navigate to the SiteScope installation folder from which you want to import configuration data.
- **Include log files.** Enables you to import log files from the selected SiteScope installation folder.

14 The Summary screen opens.



Check that the information is correct and click **Next** to continue, or **Back** to return to previous screens to change your selections.

- 15** In the Done screen, click **Finish** to close the SiteScope Configuration Wizard.
- 16** When the installation finishes, the Installation Complete window opens displaying a summary of the installation paths used and the installation status.

If the installation was not successful, review the installation log file for any errors by clicking the **View log file** link in the **Installation Complete** window to view the log file in a web browser.

For more information about the installed packages, click the **Details** tab.

Click **Done** to close the installation program.

If the installation program determines that the server must be restarted, it prompts you to restart the server.

Accessing System Health

You can access System Health:

- ▶ Directly, through a Web browser using the syntax:
http://<server_name>.<domain_name>:<SiteScope Server port number>/, where <server_name> is the name of the Gateway or dedicated server that System Health is deployed on, depending on the type of deployment you are using.
- ▶ As an application embedded in BSM, after configuring the appropriate URL in the Infrastructure Settings section of Platform Administration. For details, see the procedure below.

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

To access System Health directly, through a Web browser:

- 1** Ensure that System Health has been installed properly, either on your dedicated server or on your Gateway Server.
- 2** Enter the following link into your browser window:

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

where:

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

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

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

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

- ▶ Initial access can be gained using the following default login parameters:

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

- ▶ Administrator level access can be gained using the following default login parameters:

Login Name = **administrator**, Password = **syshealthadmin**

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

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

To access System Health in BSM:

- 1** Ensure that System Health has been installed, either on your dedicated server or on your Gateway Server.
- 2** Log into your BSM machine. For details, see "How to Log In and Out" on page 37.
- 3** Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**, choose **Foundations**, select **System Health**, and locate the **URL** entry in the System Health table. Modify the value to the following URL:

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

where:

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

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

- 4 Click **Save** to register the URL for accessing System Health in BSM.

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

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

Deploying System Health in a Secured Environment

When deploying System Health in a secured environment, note the following:

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

How to Ensure the Health of Your System

This task describes how to monitor the components of your system and ensure they are functioning properly.

This task includes the following steps:

- "Prerequisites" on page 171
- "Configure Remote Connection Details for Monitors" on page 171
- "Monitor Performance of Components" on page 171
- "Move Backend Services" on page 172
- "Configure Backup Servers" on page 173
- "Manage BSM Processes" on page 174
- "Display a Quick Report" on page 174

Prerequisites

Before you can monitor the health of your BSM system, you must ensure that System Health is deployed properly. For task details, see "How to Deploy and Access System Health" on page 162.

Configure Remote Connection Details for Monitors

You optionally provide the server's remote connection details for the BSM monitors that require it, using the System Health Setup Wizard. You can also configure recipients to receive System Health alerts through email. For user interface details, see "System Health Setup Wizard" on page 269.

Monitor Performance of Components

You can monitor the performance of the servers, databases, and data collectors running as part of your BSM system and view the results using either the System Health Dashboard tab or the Inventory tab. For details on the available System Health displays, see "System Health Displays" on page 151.

Move Backend Services

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

For user interface details, see "Service Manager Dialog Box" on page 281.

Example:



- 1** On the Toolbar on either the System Health Dashboard or the Inventory tab, click the **Service Manager** button.
- 2** In the **Select Source Machine** window, select the machine that you want to move services from.
- 3** In the **Select Operation** window, select the operation you want to perform.
- 4** In the **Select Target Machine** window, select the machine you want to move services to.
- 5** Click the **Execute** button. The **Operation Status** window indicates whether or not the operation request was sent successfully.

Move services from one server to other server of the same type.

Select Source Machine	Select Operation	Select Target Machine
<div style="border: 1px solid gray; padding: 5px;"> labm2am217 labm2am255 labm2am248 </div>	<div style="border: 1px solid gray; padding: 5px;"> Move all services Move offline services Move modeling services Move online services </div>	<div style="border: 1px solid gray; padding: 5px;"> labm2am255 labm2am248 </div>

Operation Status

Configure Backup Servers

In the Configure Backup Servers dialog box, you define a backup server, in case the server machine is not functioning properly or requires downtime for servicing. For user interface details, see "Backup Server Setup Window" on page 283.

Example:



- 1** On the Toolbar on the System Health Dashboard or the Inventory tab, click the **Backup Server Configuration** button.
- 2** In the left pane, select a backup server.
- 3** In the right pane, select a server to be backed-up.
- 4** Click the **Enable Automatic Failover** check box to activate your backup server selection.
- 5** Click **Execute** to register your backup server. The **Operation Status** window indicates whether or not the operation succeeded.

Define backup server.

- 1) Select backup server in the left list.
- 2) Check the servers to be backed up by selected backup server.
- 3) Automatic Failover must be checked in order to activate backup.

Select Backup Server

- labm2am217
- labm2am255
- labm2am248

Select Backed-up Servers

- labm2am255
- labm2am248

Enable Automatic Failover.

Operation Status

Automatic failover has been activated successfully.
The configuration will take effect immediately.

Manage BSM Processes

In the Process Manager dialog box, you stop or start processes on specific servers. For user interface details, see "Process Manager Dialog Box" on page 284.

Display a Quick Report



Click the **Quick Report** button to display a Quick Report with information gathered over the past 24 hours on the monitors deployed on the selected component. For user interface details, see "Quick Report Screen" on page 286.

Example:

Table Format Error List Warning List Good List		Close Window			
<h3>Summary for Multiple Monitors</h3> <p>(information from 8:58 AM 7/9/07 to 12:18 PM 7/9/07)</p> <h4>Uptime Summary</h4>					
Name	Uptime %	Error %	Warning %	Last	
Durable Subscriber Group	94.73	0	5.27	good	
Monitor Broker Group	94.73	0	5.27	good	
Monitor Subscriber Group	94.73	0	5.27	good	
Monitor Container Group	94.73	0	5.27	good	
Log Level for D:\HPBAC\conf\core\Tools\log4j\mercury_online_engine	100	0	0	good	
Log Level for D:\HPBAC\conf\core\Tools\log4j\mercury_offline_engine	100	0	0	good	
Log Level for D:\HPBAC\conf\core\Tools\log4j\mercury_data_upgrade	100	0	0	good	
Log Level for D:\HPBAC\conf\core\Tools\log4j\mam	100	0	0	good	
Log Level for D:\HPBAC\conf\core\Tools\log4j\mercury_upgrade_wizard	100	0	0	good	
Log Level for D:\HPBAC\conf\core\Tools\log4j\cmdb	100	0	0	good	
Log Level for D:\HPBAC\conf\core\Tools\log4j\common	100	0	0	good	
Log Level for D:\HPBAC\conf\core\Tools\log4j\mercury_wde	100	0	0	good	
Log Level for D:\HPBAC\conf\core\Tools\log4j\data_marking	100	0	0	good	
Log Level for D:\HPBAC\conf\core\Tools\log4j\PlainJava	100	0	0	good	
Log Level for D:\HPBAC\conf\core\Tools\log4j\EJB	100	0	0	good	
Log Level for D:\HPBAC\conf\core\Tools\log4j\mercury_pm	100	0	0	good	
Log Level for D:\HPBAC\conf\core\Tools\log4j\Servlets	100	0	0	good	
Log Level for D:\HPBAC\conf\core\Tools\log4j\bus	100	0	0	good	
Log Level for D:\HPBAC\conf\core\Tools\log4j\mercury_db_loader	100	0	0	good	
Out of Memory in log	100	0	0	good	
Logged in Users	94.73	0	5.27	good	

How to Add Additional Monitors to System Health Using a Template

This task describes how to add monitors to System Health that are not deleted after a full synchronization.

This task includes the following steps:

- "Prerequisites" on page 175
- "Create a monitoring template" on page 175
- "Add the template to the templates.xml file" on page 176
- "Perform a Hard Synchronization in System Health" on page 177

1 Prerequisites

For template monitors to be displayed correctly in System Health, they must be created directly under a template entity, instead of in a template group (the default setting). In SiteScope, click **Preferences > Infrastructure Preferences > Template Settings**, select the **Allow creation of template monitors directly under template entity** check box, and then click **Restart SiteScope**.

2 Create a monitoring template

- a In SiteScope, open the **Templates** context, and create a template container and a template in the template tree.

Note: It is not recommended to create the template in the System Health template container, since any template changes are lost if the System Health template needs to be redeployed.

- b** Select the monitor instances you want to add to the template, and enter values for the monitor properties. If you are using template variables, use the same System Health parameters that are supplied to the template deployment on runtime. For example, if the monitor requires a host name, you can enter %%SH_MACHINE_NAME%% in the **Server** box.
- c** Create monitor alerts if required.

3 Add the template to the templates.xml file

To prevent monitors and alerts being deleted from System Health after a Full Model Synchronization, perform the following:

- a** Open the <SiteScope root directory>\conf\sh\templates.xml file.
- b** Find the node and component type under which you want to deploy the template, and enter the template name. You can check in the SiteScope monitor tree for the group name mapped to the component type.

Example:

To deploy a template named MyCPUTemplate containing a CPU monitor to the Server monitors group, add the template name under the SERVERS node and component type name (Physical is the name of the group mapping in SiteScope).

```
<!-- SERVERS NODES -->
- <type name="physical">
  <template name="MyCPUTemplate" />
  <template name="PingMon" />
  <template name="NTBasicMachineRemoteMon" os_type="WINDOWS" />
  <template name="NTExtraMachineRemoteMon" os_type="WINDOWS" />
  <template name="UNIXBasicMachineRemoteMon" os_type="SOLARIS" />
  <template name="UNIXExtraMachineRemoteMon" os_type="SOLARIS" />
</type>
```

- c** Save the changes you make to the **templates.xml** file.

4 Perform a Hard Synchronization in System Health



In System Health, click the **Full Model Synchronization** button to synchronize the status and model of the components. In the left pane, select the component to which the template was added. The template monitors and alerts are displayed in the Monitors table in the right pane.

Reference

BSM Components

The System Health interface displays the following components:

- ▶ **Data Collectors.** Tools that collect availability and performance data. Data collectors include:
 - ▶ **BPMs.** Business Process Monitors, which run scripts simulating user actions and collect resulting data.
 - ▶ **RUM Engines.** Real User Monitors, which monitor actual user traffic and activity and collect resulting data.
 - ▶ **SiteScopes.** Monitor performance of IT infrastructure.
- ▶ **Discovery Probes.** Discovers the components of your IT infrastructure, creates CIs for them, and sends the data to the RTSM.
- ▶ **BSM Servers.** System Health displays the following types of BSM servers:
 - ▶ **Gateway Machines.** Servers on which BSM runs. Gateway Servers are responsible for:
 - ▶ Running BSM applications
 - ▶ Producing reports
 - ▶ Operating Platform Administration
 - ▶ Receiving data samples from the data collectors and distributing this data to the relevant BSM components
 - ▶ Supporting the bus
 - ▶ **Data Processing Machines.** Servers on which BSM runs. Data Processing Servers are responsible for:
 - ▶ Aggregating and partitioning data
 - ▶ Running the Business Logic Engines
 - ▶ Controlling the RTSM-related services

Server components are displayed on both the System Health Dashboard and the Inventory tab.

- ▶ **Load Balancing Machines.** Displayed only if deployed. Load balancers ensure that the data flow is evenly distributed among all BSM Gateway Servers so that no one particular server becomes overloaded.
- ▶ **Business Process Insight Machines.** Displayed only if deployed. A separate Business Process Insight (BPI) server (BPI Full) enables instance tracking and full BPI functionality. For details on the BPI machine, see *Using Business Process Insight*, in the BSM Documentation Library.
- ▶ **Databases.** Monitors the databases BSM is using.
- ▶ **Reverse Proxy Server.** Displayed only when System Health is configured in a secure environment. For details on Reverse Proxies, see "Using a Reverse Proxy in BSM" in the *HP Business Service Management Hardening Guide* PDF.

BSM Processes

The following table displays the processes that run on the BSM servers:

UI Element (A-Z)	Description
bpi_process_repository	Manages process definitions, which you create using the BPI Modeler, to monitor IT operational resources defined within the RTSM. Process name: BPI Process Repository
data_upgrade	Enables transferring of data from a previous version of BSM to a newer version. Process name: DataUpgrade
dbloader	Runs the component on the server which loads the data into the database. Process name: mercury_db_loader
domain_manager	Responsible for all the bus processes in all BSM servers. Process name: DomainManager

UI Element (A-Z)	Description
ldap	Runs queries and modifications for directory services. Process name: slapd
mercuryAS	Runs the JBoss application server, which provides access to all BSM applications. Process name: MercuryAS
message_broker	Enables the transference of a message from the formal messaging protocol of the sending machine to the formal messaging protocol of the receiving machine. Process name: MessageBroker
offline_engine	Runs the engine which controls the offline components of the BSM system. Process name: mercury_offline_engine
online_engine	Runs the engine which controls the online components of the BSM system. Process name: mercury_online_engine
pmanager	Runs the Partition Manager to create new or purge old partitions in the profile database, as necessary. Process name: mercury_pm
RTSM Process	Runs on the RTSM database that stores all the configuration item data. It does not always run, depending on your BSM deployment. Process name: RTSM
schedulergw	Enables scheduling tasks to be continually run on the Gateway Server. Process name: schedulergw

UI Element (A-Z)	Description
schedulerpr	Enables scheduling tasks to be continually run on the Data Processing. Process name: schedulerpr
WDE	Runs the Web Data Entry component of the Gateway Server, which receives data from all registered data collectors and publishes the data to all BSM engines. Process name: mercury_wde

System Health Monitors

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

Note: The documentation for SiteScope monitors is found in *Monitor Reference* in the SiteScope Help. You can access the SiteScope Help from the directory where your System Health is installed (<**System Health root directory**>\sisdocs\doc_lib), or from a SiteScope server by selecting **Help > SiteScope Help**, and navigating to the Help page for the specific SiteScope monitor in the Monitor Reference guide.

Monitors are displayed in the **Monitors** table, located in the right pane of the System Health Dashboard. For details on the Monitors table, see "Monitors Table" on page 258.

This section describes the following groups of monitors:

- "Machine Hardware Monitors" on page 182
- "Database Monitors" on page 183
- "BSM Server Monitors" on page 184
- "Gateway Server Monitors" on page 195

- "Data Processing Server Monitors" on page 215
- "BPI Server Monitors" on page 239
- "Data Collectors" on page 243

 **Machine Hardware Monitors**

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

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
<p>Ping</p>	<p>Checks the availability of the host using the network. Runs on BSM and Database servers. If BSM includes a proxy server or load balancer, this monitor runs on the mediator or load balancer.</p> <p>Included Measurements:</p> <ul style="list-style-type: none"> ➤ Round Trip Time ➤ Loss Percentage <p>Threshold Configured In: SiteScope (Ping monitor)</p>	<p>Effect on BSM: This monitor is in error when the host is inaccessible from the System Health server</p> <p>Troubleshooting: Check to see if:</p> <ul style="list-style-type: none"> ➤ the host is down ➤ the network is down ➤ network security prevents System Health from accessing the host (which means no monitoring can be done on this server)
<p>Server Virtual Memory</p>	<p>Tracks how much virtual memory is currently in use on the server. Runs on BSM and Database servers.</p> <p>Threshold Configured In: SiteScope (Memory monitor)</p>	<p>Troubleshooting: If a server is running low on virtual memory, you can:</p> <ul style="list-style-type: none"> ➤ Restart the server (this may provide a temporary fix) ➤ Upgrade the server's memory (might be required for a long term solution)

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Server CPU	Tracks how much CPU is currently in use on the server. Runs on BSM and Database servers. Threshold Configured in: SiteScope (CPU monitor)	Troubleshooting: For high CPU usage: <ul style="list-style-type: none"> ▶ check which processes are running on the server ▶ see if any of the processes can be removed or moved to another server
Server Disk Space	Tracks how much disk space is currently in use on the hard disk drive where BSM is installed. Runs only on the server. Threshold Configured In: SiteScope (Disk Space monitor)	Troubleshooting: To free up disk space, you can: <ul style="list-style-type: none"> ▶ delete unnecessary files on the server ▶ remove installed programs that require a lot of space ▶ upgrade the server disk to a larger hard drive

Database Monitors

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

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
DB Statistics	Verifies that database statistics have been collected for all tables created more than 24 hours ago.	Effect on BSM: Poor database engine performance, incorrect execution plans used by the database optimizer, or a connection pool timeout ending the transaction. Troubleshooting: Run statistics collection against BSM databases on a regular basis by creating a job, or have the product database administrator run it manually.

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Database Connectivity	Verifies the connection between BSM and the database.	<p>Effect on BSM: Failure in BSM to start up or run, no persistency data in the database, or the reports fail to run or contain no data.</p> <p>Troubleshooting:</p> <ul style="list-style-type: none"> ➤ On the database side, check that the instance is up, and verify there are no database server errors such as running out of storage, database corruption, or running out of connections. ➤ On the BSM side, check the network between the BSM client and the database server for issues such as network delays, firewall problems, IP/DNS resolution, packet loss, and so forth.

 **BSM Server Monitors**

The following monitors run on the Gateway Server, the Processing server, or, if not otherwise indicated, both:

- "General Monitors" on page 185
- "Process Monitors" on page 186
- "Bus" on page 189
- "UCMDB/RTSM" on page 190
- "Modeling/Viewing System" on page 194

General Monitors

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Out of Memory in Log	<p>Searches for unexpected behavior due to the server being out of memory, displayed as instances of Out of Memory in topaz_all.ejb.log.</p> <p>Threshold Configured In: SiteScope (Log File monitor)</p>	<p>Effect on BSM: Some data might not be available in Service Health and in reports, and some of the applications might not work.</p> <p>Troubleshooting:</p> <ul style="list-style-type: none"> ▶ Check for other monitors in error when trying to resolve out of memory issues ▶ Verify the BSM deployment and expected load using the BSM Capacity calculator ▶ Based on information found in the other monitors, you might need to restart the Gateway Server or upgrade your hardware
Nanny Manager Process	<p>Monitors whether BSM server processes are up and running.</p> <p>Threshold Configured In: SiteScope (Service monitor)</p>	<p>Effect on BSM: If a process is down, the Nanny Manager Process monitor tries to start it automatically.</p> <p>Troubleshooting: Contact HP Software Support if the monitor cannot start the process.</p>
Log Level for <configuration directory>	<p>Checks if any of the log files in the specified directory are configured to debug log level (i.e., searches for the string loglevel=debug).</p> <p>Threshold Configured In: SiteScope (Log File monitor)</p>	<p>Effect on BSM: Debug log level affects the amount of output in the log which consumes more disk space and slows down the application.</p> <p>Troubleshooting: Change the configuration back to loglevel=ERROR.</p>

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
BSM Application Server Response	Checks that the BSM Application server is responsive. Information goes straight to the application server and does not travel by way of the web server. This monitor runs only on the Gateway Server. Threshold Configured In: SiteScope (URL monitor)	Effect on BSM: BSM is not accessible if the application server is not responsive. Responsiveness issues with the BSM Application server are usually a symptom of other problems. Troubleshooting: Check for monitors in error when trying to resolve application server response issues.
Logged In Users	Displays the percentage and number of total users logged into BSM.	Effect on BSM: This can result in responsiveness issues in a number of different applications. Troubleshooting: Make sure that the total number of logged in users does not exceed the recommended amount of users.

Process Monitors

For descriptions of the processes, see "Process Manager Dialog Box" on page 284.

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

- analytics_loader
- DataUpgrade
- mercury_db_loader
- mercury_offline_engine
- mercury_online_engine
- mercury_wde
- MercuryAS
- MessageBroker

- pi_engine
- pmanager
- RTSM

The <process name> monitor monitors both the Java and non-Java processes. For details on the processes, see "BSM Processes" on page 179.

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
<Process Name> JVM Statistics Memory Monitors	Monitors the memory measurements for a Java process. Included Measurements: <ul style="list-style-type: none"> ➤ Heap Free. Displays the amount of Heap Free space in JVM. ➤ Permanent Heap Free Memory. Displays the amount of Permanent Heap Free space in JVM. 	Effect on BSM: Some data might not be available in Service Health and in reports. Troubleshooting: Verify the BSM deployment type, memory (RAM), and expected load (reported samples per second) using the BSM capacity calculator. This type of exception usually occurs if BSM is installed on hardware that has insufficient resources for the current load.

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
<Process Name> JVM Statistics Threads Monitors	<p>Monitors the threads measurements for a Java process. The process name is in the name of the monitor.</p> <p>Included Measurements:</p> <ul style="list-style-type: none"> ▶ Current Thread Count. Current number of threads used by the process. ▶ Dead Locked Threads. Number of deadlocked threads in the process. 	<p>Effect on BSM: Some data might not be available in Service Health and in reports.</p> <p>Troubleshooting: Verify the BSM deployment type, memory (RAM), and expected load (reported samples per second) using the BSM capacity calculator. This type of exception usually occurs if BSM is installed on hardware that has insufficient resources for the current load.</p>
<process name>	<p>Verifies whether the <process name> process is running, its CPU, and virtual memory utilization.</p> <p>Uses the SiteScope Service monitor.</p>	<p>Effect on BSM: The effect on BSM depends on which process is running.</p> <p>Troubleshooting: Verify the BSM deployment type, memory (RAM), and expected load (reported samples per second) using the BSM capacity calculator. This type of exception usually occurs if BSM is installed on hardware that has insufficient resources for the current load.</p>

Bus

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Subscriber Group	<p>Monitors the number and size of messages waiting for regular subscribers.</p> <p>Threshold Configured In: Infrastructure Settings.</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.</p>	<p>Effect on BSM: If the number or size of messages waiting for processing is high, the bus may suffer from low performance. This may also cause out of memory exceptions.</p> <p>Troubleshooting: Contact your system administrator if the message threshold is met.</p>
Broker Group	<p>Monitors the overall measurements of the broker (bytes and number of messages).</p> <p>Threshold Configured In: Infrastructure Settings.</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.</p>	<p>Effect on BSM: If the number or size of messages waiting for processing is high, the bus may suffer from low performance. This may also cause out of memory exceptions.</p> <p>Troubleshooting: Contact your system administrator if the message threshold is met.</p>
Durable Subscriber Group	<p>Monitors the number and size of messages waiting for durable subscribers in the broker.</p> <p>Threshold Configured In: Infrastructure Settings.</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.</p>	<p>Effect on BSM: If the number of messages waiting for durable subscribers is high, this affects the size and performance of the local database. The bus may suffer from low performance and may get stuck when the database files grow by more than a few gigabytes.</p> <p>Troubleshooting: Contact your system administrator if the message threshold is met.</p>

UCMDB/RTSM

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Model Objects Quota and Count	<p>Compares current CI count with the CI quota.</p> <p>Threshold Configured In: Infrastructure Settings.</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.</p>	<p>Effect on BSM: If the quota is exceeded, no more CIs and links can be added.</p> <p>Troubleshooting:</p> <ul style="list-style-type: none"> ➤ Increase the CI quota ➤ Delete unnecessary CIs ➤ Refine the discovery process so it discovers less data
TQL Quota and Count	<p>Compares current TQL count with the TQL quota.</p> <p>Threshold Configured In: Infrastructure Settings.</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.</p>	<p>Effect on BSM: If the quota is exceeded, no new active TQLs can be added.</p> <p>Troubleshooting:</p> <ul style="list-style-type: none"> ➤ Increase the quota ➤ Delete unnecessary TQLs
Oversized TQLs	<p>Displays TQLs that are larger than the size permitted by the configured threshold.</p> <p>Threshold Configured In: Infrastructure Settings.</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.</p>	<p>Effect on BSM: If the TQL result is larger than the threshold, the TQL is deactivated.</p> <p>Troubleshooting: Change the TQL definition.</p>

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Availability and Performance	<p>Checks system availability and response time.</p> <p>Included Measurements:</p> <ul style="list-style-type: none"> ➤ Run AdHoc TQL. Checks how long the Run AdHoc TQL operation takes. ➤ Load ClassModel. Checks how long the Load ClassModel operation takes. <p>If response time exceeds 2 seconds, monitor status changes to Warning. If response time exceeds 15 seconds, monitor status changes to Error.</p> <p>Threshold Configured In: Infrastructure Settings.</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.</p>	<p>Effect on BSM: System availability issues and slow response time affect BSM performance.</p> <p>Troubleshooting: Check the log files, and try to resolve the problem from the information provided.</p>
DB - Could not reset timeout because the object is not monitored	<p>Searches for Couldn't reset timeout because the object isn't monitored in cmdb.log.</p> <p>Threshold Configured In: SiteScope (Log File monitor)</p>	<p>Troubleshooting: If this error is registered in the log file, there are problems in the database. Contact your database administrator for assistance.</p>
DB - Failed to borrow object from pool	<p>Searches for Failed to borrow object from pool in cmdb.log.</p> <p>Threshold Configured In: SiteScope (Log File monitor)</p>	<p>Troubleshooting: If this error is registered in the log file, there are problems in the database. Contact your database administrator for assistance.</p>

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
<p>DB - Failed to create a connection</p>	<p>Searches for Failed to create a connection for in cmdb.log. Threshold Configured In: SiteScope (Log File monitor)</p>	<p>Troubleshooting: If this error is registered in the log file, there are problems in the database. Contact your database administrator for assistance.</p>
<p>Notification - Cannot Publish</p>	<p>Searches for cannot publish in cmdb.log. Threshold Configured In: SiteScope (Log File monitor)</p>	<p>Effect on BSM: There are no notifications about active TQLs or model updates, and BSM applications and Service Health are not notified about changes in topology (such as added hosts or business transactions). Troubleshooting: Check the bus log file to determine what caused the problem.</p>

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Notification - Cannot get notifications from the BUS	Searches for error occurred during receive of JMS message in cmdb.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM if this error is registered in the log file: There are no notifications about active TQLs or model updates, and BSM applications and Service Health are not notified about changes in topology (such as added hosts or business transactions). Troubleshooting: Check the bus log file to determine what caused the problem.
Performance - Request Timeout	Searches for Request Timeout in cmdb.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM if this error is registered in the log file: This error may indicate a general problem, or it may have been caused by a temporary issue such as running a large number of TQLs. Troubleshooting: Check the log file to determine what caused the problem.

Modeling/Viewing System

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
All Symbols Quota and Count	<p>Compares current symbols count with symbols quota. You can create a view on top of a TQL. Each element in the view tree is called a symbol. The quota is determined in the settings.</p> <p>Threshold Configured In: Infrastructure Settings.</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.</p>	<p>Effect on BSM: If the quota is exceeded, no new active views can be created.</p> <p>Troubleshooting: Deactivate unnecessary views or increase the quota.</p>
Views Quota and Count	<p>Compares current views count with views quota.</p> <p>Threshold Configured In: Infrastructure Settings.</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.</p>	<p>Effect on BSM: If the quota is exceeded, no new views can be created.</p> <p>Troubleshooting: Deactivate unnecessary views or increase the quota.</p>

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Oversized Views	<p>Checks for views that are larger than the threshold configured in Infrastructure Settings.</p> <p>Threshold Configured In: Infrastructure Settings.</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.</p>	<p>Effect on BSM: Oversized views are deactivated.</p> <p>Troubleshooting: Change the view definition.</p>

Gateway Server Monitors

The following monitors run on the Gateway Server:

- "Data In/Web Data Entry" on page 196
- "Data In/Loader" on page 198
- "Data In/Analytics Loader" on page 201
- "Data In/Operations Management Gateway" on page 205
- "Service Health Application" on page 208
- "Operations Management Application" on page 211
- "Portal Application" on page 214
- "Verticals Application" on page 214
- "System Availability Management Application" on page 215

Data In/Web Data Entry

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Web Data Entry Status	<p>Determines the overall status of the Web Data Entry component.</p> <p>Included Measurements:</p> <ul style="list-style-type: none"> ➤ Bus Status. Determines Web Data Entry connection to the bus. ➤ Gateway Status. Determines Gateway availability. ➤ Failures to Publish. Indicates number of samples which failed to publish. ➤ Output EPS. Determines the number of published samples per second. 	<p>Effect on BSM: Samples arriving to Web Data Entry are discarded or are not published to the bus. This means there is no sample data in BSM.</p> <ul style="list-style-type: none"> ➤ Problems with the bus result in the Web Data Entry component rejecting samples arriving from data collectors ➤ Samples are rejected if the Gateway Server is unavailable ➤ Events per second (EPS) that exceed the bus capability result in locking Web Data Entry from receiving samples <p>Troubleshooting: Check the following logs in the <HPBSM root directory>\log\mercury_wde\ directory:</p> <ul style="list-style-type: none"> ➤ wde.log ➤ wdeIgnoredSamples.log ➤ wdeStatistics.log ➤ wde.all.log
Out of Memory Exception in Log	<p>Searches for unexpected behavior, displayed as instances of the string OutofMemoryExceptionInLog in the wde.log file. This is caused by samples or buffers arriving to WDE with too much data.</p> <p>Uses the SiteScope Log File monitor.</p>	<p>Effect on BSM: Some data might not be available in the Service Health and in reports.</p> <p>Troubleshooting: Verify the BSM deployment type, memory (RAM), and expected load (reported samples per second) using the BSM Capacity Calculator. This type of exception usually occurs if BSM is installed on hardware that has insufficient resources for the current load.</p>

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Class Not Found Exception in Log	<p>Searches for unexpected behavior, displayed as instances of the string <code>ClassNotFoundException</code> in the wde.log file. This might be caused by a bug in the system or the incorrect probe version being connected to the BSM server.</p> <p>Uses the SiteScope Log File monitor.</p>	<p>Effect on BSM: Some data might not be available in the Service Health and in reports.</p> <p>Troubleshooting: Make sure that the correct version of the probe is connected to the BSM server. If the correct probe version is being used, contact HP Software Support.</p>
Web Data Entry Availability	<p>Determines if Web Data Entry is up and running.</p> <p>Uses the SiteScope Log File monitor.</p>	<p>Effect on BSM: No data is arriving to BSM.</p> <p>Troubleshooting: Check the following logs in the <HPBSM root directory>\log\mercury_wde\ directory:</p> <ul style="list-style-type: none"> ➤ wde.log ➤ wde.all.log

Data In/Loader

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
<p>Main Flow</p>	<p>Measures flow of data in component.</p> <p>Included Measurements:</p> <ul style="list-style-type: none"> ▶ Number of Samples in Queues. Used to control memory usage of the loader. ▶ Bus Connection Status. Checks loader connectivity to the bus. 	<p>Effect on BSM: No data in the BSM database (the loader is unable to collect samples from the bus).</p> <ul style="list-style-type: none"> ▶ Problems with the bus indicate no persistency data in the database, and the reports show no data ▶ Too many samples in queues indicate a backlog, or unavailability of the profile database <p>Troubleshooting:</p> <ul style="list-style-type: none"> ▶ Check the status of the bus ▶ Contact your database/network administrator for assistance on connectivity to the profile database and database load
<p>EPS ratio in main flow</p>	<p>Enables you to evaluate the ratio of the average insert rate to the loader with the average data insert rate to the database from the loader.</p> <p>Threshold Configured In: Infrastructure Settings.</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings > Foundations > Loader.</p>	<p>Effect on BSM: A high EPS value may cause a delay in the data being written to the database, and increase the disk space being used by recovery persistency data files.</p>

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Connection to DB	Checks connection to the database from loader process.	<p>Effect on BSM: Reports are displayed without data. This indicates that no data persisted in the database.</p> <p>Troubleshooting: Check dbloader logs for the connectivity error, and contact your database administrator for assistance.</p>
Average Insert Rate to DB (Recovery Flow)	<p>Monitors the average insert rate to the database from the recovery persistency folder. A long insert rate indicates database performance problems.</p> <p>Threshold Configured In: Infrastructure Settings.</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.</p>	<p>Troubleshooting: Contact your database administrator for assistance.</p>
Out of Memory Exception in Log	<p>Searches for the string Out of Memory in Loader.log.</p> <p>This is caused by samples or buffers arriving to the loader with too much data.</p> <p>Uses the SiteScope Log File monitor.</p>	<p>Effect on BSM: Some data might not be available in Service Health and reports.</p> <p>Troubleshooting: Verify the BSM deployment type, memory (RAM), and expected load (reported samples per second) using the BSM Capacity Calculator. This type of exception usually occurs if BSM is installed on hardware that has insufficient resources for the current load.</p>

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Class Not Found Exception in Log	<p>Searches for errors in Loader.log. This might be caused by a bug in the system or the incorrect probe version being connected to the BSM server.</p> <p>Uses the SiteScope Log File monitor.</p>	<p>Effect on BSM: Some data might not be available in Service Health and reports.</p> <p>Troubleshooting: Make sure that the correct version of the probe is connected to the BSM server. If the correct probe version is being used, contact HP Software Support.</p>
Max Files in Queue in Recovery Persister	<p>Displays the number of files in the longest queue in the recovery persister directory.</p> <p>Threshold Configured In: Infrastructure Settings.</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.</p>	<p>Effect on BSM: No data is displayed in reports if too many files are in the recovery persistency queue.</p> <p>This can be caused by:</p> <ul style="list-style-type: none"> ➤ A high number of EPS ➤ Slow database insert rate ➤ Limited database availability <p>Troubleshooting: Contact your database/network administrator for assistance on connectivity to the profile database and database load.</p>

Data In/Analytics Loader

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Main Flow	<p>Measures flow of data in component.</p> <p>Included Measurements:</p> <ul style="list-style-type: none"> ▶ Number of Samples in Queues. Used to control memory usage of the loader. ▶ Bus Connection Status. Checks loader connectivity to the bus. 	<p>Effect on BSM: No data in the BSM database (the loader is unable to collect samples from the bus).</p> <ul style="list-style-type: none"> ▶ Problems with the bus indicate no persistency data in the database, and the reports show no data ▶ Too many samples in queues indicate a backlog, or unavailability of the profile database <p>Troubleshooting:</p> <ul style="list-style-type: none"> ▶ Check the status of the bus ▶ Contact your database/network administrator for assistance on connectivity to the profile database and database load
EPS ratio in main flow	<p>Enables you to evaluate the ratio of the average insert rate to the loader with the average data insert rate to the database from the loader.</p> <p>Threshold Configured In: Infrastructure Settings.</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings > Foundations > Loader.</p>	<p>Effect on BSM: A high EPS value may cause a delay in the data being written to the database, and increase the disk space being used by recovery persistency data files.</p>

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Connection to DB	Checks connection to the database from loader process.	<p>Effect on BSM: Reports are displayed without data. This indicates that no data persisted in the database.</p> <p>Troubleshooting: Check dbloader logs for the connectivity error, and contact your database administrator for assistance.</p>
Average Insert Rate to DB (Recovery Flow)	<p>Monitors the average insert rate to the database from the recovery persistency folder. A long insert rate indicates database performance problems.</p> <p>Threshold Configured In: Infrastructure Settings.</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.</p>	<p>Troubleshooting: Contact your database administrator for assistance.</p>
Out of Memory Exception in Log	<p>Searches for the string Out of Memory in Loader.log.</p> <p>This is caused by samples or buffers arriving to the loader with too much data.</p> <p>Uses the SiteScope Log File monitor.</p>	<p>Effect on BSM: Some data might not be available in Service Health and reports.</p> <p>Troubleshooting: Verify the BSM deployment type, memory (RAM), and expected load (reported samples per second) using the BSM Capacity Calculator. This type of exception usually occurs if BSM is installed on hardware that has insufficient resources for the current load.</p>

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Class Not Found Exception in Log	<p>Searches for errors in Loader.log. This might be caused by a bug in the system or the incorrect probe version being connected to the BSM server.</p> <p>Uses the SiteScope Log File monitor.</p>	<p>Effect on BSM: Some data might not be available in Service Health and reports.</p> <p>Troubleshooting: Make sure that the correct version of the probe is connected to the BSM server. If the correct probe version is being used, contact HP Software Support.</p>
Max Files in Queue in Recovery Persister	<p>Displays the number of files in the longest queue in the recovery persister directory.</p> <p>Threshold Configured In: Infrastructure Settings.</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.</p>	<p>Effect on BSM: No data is displayed in reports if too many files are in the recovery persistency queue.</p> <p>This can be caused by:</p> <ul style="list-style-type: none"> ➤ A high number of EPS ➤ Slow database insert rate ➤ Limited database availability <p>Troubleshooting: Contact your database/network administrator for assistance on connectivity to the profile database and database load.</p>
Analytics Loader log monitor	<p>Searches for unexpected behavior, displayed as instances of error.</p>	<p>Effect on BSM: Process may not function correctly.</p> <p>Troubleshooting: Check the log file and try to resolve the problem from the error message provided.</p>
Analytics Loader General log monitor	<p>Searches for unexpected behavior, displayed as instances of error.</p>	<p>Effect on BSM: Process may not function correctly.</p> <p>Troubleshooting: Check the log file and try to resolve the problem from the error message provided.</p>

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Loader log monitor	Searches for unexpected behavior, displayed as instances of error.	<p>Effect on BSM: Process may not function correctly.</p> <p>Troubleshooting: Check the log file and try to resolve the problem from the error message provided.</p>
Analytics Loader Statistics log monitor	Monitors the statistics for the analytics_loader process.	<p>Effect on BSM: Some data might not be available in SHA.</p> <p>Troubleshooting: Verify the BSM deployment type, memory (RAM), and expected load (reported samples per second) using the BSM capacity calculator. This type of exception usually occurs if BSM is installed on hardware that has insufficient resources for the current load.</p>
Analytics CIs	Shows the amount of Analytics CIs	<p>Effect on BSM: Some data may not be inserted into the Analytics DB.</p> <p>Troubleshooting: Contact HP Software Support in case of error (99% occupied).</p>
SHA Plugin	Shows the amount of traced metrics.	For information only.

Data In/Operations Management Gateway

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
OPR Common	Searches for unexpected behavior, displayed as instances of ERROR, in opr-common.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Operations Management communication with data sources, for example, receiving and synchronizing events. Troubleshooting: Check the log file, and try to resolve the problem from the error messages provided.
OPR Common.properties	Scans the OPR Common.properties file. Loglevel with values of 'Debug', 'All' or 'Off' are considered inappropriate for production environments and therefor will report error. Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Debug log level affects the amount of output in the log which consumes more disk space and slows down the application. Troubleshooting: Change the configuration back to loglevel=ERROR .
OPR Event sync adapter.properties	Scans the OPR Event sync adapter.properties file. Loglevel with values of 'Debug', 'All' or 'Off' are considered inappropriate for production environments and therefor will report error. Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Debug log level affects the amount of output in the log which consumes more disk space and slows down the application. Troubleshooting: Change the configuration back to loglevel=ERROR .

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
<p>OPR Flowtrace.Common</p>	<p>Searches for unexpected behavior, displayed as instances of ERROR, in opr-flowtrace-common.log.</p> <p>Threshold Configured In: SiteScope (Log File monitor)</p>	<p>Effect on BSM: Flow of Operations Management events through the gateway adapter might not function correctly.</p> <p>Troubleshooting: Check the log file, and try to resolve the problem from the error messages provided.</p>
<p>OPR Gateway</p>	<p>Searches for unexpected behavior, displayed as instances of ERROR, in opr-common.log.</p> <p>Threshold Configured In: SiteScope (Log File monitor)</p>	<p>Effect on BSM: Forwarding, receiving and synchronizing events with thrid-party applications might not function correctly.</p> <p>Troubleshooting: Check the log file, and try to resolve the problem from the error messages provided.</p>
<p>OPR Gateway Flowtrace</p>	<p>Searches for unexpected behavior, displayed as instances of ERROR, in opr-common.log.</p> <p>Threshold Configured In: SiteScope (Log File monitor)</p>	<p>Effect on BSM: Flow of events between Operations Management and hrid-party applications might not function correctly.</p> <p>Troubleshooting: Check the log file, and try to resolve the problem from the error messages provided.</p>
<p>OPR Gateway.properties</p>	<p>Scans the OPR Gateway.properties file. Loglevel with values of 'Debug', 'All' or 'Off' are considered inappropriate for production environments and therefor will report error.</p> <p>Threshold Configured In: SiteScope (Log File monitor)</p>	<p>Effect on BSM: Debug log level affects the amount of output in the log which consumes more disk space and slows down the application.</p> <p>Troubleshooting: Change the configuration back to loglevel=ERROR.</p>

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
OPR SVCDiscServer	Searches for unexpected behavior, displayed as instances of ERROR, in opr-common.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Dynamic topology synchronization might not function correctly. Troubleshooting: Check the log file, and try to resolve the problem from the error messages provided.
OPR SVCDiscServer Flowtrace	Searches for unexpected behavior, displayed as instances of ERROR, in opr-common.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Flow of dynamic topology information might not function correctly. Troubleshooting: Check the log file, and try to resolve the problem from the error messages provided.
OPR SVCDiscServer.properties	Scans the OPR SVCDiscServer.properties file. Loglevel with values of 'Debug', 'All' or 'Off' are considered inappropriate for production environments and therefor will report error. Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Debug log level affects the amount of output in the log which consumes more disk space and slows down the application. Troubleshooting: Change the configuration back to loglevel=ERROR .

Service Health Application

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Service Health Admin	Searches for unexpected behavior, displayed as instances of ERROR, in bam.admin.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Service Health Administration may not function correctly. This could be caused by problems in Service Health Administration backend (for example, KPI administration, Geographical Map administration, RTSM Service Health administration actions), if some administration configuration action failed or could not be performed.
Service Health Application	Searches for unexpected behavior, displayed as instances of ERROR, in bam.app.log . The log reports problems in the Service Health application user interface. Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: This may result in tabs not being available, or system logout. Troubleshooting: Try to resolve the problem from the error messages reported in the Service Health application.
Service Health Application Front-end	Searches for unexpected behavior, displayed as instances of ERROR, in bam.app.frontend.log . The log reports problems in the Service Health application user interface. Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: This may result in tabs not being available, or system logout. Troubleshooting: Try to resolve the problem from the error messages reported in the Service Health application.

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Service Health Front-end Actions	Searches for unexpected behavior, displayed as instances of ERROR, in bam.actionbase.log . This log reports problems that impact the Service Health application. Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: This may result in tabs not being available, or system logout. Troubleshooting: Check the log file, and try to resolve the problem from the error messages provided.
Service Health BLE Plug-in	Searches for unexpected behavior, displayed as instances of ERROR, in bam.ble.plugin.log . This indicates a problem in the Business Logic Engine online loading. Threshold Configured In: SiteScope (Log File monitor)	Troubleshooting: Check Service Health for visual errors. If you find any, contact HP Software Support.
Service Health Rules	Searches for unexpected behavior, displayed as instances of ERROR, in bam.app.rules.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Some KPIs may not be calculated correctly. This could be caused by problems in Service Health Administration backend (for example, KPI administration, Geographical Map administration, RTSM Service Health administration actions), if some administration configuration action failed or could not be performed.
Service Health Business Reports	Searches for unexpected behavior, displayed as instances of ERROR, in bzd.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Problems generating Service Health reports, such as KPI Summary Report and KPI Trend Report. Troubleshooting: Check the reports for visual errors. If you find any, contact HP Software Support.

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
<p>Service Health Open API</p>	<p>Searches for unexpected behavior, displayed as instances of ERROR, in bam.open.api.log. Threshold Configured In: SiteScope (Log File monitor)</p>	<p>Effect on BSM: Errors in this log can impact the Service Health Ticker application and mobile console (handheld devices) users. Troubleshooting: Verify that you are able to use the mobile console. No other action is required. An error might indicate a Ticker client trying to retrieve a view or CI that is no longer in the RTSM.</p>
<p>Service Health Context Menu UI</p>	<p>Searches for unexpected behavior, displayed as instances of ERROR, in context.menu.log. Threshold Configured In: SiteScope (Log File monitor)</p>	<p>Effect on BSM: Problems in Service Health repositories context menu or menu items (for example, when creating new menu items, editing context menus, or cloning context menus). Problems may also occur while creating or editing the context menu or menu items. Troubleshooting: Check for visual errors. If you find any, contact HP Software Support.</p>
<p>Center High Availability</p>	<p>Searches for unexpected behavior, displayed as instances of ERROR, in bac.ha.centers.log. This log is for sticky sessions. Threshold Configured In: SiteScope (Log File monitor)</p>	<p>Effect on BSM: BSM goes down. Troubleshooting: When one BSM goes down, you can use your data with another center. Check the log file, and try to resolve the problem from the information provided.</p>

Operations Management Application

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
OPR Admin	Searches for unexpected behavior, displayed as instances of ERROR, in opr-admin.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Operations Management Administration UI might not function correctly. Troubleshooting: Check the log file, and try to resolve the problem from the error messages provided.
OPR Admin. properties	Scans the OPR Admin.properties file. Loglevel with values of 'Debug', 'All' or 'Off' are considered inappropriate for production environments and therefor will report error. Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Debug log level affects the amount of output in the log which consumes more disk space and slows down the application. Troubleshooting: Change the configuration back to loglevel=ERROR .
OPR Common	Searches for unexpected behavior, displayed as instances of ERROR, in opr-common.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Operations Management Application and Administrations UIs maight not function correctly. Troubleshooting: Check the log file, and try to resolve the problem from the error messages provided.
OPR Common. properties	Scans the OPR Common.properties file. Loglevel with values of 'Debug', 'All' or 'Off' are considered inappropriate for production environments and therefor will report error. Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Debug log level affects the amount of output in the log which consumes more disk space and slows down the application. Troubleshooting: Change the configuration back to loglevel=ERROR .

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
OPR Console	Searches for unexpected behavior, displayed as instances of ERROR, in opr-console.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Operations Management Application UI might not function correctly. Troubleshooting: Check the log file, and try to resolve the problem from the error messages provided.
OPR Console. properties	Scans the OPR Console.properties file. Loglevel with values of 'Debug', 'All' or 'Off' are considered inappropriate for production environments and therefor will report error. Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Debug log level affects the amount of output in the log which consumes more disk space and slows down the application. Troubleshooting: Change the configuration back to loglevel=ERROR .
OPR Ctxm Server. properties	Scans the OPR Ctxm server.properties file. Loglevel with values of 'Debug', 'All' or 'Off' are considered inappropriate for production environments and therefor will report error. Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Debug log level affects the amount of output in the log which consumes more disk space and slows down the application. Troubleshooting: Change the configuration back to loglevel=ERROR .
OPR Event	Searches for unexpected behavior, displayed as instances of ERROR, in opr-event-ws.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Operations Management Event Web service might not function correctly. Troubleshooting: Check the log file, and try to resolve the problem from the error messages provided.

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
OPR Event Sync Adapter.properties	Scans the OPR Event Sync Adapter.properties file. Loglevel with values of 'Debug', 'All' or 'Off' are considered inappropriate for production environments and therefor will report error. Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Debug log level affects the amount of output in the log which consumes more disk space and slows down the application. Troubleshooting: Change the configuration back to loglevel=ERROR.
OPR Event.properties	Scans the OPR Event.properties file. Loglevel with values of 'Debug', 'All' or 'Off' are considered inappropriate for production environments and therefor will report error. Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Debug log level affects the amount of output in the log which consumes more disk space and slows down the application. Troubleshooting: Change the configuration back to loglevel=ERROR.
OPR Flowtrace	Searches for unexpected behavior, displayed as instances of ERROR, in opr-flowtrace-common.log. Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Operations Management Application and Administrations UIs maight not function correctly. Troubleshooting: Check the log file, and try to resolve the problem from the error messages provided.

Portal Application

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
MyBSM	<p>Searches for unexpected behavior, displayed as instances of ERROR, in portal.log.</p> <p>Threshold Configured In: SiteScope (Log File monitor)</p>	<p>Effect on BSM: This may impact on MyBSM, and indicates problems in configuration or failed administration operations.</p> <p>Troubleshooting:</p> <ul style="list-style-type: none"> ➤ Check for any error messages in MyBSM, or for any missing portlets ➤ Check if the errors in the log reappear, or if this was a one time occurrence ➤ If you do not notice an impact, take no further action

Verticals Application

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Verticals Core	<p>Searches for unexpected behavior, displayed as instances of ERROR, in vertical.ejb.log.</p> <p>Threshold Configured In: SiteScope (Log File monitor)</p>	<p>Troubleshooting: Verify that Verticals is working correctly. Check the log file, and try to resolve the problem from the error messages provided.</p>
BSM for Siebel	<p>Searches for unexpected behavior, displayed as instances of ERROR, in siebel.ejb.log.</p> <p>Threshold Configured In: SiteScope (Log File monitor)</p>	<p>Troubleshooting: Verify that the Siebel solution is working correctly. Check the log file, and try to resolve the problem from the error messages provided.</p>
BSM for SAP	<p>Searches for unexpected behavior, displayed as instances of ERROR, in sap.ejb.log.</p> <p>Threshold Configured In: SiteScope (Log File monitor)</p>	<p>Troubleshooting: Verify that the SAP solution is working correctly. Check the log file, and try to resolve the problem from the error messages provided.</p>

System Availability Management Application

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
SAM Admin Fatal	Searches for unexpected behavior, displayed as instances of FATAL, in sam-admin.log . Threshold Configured In: SiteScope (Log File monitor)	Troubleshooting: Contact HP Software Support.
SAM Admin SiteScope Profiles on DB	Searches for unexpected behavior, displayed as instances of ERROR-Unable to get SiteScope profiles from DB, in sam-admin.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Unable to see the SiteScope profile in SAM Admin. This is probably a problem with the database or the profile ID. Troubleshooting: Check database connectivity.
SAM Admin SiteScope Profiles List	Searches for unexpected behavior, displayed as instances of Failed to retrieve SiteScope profiles list, in sam-admin.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Unable to see the SiteScope profile in SAM Admin. This is probably a problem with the database or the profile ID. Troubleshooting: Check database connectivity.

Data Processing Server Monitors

The following component monitors run on the Data Processing server:

- "Alerts Engine" on page 216
- "Bus" on page 217
- "Database Services/Partition Manager" on page 219
- "Application Engines/Service Health Engine" on page 220
- "Application Engines/Service Level Management (SLM) Engine" on page 222
- "Application Engines/Reports DB Aggregator" on page 224
- "Application Engines/CDM" on page 226
- "Modeling/RTSM" on page 226

- "Modeling/Viewing System" on page 230
- "KPI Enrichment Service Monitors" on page 231
- "Operations Management Monitors" on page 233
- "Rapid Anomaly Detection Engine Monitors" on page 237

Alerts Engine

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
BLE-BUS Connection Monitor	Monitors connection between the Business Logic Engine offline engine and the bus. This monitor is displayed as red if alerts are not sent.	Troubleshooting: Check for problems in other bus monitors and bus logs, and try to resolve the problem from the information provided.
queue/alert_engine_alert	<p>Measures the size of the queue between the Business Logic Engine and the Alerts Listener. This indicates the extent to which alert delivery is being delayed.</p> <p>Threshold Configured In: Infrastructure Settings (context alerts).</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.</p>	Troubleshooting: Check the log\alerts\alerts.ejb.log and the bus logs, and try to resolve the problem from the information provided.

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
queue/alert_engine_notification	<p>Measures the size of the queue between the Alerts Listener and the Notification Listener. This indicates the extent to which alert delivery is being delayed.</p> <p>Threshold Configured In: Infrastructure Settings (context alerts).</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.</p>	<p>Troubleshooting:</p> <ul style="list-style-type: none"> ▶ Check the SMTP/SNMP configuration in the Infrastructure Settings ▶ Check the log\alerts\alerts.ejb.log file and the bus logs, and try to resolve the problem from the information provided

Bus

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Subscriber Group	<p>Monitors subscriber related measurements.</p> <p>Threshold Configured In: Infrastructure Settings.</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.</p>	<p>Effect on BSM: If the number or size of messages waiting for processing is high, the bus may suffer from low performance. This may also cause out of memory exceptions.</p> <p>Troubleshooting: Contact your system administrator if the message threshold is met.</p>

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Broker Group	<p>Monitors the overall measurements of the broker (bytes and number of messages).</p> <p>Threshold Configured In: Infrastructure Settings.</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.</p>	<p>Effect on BSM: If the number or size of messages waiting for processing is high, the bus may suffer from low performance. This may also cause out of memory exceptions.</p> <p>Troubleshooting: Contact your system administrator if the message threshold is met.</p>
Durable Subscriber Group	<p>Monitors the number and size of messages waiting for durable subscribers in the broker.</p> <p>Threshold Configured In: Infrastructure Settings.</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.</p>	<p>Effect on BSM: If the number of messages waiting for durable subscribers is high, this affects the size and performance of the local database. The bus may suffer from low performance and may be stuck when the database files grow by more than a few gigabytes.</p> <p>Troubleshooting: Contact your system administrator if the message threshold is met.</p>

Database Services/Partition Manager

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Partition Timely Creation	<p>Verifies that partitions are created according to partitioning policy.</p> <p>Note: This monitor is displayed as red for two hours after being connected.</p>	<p>Effect on BSM: Missing partition means that there is no persistency data in the system and the reports will be empty.</p> <p>Troubleshooting: Check the following log files on the BSM Data Processing Server machine for the cause of the problem:</p> <ul style="list-style-type: none"> ➤ pmanager.log ➤ pm_statistics.log
Oversized Partitions	<p>Finds partitions with more than the allotted number of rows specified in threshold settings.</p> <p>Threshold Configured In: <HPBSM root directory>\conf\pmanager.properties, located on the Gateway Server.</p> <p>You can edit these settings in the properties file:</p> <ul style="list-style-type: none"> ➤ MAX_ROWS_PER_PARTITION. The optimal number of rows per partition that Partition Manager strives to create. ➤ WARN_ROWS_PER_PARTITION. The number of rows in the partition that generates a warning. ➤ ERROR_ROWS_PER_PARTITION. The number of rows in the partition that generates an error. 	<p>Effect on BSM: Low performance in the reports caused by too many rows in data tables.</p> <p>Troubleshooting:</p> <ol style="list-style-type: none"> 1. Change or tune the Partition Manager policy according to the EPS default values in <HPBSM root directory>\conf\pmanager.properties file. 2. Restart the Partition Manager.

Application Engines/Service Health Engine

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
BLE Online Monitor	<p>Monitors Business Logic Engine online calculations.</p> <p>Included Measurements:</p> <ul style="list-style-type: none"> ▶ Size of Model. Percentage of model size relative to the maximum capacity. ▶ DB Availability. Verifies connection to the database. ▶ Bus Connectivity. Verifies connection to the bus. ▶ Calculation Duration. Average calculation time. <p>Threshold Configured In: Infrastructure Settings. To configure threshold, navigate to Admin > Platform > Setup and Maintenance > Infrastructure Settings. Choose Foundations, select Distributed Online Business Logic Engine - Supervisor and modify Maximum interval between two consecutive model calculations.</p>	<ul style="list-style-type: none"> ▶ Size of Model. If the model is too large, it causes performance problems, out of memory exceptions, and Service Health might not be available. Decrease the model to a supported size. You can also switch to a larger deployment (in case you are not using it already). ▶ DB Availability. If there is no connection to the database, persistency, repositories, and settings are affected. Ask your database/network administrator to check the database connection and/or any network issues. ▶ Bus Connectivity. If there is no connection to the bus, Business Logic Engine does not receive samples and is unable to send samples to the bus. Check the bus log file for the cause of the problem. ▶ Calculation Duration. Service Health responsiveness is affected if the calculation takes too long, since no requests from Service Health are processed during the calculation. Slow calculation might be caused by a large model, very high EPS, or if the log level is set to DEBUG.

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Service Health BLE Plug-in	Searches for unexpected behavior, displayed as instances of ERROR, in bam.ble.plugin.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Service Health cannot get status information from the online engine.
Service Health Rules	Searches for unexpected behavior during execution of Service Health rules, displayed as instances of ERROR, in bam.app.rules.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Indicator statuses might not be calculated, or might be calculated incorrectly. This is visible in the System Health application. Troubleshooting: Check for the root cause of the problem in the log file.

Application Engines/Service Level Management (SLM) Engine

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
BLE Offline Tasks	<p>Indicates whether the time taken to perform the SLM tasks took longer than the time allotted in Infrastructure Settings.</p> <p>Included Measurements:</p> <ul style="list-style-type: none"> ➤ Delayed Tasks. Shows whether there are delayed or failed SLM calculation tasks. ➤ Cycle Time. Shows the percentage of the overall measurement period used to complete calculation of ongoing SLM tasks. <p>Threshold Configured In: Infrastructure Settings. To configure threshold, navigate to Admin > Platform > Setup and Maintenance > Infrastructure Settings. Choose Foundations, select Offline Aggregator and modify Monitor Threshold for SLM Aggregator.</p>	<p>Effect on BSM: No data in the database for reports for the latest SLM calculation. This can result in slow database performance, task failure, invalid SLM configuration, database access problems, and RTSM access problems.</p> <p>Troubleshooting: Check the following log files for the cause of the problem:</p> <ul style="list-style-type: none"> ➤ NOAScheduler.log ➤ bambino.log ➤ BambinoStatistics.log ➤ offline.engine.all.log

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
BLE Offline Monitor	<p>Monitors Business Logic Engine offline calculations.</p> <p>Included Measurements:</p> <ul style="list-style-type: none"> ▶ DB Availability. Verifies connection to the database. ▶ Bus Connectivity. Verifies connection to the bus. ▶ Persistency. Indicates the number of failures in saving persistency data. ▶ Max Task Duration. Displays the duration of the longest task over the time configured in Infrastructure Settings, indicating whether or not the SLM calculation is too slow. ▶ Data Stream Fuse Violations. Indicates performance problems due to the amount of data queried for SLM calculations. <p>Threshold Configured In: Infrastructure Settings. To configure threshold, navigate to Admin > Platform > Setup and Maintenance > Infrastructure Settings. Choose Foundations, select Offline Business Logic Engine and modify Maximum number of rows that the Data Streamer can count.</p>	<p>Effect on BSM: No data in the database for reports for the latest SLM calculation. This can result in no connection to the database, failure to connect to the bus, low calculations performance, and no memory space to calculate the SLA.</p> <p>Troubleshooting: For low calculations performance, check the BambinoStatistics.log for bottlenecks.</p> <p>For no memory space to calculate the SLA:</p> <ul style="list-style-type: none"> ▶ Check bambino.log and BambinoStatistics.log. ▶ Increase memory for processes in the mercury_offline_engine_vm_params.ini file and the fuse setting (BSM Admin Infrastructure settings UI). ▶ Limit the number of SLAs that are calculated simultaneously in Admin > Platform > Setup and Maintenance > Infrastructure Settings.

Application Engines/Reports DB Aggregator

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
DB Aggregator	<p>Indicates whether the time to perform the DB Aggregation task took longer than the time configured in Infrastructure Settings.</p> <p>Included Measurements:</p> <ul style="list-style-type: none"> ➤ Delayed Tasks. Displays whether delayed or failed tasks are found. ➤ Cycle Time. Shows the percentage of the overall measurement period used to complete aggregation calculations. <p>Threshold Configured In: Infrastructure Settings.</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.</p>	<p>Effect on BSM: No data in the database for reports using aggregation data. This can result in slow database performance, task failure, invalid SLM configuration, database access problems, and RTSM access problems.</p> <p>Troubleshooting: Check the following log files for the cause of the problem:</p> <ul style="list-style-type: none"> ➤ NOAScheduler.log ➤ bambino.log ➤ NOAStatistics.log ➤ offline.engine.all.log

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Validator	<p>Responsible for the creation of DB Aggregation and SLM tasks.</p> <p>Included Measurements:</p> <ul style="list-style-type: none"> ▶ Validation Time. Checks whether validation ran within the time frame defined in the Offline Aggregation settings. <p>Threshold Configured In: Infrastructure Settings.</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.</p>	<p>Effect on BSM: No data in the database for reports using aggregation data.</p> <p>Troubleshooting: Check the following log files for the cause of the problem:</p> <ul style="list-style-type: none"> ▶ NOAValidator.log ▶ offline.engine.all.log
Scheduler	<p>Schedules when the DB Aggregator and SLM tasks are performed.</p> <p>Included Measurements:</p> <ul style="list-style-type: none"> ▶ Threads Alive. Checks for active threads in the offline aggregation scheduler. 	<p>Effect on BSM: No data in the database for reports using aggregation data. This can result in database and RTSM access problems.</p> <p>Troubleshooting: Check the following log files for the cause of the problem:</p> <ul style="list-style-type: none"> ▶ NOAScheduler.log ▶ bambino.log ▶ NOAStatistics.log ▶ offline.engine.all.log

Application Engines/CDM

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Adapters Framework	Searches for unexpected behavior, displayed as instances of ERROR, in bam.shared.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Not relevant for BSM 9.10, since all data collectors send their topology directly to RTSM (which previously was done by adapters).

Modeling/RTSM

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Model Objects Quota and Count	Compares current CI count with the CI quota. Threshold Configured In: Infrastructure Settings. To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.	Effect on BSM: If the quota is exceeded, no more CIs and links can be added. Troubleshooting: Increase the quota, delete unnecessary CIs, or refine the discovery process so it discovers less data.
TQL Quota and Count	Compares current TQL count with the TQL quota. Threshold Configured In: Infrastructure Settings. To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.	Effect on BSM: If the quota is exceeded, no new active TQLs can be added. Troubleshooting: Increase the quota or delete unnecessary TQLs.

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Oversized TQLs	<p>Displays TQLs that are larger than the size permitted by the configured threshold.</p> <p>Threshold Configured In: Infrastructure Settings.</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.</p>	<p>Effect on BSM: If the TQL result is larger than the threshold, the TQL is deactivated.</p> <p>Troubleshooting: Change the TQL definition.</p>
Availability and Performance	<p>Checks system availability and response time. If response time exceeds 2 seconds, monitor status changes to Warning. If response time exceeds 15 seconds, monitor status changes to Error.</p> <p>Included Measurements:</p> <ul style="list-style-type: none"> ▶ Run AdHoc TQL. Checks how long the Run AdHoc TQL operation takes. ▶ Load ClassModel. Checks how long the Load ClassModel operation takes. <p>Threshold Configured In: Infrastructure Settings.</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.</p>	<p>Effect on BSM: System availability issues and slow response time affect BSM performance.</p> <p>Troubleshooting: Check the log files for the cause of the problem.</p>

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
DB - Could not reset timeout because the object is not monitored	Searches for Couldn't reset timeout because the object isn't monitored in cmdb.log . Threshold Configured In: SiteScope (Log File monitor)	Troubleshooting: If this error is registered in the log file, it means there are problems in the database. Contact your database administrator for assistance.
DB - Failed to borrow object from pool	Searches for Failed to borrow object from pool in cmdb.log . Threshold Configured In: SiteScope (Log File monitor)	Troubleshooting: If this error is registered in the log file, it means there are problems in the database. Contact your database administrator for assistance.
DB - Failed to create a connection	Searches for Failed to create a connection for in cmdb.log . Threshold Configured In: SiteScope (Log File monitor)	Troubleshooting: If this error is registered in the log file, it means there are problems in the database. Contact your database administrator for assistance.
Notification - Cannot Publish	Searches for cannot publish in cmdb.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM if this error is registered in the log file: There are no notifications about active TQLs or model updates, and BSM applications and Service Health are not notified about changes in topology (such as added hosts or business transactions). Troubleshooting: Check the bus log for problems.

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Notification - Cannot get notifications from the BUS	Searches for error occurred during receive of JMS message in cmdb.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM if this error is registered in the log file: There are no notifications about active TQLs or model updates, and BSM applications and Service Health are not notified about changes in topology (such as added hosts or business transactions). Troubleshooting: Check the bus log for the cause of the problem.
Performance - Request Timeout	Searches for Request Timeout in cmdb.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM if this error is registered in the log file: This error may indicate a general problem, or it may have been caused by a temporary issue such as running a large number of TQLs. Troubleshooting: Check the log file for the cause of the problem.

Modeling/Viewing System

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
All Symbols Quota and Count	<p>Compares current symbols count with symbols quota. You can create a view on top of a TQL. Each element in the view tree is called a symbol. The quota is determined in the settings.</p> <p>Threshold Configured In: Infrastructure Settings.</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.</p>	<p>Effect on BSM: If the quota is exceeded, no new active views can be created.</p> <p>Troubleshooting: Deactivate views or increase the quota.</p>
Views Quota and Count	<p>Compares current views count with views quota.</p> <p>Threshold Configured In: Infrastructure Settings.</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.</p>	<p>Effect on BSM: If the quota is exceeded, no new views can be created.</p> <p>Troubleshooting: Deactivate views or increase the quota.</p>
Oversized Views	<p>Checks for views that are larger than the threshold configured in Infrastructure Settings.</p> <p>Threshold Configured In: Infrastructure Settings.</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.</p>	<p>Effect on BSM: Oversized views are deactivated.</p> <p>Troubleshooting: Change the view definition.</p>

KPI Enrichment Service Monitors

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
KES Availability	<p>Monitors that Assignment Mechanism is up and running for each customer. For details, see "Assignment Mechanism" in <i>Using Service Health</i>.</p> <p>Included Measurements:</p> <ul style="list-style-type: none"> ➤ KES Availability per customer <p>The monitor measurements list is dynamic and determined according to the number of customers running Assignment Mechanism service on this Data Processing Server.</p> <p>For example: If a Data Processing Server is running KES service for customers 1-3, the monitor will be deployed with three measurements:</p> <ul style="list-style-type: none"> ➤ KES Availability for customer 1 ➤ KES Availability for customer 2 ➤ KES Availability for customer 3 	<p>Troubleshooting: Verify that KES service is running. Check the following log files in <HPBSM root directory>\log\EJBContainer for the cause of the problem:</p> <ul style="list-style-type: none"> ➤ kes.server.log ➤ kes.manager.log

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
<p>KES Content</p>	<p>Monitors that Assignment Mechanism content is valid: checks that there are no invalid SLM/Service Health KPI/Hi assignments for each customer running Assignment Mechanism.</p> <p>Included Measurements</p> <ul style="list-style-type: none"> ➤ SLM KES content per customer ➤ DASHBOARD KES content per customer <p>The monitor measurements list is dynamic and determined according to the number of customers running KES service on this data processing server.</p> <p>For example: In a data processing server running KES service for customers 1-2, the monitor will be deployed with four measurements:</p> <ul style="list-style-type: none"> ➤ SLM KES content for customer 1 ➤ DASHBOARD KES content for customer 1 ➤ SLM KES content for customer 2 ➤ DASHBOARD KES content for customer 2 	<p>If there is an invalid assignment in the SLM or Service Health application for a customer, the KPI/Hi assignment will be ignored by the assignment mechanism and KPIs/HIs may not be assigned for CIs. (In case of overriding invalid assignment, the overridden assignment HIs/KPIs will be assigned to CIs instead.) Locate the assignment and fix it according to validation error in the UI.</p>

Operations Management Monitors

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
OPR Backend	Searches for unexpected behavior, displayed as instances of ERROR, in opr-backend.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Operations Management event processing (such as Topology-base event correlation, ETI resolution, CI resolution) might not function correctly. Troubleshooting: Check the log file, and try to resolve the problem from the error messages provided.
OPR Backend Boot	Searches for unexpected behavior, displayed as instances of ERROR, in opr-backend-boot.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Startup of the Operations Management OPR-Backend process might not function correctly. Troubleshooting: Check the log file, and try to resolve the problem from the error messages provided.
OPR Backend Shutdown	Searches for unexpected behavior, displayed as instances of ERROR, in opr-backend_shutdown.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Shutdown of the Operations Management OPR-Backend process might not function correctly. Troubleshooting: Check the log file, and try to resolve the problem from the error messages provided.

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
OPR Backend.properties	Scans the OPR Backend.properties file. Loglevel with values of 'Debug', 'All' or 'Off' are considered inappropriate for production environments and therefor will report error. Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Debug log level affects the amount of output in the log which consumes more disk space and slows down the application. Troubleshooting: Change the configuration back to loglevel=ERROR .
OPR CiResolver	Searches for unexpected behavior, displayed as instances of ERROR, in opr-ciresolver.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Operations Management CI Resolver might not function correctly. Troubleshooting: Check the log file, and try to resolve the problem from the error messages provided.
OPR Common	Searches for unexpected behavior, displayed as instances of ERROR, in opr-common.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Operations Management event processing, RTSM connections and database transactions might not function correctly. Troubleshooting: Check the log file, and try to resolve the problem from the error messages provided.
OPR Common.properties	Scans the OPR Common.properties file. Loglevel with values of 'Debug', 'All' or 'Off' are considered inappropriate for production environments and therefor will report error. Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Debug log level affects the amount of output in the log which consumes more disk space and slows down the application. Troubleshooting: Change the configuration back to loglevel=ERROR .

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
OPR EPI Server	Searches for unexpected behavior, displayed as instances of ERROR, in opr-epi-server.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Operations Management Event Processing Interface might not function correctly. Troubleshooting: Check the log file, and try to resolve the problem from the error messages provided.
OPR EPI Server.properties	Scans the OPR Server.properties file. Loglevel with values of 'Debug', 'All' or 'Off' are considered inappropriate for production environments and therefor will report error. Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Debug log level affects the amount of output in the log which consumes more disk space and slows down the application. Troubleshooting: Change the configuration back to loglevel=ERROR .
OPR Event Sync Adapter	Searches for unexpected behavior, displayed as instances of ERROR, in opr-event-sync-adapter.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Operations Management communication between the Data Processing Server and the Gateway Servers might not function correctly. Troubleshooting: Check the log file, and try to resolve the problem from the error messages provided.
OPR Event Sync Adapter.properties	Scans the OPR Event Sync Adapter.properties file. Loglevel with values of 'Debug', 'All' or 'Off' are considered inappropriate for production environments and therefor will report error. Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Debug log level affects the amount of output in the log which consumes more disk space and slows down the application. Troubleshooting: Change the configuration back to loglevel=ERROR .

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
<p>OPR Flowtrace</p>	<p>Searches for unexpected behavior, displayed as instances of ERROR, in opr-flowtrace-common.log.</p> <p>Threshold Configured In: SiteScope (Log File monitor)</p>	<p>Effect on BSM: Flow of Operations Management events through the gateway adapter might not function correctly.</p> <p>Troubleshooting: Check the log file, and try to resolve the problem from the error messages provided.</p>
<p>OPR Topologysync.properties</p>	<p>Scans the OPR Topologysync.properties file. Loglevel with values of 'Debug', 'All' or 'Off' are considered inappropriate for production environments and therefore will report error.</p> <p>Threshold Configured In: SiteScope (Log File monitor)</p>	<p>Effect on BSM: Debug log level affects the amount of output in the log which consumes more disk space and slows down the application.</p> <p>Troubleshooting: Change the configuration back to loglevel=ERROR.</p>

Rapid Anomaly Detection Engine Monitors

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Service Health Analyzer Engine	Monitors SHA Engine. Included Measurements: <ul style="list-style-type: none"> ▶ Cycle Time. Shows the percentage of the overall measurement period used to complete calculation. The default threshold is 66.7%. ▶ Delayed Tasks. Shows if there are delayed tasks. ▶ Worst Task Performance ▶ Worst Method Performance ▶ Open Anomalies (for information only) ▶ Traced Metrics. Shows amount of traced metrics (for information only) 	Effect on BSM: Stronger server is needed.
SHA Engine log monitor	Searches for unexpected behavior, displayed as instances of error.	Effect on BSM: Process may not function correctly. Troubleshooting: Check the log file and try to resolve the problem from the error message provided.
SHA Engine General log monitor	Searches for unexpected behavior, displayed as instances of error.	Effect on BSM: Process may not function correctly. Troubleshooting: Check the log file and try to resolve the problem from the error message provided.

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
SHA Engine Statistics log monitor	Monitors the statistics for the pi_engine process.	<p>Effect on BSM: Some data might not be available in SHA.</p> <p>Troubleshooting: Verify the BSM deployment type, memory (RAM), and expected load (reported samples per second) using the BSM capacity calculator. This type of exception usually occurs if BSM is installed on hardware that has insufficient resources for the current load.</p>
SHA Application General log monitor	Searches for unexpected behavior, displayed as instances of error.	<p>Effect on BSM: Process may not function correctly.</p> <p>Troubleshooting: Check the log file and try to resolve the problem from the error message provided.</p>


BPI Server Monitors

The following component monitors run on the BPI Server:

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Data Samples Provider	Searches for [SEVERE ERROR] in bia_bacdatasamples0_0.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: BPI data samples might not be sent to BSM. Information in the BPI health page and Service Health is not updated, and the current status of Health Indicators and KPIs might be incorrect. Troubleshooting: <ul style="list-style-type: none"> ➤ Check the error message, and try to resolve the problem from the information provided ➤ Check that the Web data entry component of BSM is working correctly ➤ Restart the BPI Server ➤ If the problem persists, check with BSM Administrator
Notification Server	Searches for [SEVERE ERROR] in bia_notify0_0.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: BPI business process threshold violation notifications might not be sent to the users specified using BPI notification administration in BSM. Troubleshooting: <ul style="list-style-type: none"> ➤ Check the error message, and try to resolve the problem from the information provided ➤ Check that the BPI notification mail server is configured correctly ➤ Restart the BPI Server ➤ If the problem persists, check with BSM Administrator

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
<p>Servlet Engine</p>	<p>Searches for [SEVERE ERROR] in bia_tomcat0_0.log.</p> <p>Threshold Configured In: SiteScope (Log File monitor)</p>	<p>Effect on BSM: The BPI landing pages, monitor definer, process repository explorer, and BPI notification might not function properly in BSM.</p> <p>Troubleshooting:</p> <ul style="list-style-type: none"> ▶ Check the error message, and try to resolve the problem from the information provided ▶ Restart the BPI Server ▶ If the problem persists, check with BSM Administrator
<p>CI Status Poller</p>	<p>Searches for [SEVERE ERROR] in bia_adaptor_framework0_0.log.</p> <p>Threshold Configured In: SiteScope (Log File monitor)</p>	<p>Effect on BSM: The CI status poller component in BPI might not be able to obtain the current status of business activities, resulting in the current status not being visible in the BPI health page. The blocked and impeded process instances count might also be incorrect.</p> <p>Troubleshooting:</p> <ul style="list-style-type: none"> ▶ Check the error message, and try to resolve the problem from the information provided ▶ Restart the BPI Server ▶ If the problem persists, check with BSM Administrator

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
JMS Business Event Handler	Searches for ERROR in Rolling_Adaptor_BIAJMSEngine Adaptor.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: BPI events that are being delivered using a JMS queue are not being processed. The data shown in the BPI application and the statuses of BPI KPIs and Health Indicators might be incorrect. Troubleshooting: <ul style="list-style-type: none">➤ Check the error message, and try to resolve the problem from the information provided➤ Check the configuration properties of the JMS Business Event Handler and that the BPI Impact Engine is started➤ Restart the BPI Server➤ If the problem persists, check with BSM Administrator
Process Repository	Searches for [SEVERE ERROR] in bia_model_repository0_0.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: The BPI Modeler might fail to load or is unable to correctly modify BPI definitions. The BPI health pages might also fail to display process maps. Troubleshooting: <ul style="list-style-type: none">➤ Check the error message, and try to resolve the problem from the information provided➤ Check that the BPI database configured for BSM is running correctly➤ Restart the BPI Server➤ If the problem persists, check with BSM Administrator

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
<p>Monitor Engine</p>	<p>Searches for [SEVERE ERROR] in bia_metric_engine0_0.log.</p> <p>Threshold Configured In: SiteScope (Log File monitor)</p>	<p>Effect on BSM: BPI Monitor statistics and the current status KPIs might be incorrect.</p> <p>Troubleshooting:</p> <ul style="list-style-type: none"> ▶ Check the error message, and try to resolve the problem from the information provided ▶ Check that the BPI instance database is running correctly ▶ Restart the BPI Server ▶ If the problem persists, check with BSM Administrator
<p>Business Event Handler</p>	<p>Searches for ERROR in Rolling_Adaptor_BIAEngine Adaptor.log.</p> <p>Effect on BSM: BPI events might not be processed, and the data displayed in the BPI application and the statuses of BPI KPIs might be incorrect.</p> <p>Threshold Configured In: SiteScope (Log File monitor)</p>	<p>Troubleshooting:</p> <ul style="list-style-type: none"> ▶ Check the error message, and try to resolve the problem from the information provided ▶ Check the configuration properties of the Business Event Handler and that the BPI Impact Engine is started ▶ Restart the BPI Server ▶ If the problem persists, check with BSM Administrator
<p>Web Services Provider</p>	<p>Searches for [SEVERE ERROR] in bia_webservices0_0.log.</p> <p>Threshold Configured In: SiteScope (Log File monitor)</p>	<p>Effect on BSM: None</p>

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Business Impact Engine	Searches for [SEVERE ERROR] in bia_bce0_0.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Statistics for BPI processes and activities, and data shown in the BPI application and the statuses of BPI KPIs and health indicators might be incorrect. Troubleshooting: <ul style="list-style-type: none"> ➤ Check the error message, and try to resolve the problem from the information provided ➤ Check that the BPI instance database is running correctly ➤ Restart the BPI Server ➤ If the problem persists, check with BSM Administrator
Admin Server	Searches for [SEVERE ERROR] in bia_adminserver0_0.log . Threshold Configured In: SiteScope (Log File monitor)	Effect on BSM: Possibly unable to start or stop BPI components on the BPI server. Troubleshooting: <ul style="list-style-type: none"> ➤ Check the error message, and try to resolve the problem from the information provided ➤ Restart the BPI Server ➤ If the problem persists, check with BSM Administrator

Data Collectors

Following are the data collectors that run as part of BSM:

- "BPM Data Collector" on page 244
- "SiteScope Data Collector" on page 246
- "Discovery Probe Data Collector" on page 247
- "RUM Data Collector" on page 248

BPM Data Collector

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
<p>BPM Last Ping Time</p>	<p>Reports how much time has passed since the last time BPM data collectors requested job updates from BSM.</p> <p>If BPM last ping time exceeds 5 minutes, monitor status changes to Warning. If BPM last ping time exceeds 10 minutes, monitor status changes to Error.</p> <p>Threshold Configured In: Infrastructure Settings.</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.</p>	<p>Effect on BSM: BPM does not get configuration updates.</p> <ul style="list-style-type: none"> ➤ If the other BPM monitor is also red, this indicates that BPM is unable to connect to or send a request to BSM, or that BPM is down. ➤ If this monitor is constantly red, the BPM is unable to retrieve configuration updates. ➤ If this monitor is sometimes green and sometimes red, the job poll interval configuration (BPM configuration) may be higher than 5 minutes. <p>Troubleshooting:</p> <ul style="list-style-type: none"> ➤ If this monitor is not constantly red: <ul style="list-style-type: none"> ➤ Check the job poll interval in BPM, and reduce it if necessary. ➤ Increase the Error and Warning thresholds for BPM Last Ping Time in Infrastructure Settings. ➤ If this monitor is constantly red, check for connection errors in the BPM logs (<code>..\workspace\commcenter\commcenter.txt</code>).

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
BPM Last Reported Data Time	<p>Measures how much time has passed since the last time BPM data collectors sent samples to BSM. If this time exceeds 80 minutes, monitor status changes to Warning.</p> <p>Threshold Configured In: Infrastructure Settings.</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.</p>	<p>Effect on BSM: BPM samples are not entered into BSM.</p> <ul style="list-style-type: none"> ▶ If the other BPM monitor is also red, this indicates that BPM is unable to connect to or send a request to BSM, or that BPM is down. ▶ If this monitor is constantly red, the BPM is unable to send samples to BSM. <p>Troubleshooting:</p> <ul style="list-style-type: none"> ▶ Check for connection errors in the BPM logs (..\workspace\agent1\data\data_depot.txt) ▶ Increase the Warning threshold for BPM Last Reported Data Time in Infrastructure Settings.

SiteScope Data Collector

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
SiteScope status on <SiteScope instance>	<p>Measures the overall status of the SiteScope data collector.</p> <p>Included Measurements:</p> <ul style="list-style-type: none"> ▶ Last Heartbeat. Indicates the time of the most recent sample received from SiteScope that indicates the basic availability (i.e., heartbeat) of the system. ▶ Health Status. Indicates the status of the SiteScope Health group, and number of monitors in the group with error status. <p>Note: Both measurements are monitored only if using SiteScope version 9.0 or higher. If a previous version is installed, only the Last Heartbeat measurement is monitored.</p> <p>Threshold Configured In: Infrastructure Settings.</p> <p>To access, go to Admin > Platform > Setup and Maintenance > Infrastructure Settings and search under System Health or the applicable component application.</p>	<p>Troubleshooting:</p> <ul style="list-style-type: none"> ▶ Last Heartbeat. Check that SiteScope is up and running. In SAM Admin, check the connection between BSM and SiteScope. Check the BSM status and that BSM components are running. ▶ Health Status. In SiteScope, check the SiteScope Health group, and check the SiteScope Progress Report (in SiteScope versions 10.00 or earlier) or the SiteScope progress pages (in Server Statistics > General/Running Monitors tabs in SiteScope 10.10 or later). Check the troubleshooting for SiteScope Health monitors in <i>Using SiteScope</i> in the SiteScope Help.

Discovery Probe Data Collector





Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
Discovery Probe status on <Discovery Probe instance>	<p>Receives discovery tasks from the server, dispatches them, and sends the results back to the CMDB through the server.</p> <p>Included Measurements:</p> <ul style="list-style-type: none"> ▶ Last Report Time. The most recent report time. ▶ Amount of Reported CIs. The number of CIs reported by the probe. ▶ Last Access Time. The most recent time the probe was accessed. 	<p>Effect on BSM: No new discovery data is entered into BSM. There is an indication of a problem is if the last report time is earlier than the scheduled discovery time.</p> <p>Troubleshooting: Check that the discovery probe is running and connected to BSM.</p>

RUM Data Collector

Monitor Name	Description	Effect on BSM if there is a problem/Troubleshooting
RUM Status on <RUM Engine Instance Name>	<p>Displays the aggregated status of the Real User Monitor data collector.</p> <p>Included Measurements:</p> <ul style="list-style-type: none"> ▶ RUM Engine. Aggregated status of the Real User Monitor engine monitors. ▶ RUM Probe IP. Aggregated status of the Real User Monitor probe with the specified IP address. Each probe has its own entry. ▶ Database. Aggregated status of Real User Monitor internal DB monitors. ▶ Samples to Business Service Management server. Aggregated status of the Real User Monitor samples sent to BSM. <p>Threshold Configured In: Real User Monitor internal configuration.</p>	<p>Troubleshooting: If the Real User Monitor data collector's status is problematic, refer to the Real User Monitor web console for troubleshooting. For details, see "Monitoring the Health of HP Real User Monitor Components" in the <i>Real User Monitor Administration</i> PDF.</p>

Component and Monitor Status Indicators

The following table displays a colored icon and a description of its status, as displayed on both the Inventory tab and the Monitors table in the System Health Dashboard right pane:

Status	Description
	The component and all subcomponents are working properly (status is good).
	The component or a subcomponent has a critical problem (status is error). A red indicator is accompanied by an x symbol. It is recommended that you drill down in the component to identify its specific problematic monitors.
	The component or a subcomponent has a non-critical problem, or did not receive an answer from the server (status is warning). The yellow indicator is accompanied by a ! symbol.
	There is no data available for the monitors. Displayed if the monitors have not yet run. The gray indicator is accompanied by a - symbol.

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

System Health User Interface

This section includes (in alphabetical order):

- ▶ Inventory Tab on page 250
- ▶ Log Manager on page 254
- ▶ System Health Dashboard on page 257
- ▶ System Health Setup Wizard on page 269
- ▶ Toolbar on page 276

Inventory Tab

This tab displays the status of the BSM servers and their respective components in table format. It enables you to compare the performance of servers of the same type and to view statuses in a flat view, versus the hierarchal view of the Dashboard.

To access	Click the Inventory tab on the System Health interface.
Important information	<p>In addition to fields representing the monitors and components displayed on the System Health Dashboard, the tables contain the following fields:</p> <ul style="list-style-type: none"> ▶ Name. The name of the server. ▶ Type. The type of server (appears only for Gateway and Processing server tables). ▶ Status. The overall status of the machine, indicated by a colored icon. For details on the colored icons, see "Component and Monitor Status Indicators" on page 249. <p>Descriptions of the monitors are displayed on the Monitor Details pane.</p>
See also	"System Health Monitors" on page 181

Gateway Machines Table

Displays information about the Gateway machines being monitored by System Health, and their subcomponents.

To access	Click the Inventory tab on the System Health interface.
Important information	<ul style="list-style-type: none"> ➤ Click the arrows in the header to expand or collapse the table. ➤ The subcomponents' status is indicated by a colored ball icon. For details on the status represented by each color, see "Component and Monitor Status Indicators" on page 249. ➤ Details on the selected subcomponent appear in the <Subcomponent Name> Details table. Note: The cell names are identical to the corresponding component or subcomponent displayed on the System Health Dashboard.
See also	<ul style="list-style-type: none"> ➤ "System Health Displays" on page 151 ➤ "BSM Components" on page 178 ➤ "System Health Monitors" on page 181

Processing Machines Table

Displays information about the Data Processing machines being monitored by System Health, and their subcomponents.

To access	Click the Inventory tab on the System Health interface.
Important information	<ul style="list-style-type: none"> ➤ Click the arrows in the header to expand or collapse the table. ➤ The subcomponents' status is indicated by a colored ball icon. ➤ Details on the selected subcomponent appear in the <Subcomponent Name> Details table. <p>Note: The cell names are identical to the corresponding component or subcomponent displayed on the System Health Dashboard.</p>
See also	<ul style="list-style-type: none"> ➤ "System Health Displays" on page 151 ➤ "BSM Components" on page 178 ➤ "System Health Monitors" on page 181


<Subcomponent Name> Details Table

Displays information about the specific component or subcomponent selected in the Gateway Machines table or the Processing Machines table.







To access	Click the Inventory tab on the System Health interface.
Important information	<ul style="list-style-type: none"> ▶ The status of the subcomponent and its monitors are indicated by a either a colored icon, or, where applicable, a numerical value in the color indicating its status. For details on the colors' status, see "Component and Monitor Status Indicators" on page 249. ▶ The cell headings correspond to the monitors running on the selected component. The Name and Status cell headings display the name of the machine and its overall status, respectively. ▶ The Monitor Details pane provides additional information on the monitor selected in the <Subcomponent Name> Details table.
See also	<ul style="list-style-type: none"> ▶ "System Health Monitors" on page 181 ▶ "Monitors Table" on page 258

Log Manager

Displays the log file output associated with the various components being monitored by System Health.

To access	Click the Log Manager tab on the System Health interface.
Important information	<ul style="list-style-type: none"> ▶ You can view a log file by selecting a component in the Log Bundles pane and performing one of the following actions: <ul style="list-style-type: none"> ▶ Double-click. ▶ Drag and drop it into the Main pane. ▶ Click the Retrieve Logs  button. ▶ You can search for a string in the Main pane by selecting any point in the pane and typing the string you want to find. You can also search the content of a set of logs by saving the output to a .txt file and performing a search.
See also	"Log Manager Tab" on page 156

User interface elements are described below:

UI Element (A-Z)	Description
	<p>Retrieves logs for the specified entities. You can retrieve log files by selecting a specific file, a bundle, or a machine.</p> <p>Note:</p> <ul style="list-style-type: none"> ▶ You can also view log files by dragging the selected entity to the main frame. ▶ The Log Manager cannot display a log file larger than 1 MB. If you try to retrieve a log file larger than this, a message is displayed prompting you to download the file to your local machine.
	<p>Saves the selected log files.</p> <ul style="list-style-type: none"> ▶ When selecting this button in the main frame, the currently displayed logs are saved. ▶ When selecting this button on the Log Bundles pane, the selected entities are saved, without being displayed in the main frame. This option is useful if you are saving a large output of data, or if you want to perform a complex search on the data output.
	<p>Indicates a log bundle or machine whose content has been collapsed or not expanded in the Log Bundles hierarchical tree.</p> <p>Note: This is the default view in the Log Bundles pane.</p>
	<p>Indicates a log bundle or machine whose content has been expanded in the Log Bundles hierarchical tree.</p>
	<p>Indicates a log file. You can view a log file in one of the following ways:</p> <ul style="list-style-type: none"> ▶ Double-click the log file ▶ Drag and drop the log file into the main pane ▶ Select the log file and click the Retrieve Logs  button.

UI Element (A-Z)	Description
<tab #>	<p>Indicates a selection of any combination of bundles, machines, or log files. The tabs are numbered chronologically, according to the number of retrieval actions you have performed.</p> <p>Note: The specific logs displayed in the tab are listed at the top of the pane. If more than 5 logs have been retrieved, the message, Assorted logs (more than 5) is displayed in place of the log list.</p>
From	Select a date and time from which the log data is to begin being displayed.
To	Select a date and time until which the log data is to be displayed.

System Health Dashboard

Enables you to view BSM components and their status, including information on the properties and monitors associated with the components. This is the default display when you access System Health.

To access	Select Admin > Platform > Setup and Maintenance > System Health
Important information	<p>The System Health Dashboard consists of the following areas:</p> <ul style="list-style-type: none"> ▶ Left pane ▶ Right pane ▶ Monitors table ▶ General table <p>You can perform actions on the System Health Dashboard using the toolbar above the left pane. For details, see "Toolbar" on page 276.</p>
See also	<ul style="list-style-type: none"> ▶ "How to Deploy and Access System Health" on page 162 ▶ "System Health Setup Wizard" on page 269 ▶ "System Health Displays" on page 151

Left Pane

Displays a map of the databases, servers, data collectors, and mediators and load balancers (if they exist in your deployment) deployed on BSM. For details, see "Map of BSM System and Components" on page 262.

Important information	The status of the components is indicated by the color of the box surrounding the icon and the accompanying symbol. For details, see "Component Status and Description" on page 263.
See also	"System Health Displays" on page 151

Right Pane

Displays information on components selected in the left pane.





Important information	<p>The right pane consists of the following tables:</p> <ul style="list-style-type: none"> ▶ Monitors. Displays information about the monitors and subcomponents on the highlighted component in the left pane. ▶ General. Displays information about the properties of the highlighted server in the left pane. ▶ Data Collector Details. Displays information about the data collector highlighted in the left pane.
See also	"System Health Displays" on page 151





Monitors Table

Displays information on the monitors running on the selected component in the System Health Dashboard.

Important information	Click the arrows in the header to expand or collapse the table.
See also	"BSM Components" on page 178

User interface elements are described below:

UI Element (A-Z)	Description
	Disables the selected monitor.
	Reactivates the selected monitor's schedule.
	Runs the selected monitor immediately. The monitor must first be enabled for you to use this option.
	Expands the list of monitors to list all monitors and measurements for that object. This is the default view.

UI Element (A-Z)	Description
	Collapses the list of monitors to display only the monitors and hide the monitor measurements.
	Refreshes the list of monitors to display the latest status for the monitors.
	An individual monitor that is running on the selected component.
	A group of monitors that are running on the selected component.
Last Updated	Indicates the last time that the monitor ran.
Monitor Details	<p>Contains the following fields:</p> <ul style="list-style-type: none"> ▶ Description. Describes the selected monitor. ▶ Additional Information. Displays a text string result of the selected monitor's output. ▶ Value. Displays a numerical result of the selected monitor's output. <p>Note: Not all fields are displayed for every monitor.</p>
Monitor/Group Name	The name of the monitor or group of monitors running on the component selected in the left pane.
Status	Indicates the monitor or monitor group's status, displayed as a colored ball icon. For details on these icons, see "Component and Monitor Status Indicators" on page 249.

General Table

Displays information about the properties associated with the selected server in the left pane.

Important information	<ul style="list-style-type: none"> ➤ This table appears only when a server is selected in the System Health Dashboard. ➤ Click the arrows in the header to collapse and expand the table. ➤ Click the header name to sort by the header's value.
------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

User interface elements are described below:













UI Element (A-Z)	Description
Property Name	Lists the properties associated with the selected component, such as: <ul style="list-style-type: none"> ➤ IP Address ➤ Build number ➤ Operating system type
Value	Lists the value of the specified property.

Data Collector Details Table

Displays information, in tree form, about the data collector selected in the left pane.

Important information	<ul style="list-style-type: none"> ➤ This table appears only when a data collector is selected in the System Health Dashboard. ➤ Click the arrows in the header to collapse and expand the table.
------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

User interface elements are described below:

UI Element (A-Z)	Description
	A Discovery Probe.
	A Business Process Monitor (BPM) data collector.
	A Real User Monitor (RUM) data collector.
	A SiteScope (SiS) data collector.
	Displayed next to the IP address of the machine on which the Discovery Probe is running.
	Displayed next to the IP address of the machine on which the Business Process Monitor (BPM) data collector is running.
	Displayed next to the IP address of the machine on which the Real User Monitor (RUM) data collector is running.
	Displayed next to the IP address of the machine on which the SiteScope (SiS) data collector is running.
	Denotes an instance of a Discovery Probe.
	Denotes an instance of a Business Process Monitor (BPM) data collector.
	Denotes an instance of a Real User Monitor (RUM) data collector.
	Denotes an instance of a SiteScope (SiS) data collector.

UI Element (A-Z)	Description
Property Name	Lists the properties associated with the selected data collector, such as: <ul style="list-style-type: none"> ➤ Build number ➤ Port number ➤ Version number
Value	Lists the value of the specified property.

Map of BSM System and Components

Depicts the various BSM components measured by System Health.



To access	Click the Dashboard tab on the System Health interface. <ul style="list-style-type: none"> ➤ Database components appear on the left side of the map. ➤ Server components appear to the right of the database components. ➤ Load Balancer components (if deployed) appear to the right of the BSM Server components. <p>Note: When System Health is deployed in a secured environment, Reverse Proxy components appear with the Load Balancer components.</p> ➤ Data collector components appear on the right side of the map.
Important information	You may also see obsolete hosts that are no longer running BSM. To disable these obsolete hosts, browse to the URL http://<Gateway Server machine name>.<domain_name>/topaz/systemConsole/displayBACHosts.do and disable all obsolete hosts.
See also	<ul style="list-style-type: none"> ➤ "System Health Displays" on page 151 ➤ "Component and Monitor Status Indicators" on page 249 ➤ "Monitors Table" on page 258




Component Status and Description

Displays the status of the components monitored by System Health.

Important information	The color of all component outlines reflects the lowest functioning level subcomponent or monitor contained in the component, known as the worst child rule . The exception to this rule is the gray outlined components, which do not automatically cause their parent components to be outlined in gray.
See also	<ul style="list-style-type: none"> ➤ "System Health Displays" on page 151 ➤ "Component and Monitor Status Indicators" on page 249 ➤ "Monitors Table" on page 258






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














Status	Description
	A green outline indicates that the component and its subcomponents are working properly. The component's icon is accompanied by a check symbol inside a green square.
	<p>A red outline indicates that a critical problem exists in the component, in one of its subcomponents, or both. The component's icon is accompanied by an x symbol inside a red square.</p> <p>It is recommended that you drill down in the component to identify its specific problematic monitors.</p>




Status	Description
	<p>A yellow outline indicates one of the following:</p> <ul style="list-style-type: none"> ▶ A non-critical problem exists either in the component, in one or more of its subcomponents, or both. ▶ The component's monitors were unable to connect with the server. <p>The component's icon is accompanied by a ! symbol inside a yellow square.</p>
	<p>A gray outline indicates that there are currently no monitors scheduled to run for the component. The component's icon is accompanied by a - sign inside a gray square.</p>
	<p>A jagged blue outline, together with the component's status color represents the currently highlighted component.</p>

Icons and Buttons

Following are the component icons and buttons on the Map of BSM System and Components:

UI Element	Description
	<p>Expands the component and displays its subcomponents.</p> <p>Important: You must select the cursor button  on the System Health Dashboard toolbar to operate the Expand button.</p>
	<p>Hides the subcomponents contained within the selected component.</p> <p>Important: You must select the cursor button  on the System Health Dashboard toolbar to operate the Hide button.</p>
	<p>A Database server</p>

UI Element	Description
	A Database
	A Gateway Server
	A Processing server
	A group of processes
	A group of server monitors
	A bus component
	A logical group Example: Alerts Engine
	An application Example: Service Health
	A group of applications
	A service Example: Service Level Management Engine
	A group of Business Process Monitor data collectors
	A group of SiteScopes
	A group of Discovery Probes

UI Element	Description
	A group of Real User Monitor data collectors
	Indicates the flow of data. Note: Click the Navigation button  and then click anywhere on an arrow line to find the arrow's destination or origin.

Database Components

The databases that are deployed on BSM.

To access	Database components appear on the left side of the System Health Dashboard left pane.
Important information	You may also see obsolete hosts that are no longer running BSM. To disable these obsolete hosts, browse to the URL http://<Gateway Server machine name>.<domain_name>/topaz/systemConsole/displayBACHosts.do and disable all obsolete hosts.
See also	<ul style="list-style-type: none"> ➤ "System Health Displays" on page 151 ➤ "Component and Monitor Status Indicators" on page 249 ➤ "Monitors Table" on page 258

User interface elements are described below:

UI Element (A-Z)	Description
Foundation Database	Stores system-wide and management-related metadata for the BSM environment.
History Database	Used for storage of data, over time, of the RTSM configuration items (CIs).
Profile Database	Stores raw and aggregated measurement data obtained from the BSM data collectors.
RTSM Database	A central repository for configuration information.

Server Components and Processes

The Map of BSM System and Components includes the following server elements (listed alphabetically):

- Alerts Engine
- Applications (Service Health application, Service Level Management, System Availability Management, and Portal components)
- Applications Engines
- BPMs (Business Process Monitors)
- bus
- CDM
- Data Flow Probes
- modeling
- Portal application (MyBSM)
- Processes (for details, see "BSM Processes" on page 179)
- Real User Monitor Engines
- Reports database aggregator
- RTSM
- SAM (System Availability Management - Management of SiteScopes)
- Scheduler (NOA service scheduler)
- Service Health Engine
- Server monitors
- SiteScopes
- SLM (Service Level Management) Engine
- Validator (NOA service validator)
- Verticals (SAP service and Siebel service)

Data Collector Components

Depicts the data collector elements that are deployed on BSM.

To access	Data Collector components appear on the right side of the System Health Dashboard left pane.
Important information	You may also see obsolete hosts that are no longer running BSM. To disable these obsolete hosts, browse to the URL http://<Gateway Server machine name>.<domain_name>/topaz/systemConsole/displayBACHosts.do and disable all obsolete hosts.
See also	<ul style="list-style-type: none"> ▶ "System Health Displays" on page 151 ▶ "Component and Monitor Status Indicators" on page 249 ▶ "Monitors Table" on page 258

User interface elements are described below:

UI Element (A-Z)	Description
BPMs	Displays the status of the Business Process Monitor data collectors.
Discovery Probes	Displays the status of the Discovery Probes.
RUM Engines	Displays the status of the Real User Monitor engines.
SiteScopes	Displays the status of the SiteScopes.

System Health Setup Wizard

This wizard enables you to establish remote connectivity to the BSM and database servers for full monitoring.




<p>To access</p>	<p>Select Admin > Platform > Setup and Maintenance > System Health.</p> <p>Note:</p> <ul style="list-style-type: none"> ▶ To enable configuring the System Health application, the System Health Setup Wizard opens automatically the first time you access the application after installation. For subsequent users and user instances, the wizard does not open automatically. ▶ You can also access the System Health Setup Wizard by performing either Full Model Synchronization or Soft Synchronization. Soft Synchronization opens the wizard only if changes were made to the System Health model, and Full Model Synchronization opens the wizard only if no component is selected. ▶ The user whose remote connection information you enter into the System Health Setup Wizard can perform only those actions for which they have permissions.
<p>Important information</p>	<ul style="list-style-type: none"> ▶ If you do not enter remote connection details for the server, System Health retrieves information only for monitors that do not require credential authorization to access the BSM servers. ▶ The left pane of the System Health Setup Wizard indicates the page of the wizard on which you are currently working.

Wizard map	This wizard contains: Remote Servers Setup Page > Remote Databases Setup Page > Recipients Setup Page
See also	<ul style="list-style-type: none"> ➤ "System Health Setup Wizard – Overview" on page 150 ➤ "How to Deploy and Access System Health" on page 162 ➤ "System Health Monitors" on page 181

Sample Status and Description

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

The following table describes each color and its status:


Status	Description
	A green icon indicates that the credentials entered are sufficient for all of the monitors to access the BSM servers.
	<p>A red icon indicates that remote connectivity to the selected server has failed, due to one of the following reasons:</p> <ul style="list-style-type: none"> ➤ The permissions level of the user entered in the wizard are not sufficient for the monitors to retrieve information from the specified server. ➤ The user entered in the wizard does not exist on the BSM machine running on the specified server. ➤ A mistake has been made in the user credentials entered in the wizard. <p>A red icon is accompanied by an "x" symbol inside a red square.</p>
	<p>A gray icon indicates that no attempt was made to establish remote connectivity to the specified server.</p> <p>A gray icon is accompanied by a "-" symbol inside a gray square.</p>

Remote Servers Setup Page

This wizard page enables you to create a remote connection to BSM servers for System Health to monitor.

Important information	<ul style="list-style-type: none"> ▶ General information about this wizard is available here: "System Health Setup Wizard" on page 269. ▶ You can configure different settings for each server, or apply the same settings to all servers. ▶ You must configure the remote connection details for the server in order for System Health to run all of the server's available monitors. If you do not enter remote connection details for the server, System Health retrieves information only for monitors that do not require credential authorization to access the BSM servers.
Wizard map	The System Health Setup Wizard contains: Remote Servers Setup Page > Remote Databases Setup Page > Recipients Setup Page
See also	"System Health Setup Wizard – Overview" on page 150

User interface elements are described below:

UI Element (A-Z)	Description
	Displays descriptions of the Remote connection details fields. Click again to hide descriptions.
Apply	Applies the remote connection configurations for the selected servers.
Encoding	The encoding used by the server. Example: Cp1252, UTF-8


UI Element (A-Z)	Description
Login	<p>The login name to be used for establishing remote connectivity between the monitors and the specified servers.</p> <p>The user whose login name is entered must have the appropriate permission level for the monitors to run on the server.</p> <p>The format for entering information into this cell is DOMAINNAME\login.</p>
Method	<p>The method of communication for connecting to the BSM components.</p> <p>Example: NetBIOS, SSH</p>
OS Type	<p>The Operating System running on the server.</p> <p>Example: Windows, UNIX</p> <p>Note: This field is only visible if System Health does not identify an operating system on the server.</p>
Password	<p>The password of the login name to be used for establishing remote connectivity with the specified servers.</p> <p>The user whose password is entered must have the appropriate permission level for the monitors to run on the server.</p>

Remote Databases Setup Page

This wizard page enables you to create a remote connection to databases for System Health to monitor.

Important information	<ul style="list-style-type: none"> ▶ General information about this wizard is available here: "System Health Setup Wizard" on page 269. ▶ You can configure different settings for each server, or apply the same settings to all servers. ▶ You must configure the remote connection details for the database in order for System Health to run all of the database's available monitors. If you do not enter remote connection details for the database, System Health retrieves information only for monitors that do not require credential authorization to access the BSM servers.
Wizard map	The System Health Setup Wizard contains: Remote Servers Setup Page > Remote Databases Setup Page > Recipients Setup Page
See also	"System Health Setup Wizard – Overview" on page 150

User interface elements are described below:

UI Element (A-Z)	Description
	Displays descriptions of the Remote connection details fields. Click again to hide descriptions.
Apply	Applies configurations for the selected database.
Encoding	Indicate the encoding used by the server running the database. Example: Cp1252, UTF-8
Initialize Shell Environment	Optionally, enter any shell commands to be executed at the beginning of the session. Separate multiple commands with a semicolon (;). This option specifies shell commands to be executed on the remote machine directly after a Telnet or SSH session has been initiated.


UI Element (A-Z)	Description
Login	The login name used to access the operating system running on the server on which the database is installed. Note: The format for entering information into this cell is DOMAINNAME\login .
Login Prompt	The prompt output when the system is waiting for the login to be entered. Default: login:
Method	The method of communication for System Health to speak to the database. Example: NetBIOS, SSH
Operating System	The Operating System running on the server. Example: Windows, UNIX Note: This field is only visible if System Health does not identify an operating system on the server.
Password	The password used to access the operating system running on the server on which the database is installed.
Password Prompt	The prompt output when the system is waiting for the password to be entered. Default: password:
Prompt	The prompt output when the remote system is ready to handle a command. Default: #
Secondary Prompt	The secondary prompts if the telnet connection to the remote server causes the remote server to prompt for more information about the connection. Separate multiple prompt string by commas (,).
Secondary Response	The responses to any secondary prompts required to establish connections with this remote server. Separate multiple responses with commas (,).

Recipients Setup Page

This wizard page enables you to configure recipients to receive predefined System Health alerts through email.

Important information	General information about this wizard is available here: "System Health Setup Wizard" on page 269.
Wizard map	The System Health Setup Wizard contains: Remote Servers Setup Page > Remote Databases Setup Page > Recipients Setup Page
See also	"System Health Setup Wizard – Overview" on page 150

User interface elements are described below:

UI Element (A-Z)	Description
	Displays descriptions of the Recipient Details fields. Click again to hide descriptions.
<Recipients Pane>	Displays a list of recipients configured to receive predefined System Health alerts through email. Click the recipient's name to edit their details. Click Add new recipient to configure a new recipient.
BSM Databases	Select to receive alerts on the status of BSM Databases.
BSM servers, services, and applications	Select to receive alerts on status of BSM servers, services, and applications.
Create	Adds the configured recipient to the recipient list pane.
Email	The recipient's email address.
Mediators	Select to receive alerts on status of BSM Mediators and Load Balancers.
Name	The recipient's name.

Toolbar

The Toolbar enables you to customize the display of the BSM components on the System Health Dashboard, perform actions on the components, perform management operations on the components, and synchronize the status and model of the components.









To access	The Toolbar is located at the top of both the System Health Dashboard and the Inventory tab.
Important information	Buttons that customize the display of the BSM components (Dashboard Customization Buttons) appear only on the System Health Dashboard. All other buttons appear on both the System Health Dashboard and the Inventory tab.
See also	<ul style="list-style-type: none"> ➤ "System Health Displays" on page 151 ➤ "Service Manager Dialog Box" on page 281 ➤ "Backup Server Setup Window" on page 283 ➤ "Process Manager Dialog Box" on page 284 ➤ "Quick Report Screen" on page 286




Dashboard Customization Buttons

These buttons enable you to customize the appearance of the components on the System Health Dashboard.

Important information	The buttons that customize the display of the BSM components appear only on the System Health Dashboard, and do not appear on the Inventory tab.
------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------

User interface elements are described below:




UI Element	Description
	<p>Select. Enables selecting a component on the System Health Dashboard left pane.</p> <p>Note: This button is selected by default upon entering the System Health Dashboard.</p>
	<p>Pan. Pans the System Health Dashboard left pane.</p>
	<p>Zoom. Zooms on a specific area of the System Health Dashboard left pane.</p> <p>You zoom by holding down the left click button on your pointer. Move the pointer down to zoom in; move the pointer up to zoom out.</p>
	<p>Navigation. Enables navigating between components of the dashboard.</p> <p>You click the Navigation button and then click a line connecting two components or subcomponents. Depending on where on the line you click, the cursor navigates to either the original or endpoint component, whichever is further.</p>
	<p>Fit. Fits all open components and subcomponents into the visible area.</p>
	<p>Undo. Undoes your previous action and goes back to the previous display on the System Health Dashboard left pane.</p> <p>Note: This button is enabled only if you have generated more than one view on the System Health Dashboard left pane.</p>
	<p>Redo. Redoes an action that has been undone with the Undo button .</p> <p>Note: This button is enabled only if you have generated more than one view on the System Health Dashboard, and are not currently resting on the most recent view.</p>

UI Element	Description
	<p>Realign. Realigns System Health Dashboard left pane components, so that the components are aligned in their original order, which is (left to right):</p> <ul style="list-style-type: none"> ➤ Databases ➤ Servers ➤ Load Balancers (if deployed) ➤ Data Collectors
	<p>Rearrange. Returns the System Health Dashboard left pane to its default view. This includes closing open components and realigning component boxes to their original state.</p>
	<p>Overview. Displays an overview map of all the component boxes on the System Health Dashboard left pane.</p> <p>The Overview Map appears in a separate window, with blue lines denoting the boundaries of the System Health Dashboard left pane.</p> <p>Note: You cannot perform other functions on the System Health Dashboard while the Overview Map is open.</p>

Action Buttons

These buttons enable you to perform actions on the BSM components monitored by System Health.




User interface elements are described below:

UI Element	Description
	<p>Service Manager. Opens the Service Manager dialog box. This option enables you to move backend services from one server to another of the same type if the server machine is not functioning properly, requires downtime for servicing, or is overloaded. For details on the Service Manager dialog box, see "Service Manager Dialog Box" on page 281.</p> <p>Note: You must have more than one server of the same type configured in your BSM environment for this button to be enabled.</p>
	<p>Backup Server Configuration. Used to define a backup server, in case the current server is not functioning properly or requires downtime for servicing.</p> <p>Note: You must have more than one server of the same type configured in your BSM environment for this button to be enabled.</p>
	<p>Process Manager. Stops or starts processes on selected servers, for maintenance purposes or in case these processes display a problematic status on the System Health Dashboard or the Inventory tab.</p>

Information Buttons

These buttons enable you to retrieve information on the BSM components monitored by System Health.

User interface elements are described below:




UI Element	Description
	Quick Report. Receives a Quick Report on data collected over the past 24 hours for the selected component. For details on Quick Reports, see "Quick Report Screen" on page 286.
	Export to CSV. Exports a report containing of the System Health monitors' and BSM components' current status to a .csv file.
	Export to PDF. Generates a .zip file containing the log files of a specific server. Note: You must select a server component on the System Health Dashboard left pane for this button to be enabled.

Synchronization Buttons

These buttons enable you to synchronize the status and model of the BSM components monitored by System Health.


Important information	If an BSM component was down while Soft or Full Model Synchronization was performed, System Health may not have configured the full monitoring solution onto these components. To prevent this from happening, ensure that all components are up and running during the System Health Setup Wizard configuration, and while performing Soft or Full Model Synchronization.
------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

User interface elements are described below:

UI Element	Description
	Refresh Statuses. Refreshes the selected component and retrieves its current status, without running the component's monitors.
	Soft Synchronization. Updates System Health with any changes to the System Health model. If required, the System Health Setup Wizard is opened for the area of System Health in which the changes were applied.
	Full Model Synchronization. Resets the configuration of the selected component, including resetting of all monitors and their status. If no specific component is selected, the entire System Health configuration is reset, and the System Health Setup Wizard is opened, where you must reconfigure the connection of all system monitors to the servers. For details, see "System Health Setup Wizard" on page 269.

Service Manager Dialog Box

Enables you to move backend services from one server to another of the same type, in case the server machine is not functioning properly, requires downtime for servicing, or is overloaded.


To access	Click the Service Manager button  on the Toolbar on either the System Health Dashboard or the Inventory tab.
Important information	<ul style="list-style-type: none"> ▶ You can move services from a server only to another server of the same BSM type. ▶ You cannot move services (such as RTSM) from or to an external machine. ▶ When automatic failover moves processes to the backup machine, it may move only part of a service group, causing System Health to display the same service group on two different servers.
See also	"Understanding Service Reassignment" on page 159

User interface elements are described below:

UI Element (A-Z)	Description
Execute	Moves the indicated customer services from one server to another.
Operation Status	Displays the status of the performed operation.
Select Operation	Select the type of service you want to move.
Select Source Machine	Select the machine from which you want to move the services.
Select Target Machine	Select the machine to which you want to move the services.

Backup Server Setup Window

Enables you to define a backup server to run the BSM server components, in case the server machine is not functioning properly or requires downtime for servicing.


To access	Click the Backup Server Setup button  on the Toolbar.
Important information	<ul style="list-style-type: none"> ▶ This button is enabled only if you have configured more than one Processing server. ▶ You must click the Enable Automatic Failover box for the backup server to be enabled. ▶ External machines, such as CMDB, cannot be defined as a backup server. ▶ By default, services are reassigned to the backup server after a timeout of 20 minutes has been reached. The timeout value can be configured in Admin > Platform > Setup and Maintenance > Infrastructure Settings > Foundations > High Availability Controller. ▶ You can monitor the task assignments using System Health, or in the hac-manager JMX. The relevant logs are: <ul style="list-style-type: none"> ▶ <HPBSM root directory>\log\EJBContainerhac-locator.log. Contains the location changes for each service. ▶ <HPBSM root directory>\log<process-name>hac-launcher.log. Contains information about the relevant services for the process, and errors in case the service fails to start.
See also	"Move Backend Services" on page 172

User interface elements are described below:




UI Element (A-Z)	Description
Enable Automatic Failover	Select to activate the selected server as the backup server.
Execute	Defines the selected server as the backup server.
Operation Status	Displays the status of the performed operation.
Select Backed-up Servers	Select the servers to be backed up.
Select Backup Server	Select the backup server.




Process Manager Dialog Box

Enables you to stop or start processes on specific servers, in case these processes display a problematic status on the System Health Dashboard or Inventory tab, or the processes require maintenance.

To access	Click the Process Manager button  on the Toolbar.
Important information	You can select multiple processes to start or stop in the Process Manager dialog box.
See also	<ul style="list-style-type: none"> ▶ "Manage BSM Processes" on page 174 ▶ "BSM Processes" on page 179


User interface elements are described below:

UI Element (A-Z)	Description
	Indicates the selected process is running.
	Indicates the selected process was started and is not yet running.
	Indicates the selected process was stopped.

UI Element (A-Z)	Description
	Indicates the selected process is currently being stopped.
	Indicates the selected process was launched.
	Indicates the selected process' status is unknown.
Operation Status	Displays the status of the performed operation.
Refresh	Refreshes process statuses. Note: A stopped process appears in red.
Select Process(es)	Select the process you want to stop or start.
Select Server	Select the server on which you want to start or stop processes.
Start	Starts the selected processes.
Start All	Starts all of the processes in the Select Process(es) window.
Stop	Stops the selected processes.
Stop All	Stops all of the processes in the Select Process(es) window.

Quick Report Screen

Displays a report on data gathered from the past 24 hours on the selected component's monitors.

To access	Click the Quick Report button  on the Toolbar.
Important information	<p>The following links appear on the Quick Report screen, which enable you to view specific information on the monitors:</p> <ul style="list-style-type: none"> ▶ Table Format: ▶ Error List: ▶ Warning List: ▶ Good List: <p>For details on the information each of these links displays, see below.</p>
See also	<ul style="list-style-type: none"> ▶ "New SiteScope Quick Report Dialog Box" in <i>Using SiteScope</i> in the SiteScope Help ▶ "Display a Quick Report" on page 174


User interface elements are described below:

UI Element (A-Z)	Description
<Graphs>	Displays the monitor groups' output in graph format.
Error List	Displays the monitor runs that retrieved an error status, based on the thresholds configured for the monitor.
Good List	Displays the monitor runs that retrieved a good status, based on the thresholds configured for the monitor.
Measurement Summary Table	Displays measurement data for each of the BSM monitors.

UI Element (A-Z)	Description
Table Format	Displays the monitor groups' output in table format.
Uptime Summary Table	Displays the percentage of uptime each BSM monitor experienced over the indicated time period.
Warning List	Displays the monitor runs that retrieved a warning status, based on the thresholds configured for the monitor.

Troubleshooting and Limitations

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

Problem	Solution
Interface does not display any BSM components	Click the Refresh button on your browser. Note: This problem is most common when first logging into System Health on Microsoft Internet Explorer 7.0.
All components and monitors are displayed in gray	 Click the Full Model Synchronization button in the Toolbar on either the System Health Dashboard or the Inventory tab. The Full Model Synchronization button resets the System Health configuration and erases all of the monitors' history in BSM. You then reconfigure System Health to create remote connections to the servers which System Health monitors, using the System Health Setup Wizard. For details, see "System Health Setup Wizard" on page 269.
Monitors are not displayed on a component	

11

Audit Log

This chapter includes:

Concepts

- ▶ Audit Log — Overview on page 290

Tasks

- ▶ How to Use the Audit Log on page 293
- ▶ How to Customize a Log File for Audit Log on page 294

Reference

- ▶ Audit Log User Interface on page 295

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.
- ▶ **CI Status Alert Administration.** Displays actions related to creating alert schemes for a configuration item (CI) status alert.
- ▶ **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 Health.**
- ▶ **Service Health Administration.** Displays actions related to configurations made in the Service Health Administration.
- ▶ **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 293.
- ▶ **SLA Alert Administration.** Displays actions related to creating, modifying, or deleting SLA alerts.
- ▶ **System Availability Manager.** Displays actions related to system availability and SiteScope.
- ▶ **User Defined Reports.** 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 295.

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. BSM 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**. BSM 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.

How to Customize a Log File for Audit Log

Audit log uses the Apache log4j logging utility.

To customize the log file, edit its configuration file, located at **<HPBSM root directory>\conf\core\Tools\log4j\EJB\auditlog.properties**, using the log4j configuration syntax. The log level should be set to INFO or higher. The appender name, **com.mercury.topaz.tmc.bizobjects.audit.AuditManager.writeAudit**, should not be changed.

Reference

Audit Log User Interface

This section includes:


- Audit Log Page on page 295

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 290




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

UI Element (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 297.
<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 296.

UI Element (A-Z)	Description
Context	Select a context to view. For a detailed list of the available contexts, see "Audit Log — Overview" on page 290.
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 Element (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 Element (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 <i>Using End User Management</i> .
------------------------------	-------------------------------------------------------------------------------------------------------------------------

User interface elements are described below:

UI Element (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.

12

Working in Non-English Locales

This chapter includes:

Reference

- ▶ Installation and Deployment Issues on page 300
- ▶ Database Environment Issues on page 302
- ▶ Administration Issues on page 303
- ▶ Service Health Issues on page 304
- ▶ Service Level Management Issues on page 305
- ▶ Report Issues on page 305
- ▶ Business Process Monitor Issues on page 305
- ▶ SiteScope Issues on page 306
- ▶ Real User Monitor Issues on page 306
- ▶ End User Management Administration Issues on page 307
- ▶ Data Flow Management Issues on page 307
- ▶ Multilingual Issues on page 307
- ▶ Multilingual User (MLU) Interface Support on page 308

Reference

Installation and Deployment Issues

- ▶ If you use a CJK language in your browser, you must ensure that the Gateway Server machine running BSM has East Asian languages installed. On the machine on which the BSM Gateway Server is installed, you must select **Control Panel > Regional & Language Options > Languages > Install files for East Asian languages**.
- ▶ If you have installed BSM on a non-English Windows operating system, the command line tool output may not be displayed correctly because the Windows and OEM code pages differ. This may not be the case on many Asian language systems, but is often experienced on non-English European systems.

To fix this, Windows Command Prompt must be configured so that a TrueType font is used and the OEM code page is the same as the Windows code page.

In a Windows Command Prompt window (run cmd.exe), right-click the title bar, select **Properties**, and open the **Font** tab. Change the font from **Raster Fonts** to a TrueType font, and change the font size if necessary (for example: select Lucida Console, 12 pt). If prompted, modify the shortcut to make the font change global.

Note: If you use other command line tools, such as PowerShell or Cygwin Bash, you must change the font for each of these tools separately.

To change the codeset for the system, open the registry editor (regedit), and go to: Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\CodePage. If the values of ACP and OEMCP differ, edit OEMCP to the same value as for ACP, and reboot the system.

Note: If changing the OEM code page for the system is not acceptable, for each newly opened Command Prompt window, change the code page value using the command: **chcp <APC value>**.

- ▶ 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 BSM components must not contain non-Latin characters.
- ▶ When content packs are available in more than one language, the language of content packs automatically loaded during BSM installation depends on the current locale of the host operating system. If there are matching content packs for the current locale, these are installed. If the locale does not have localized content packs, English content packs are used. Later, a user can upload the content pack in another language manually.

At every Gateway Server startup, the contents of the following directory is checked: **<HPBSM root directory>/conf/opr/content/<locale of server>**

Any package that has not already been loaded, and that does not have unresolved package dependencies (references to packages, which are neither already loaded nor in the same folder), is loaded during this startup.

The following directory is checked next: **<HPBSM root directory>/conf/opr/content/en_US**

Any content packs that were not uploaded from the first location are uploaded. This can result in mixed-language content.

The packages are loaded with the standard import mode; already existing artifacts are not changed. Only new artifacts are added.

Note: Progress can be followed in the admin backend log file. The operation is done in the background and may still be in progress when a user logs in. The system prevents multiple content packages from being loaded at the same time.

Database Environment Issues

- ▶ To work in a non-Latin-character language BSM 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-Latin-character 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 *HP Business Service Management Database Guide* PDF.
- ▶ 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 BSM servers.
- ▶ When using the default authentication strategy, Lightweight SSO, to authenticate users logging into BSM, user names and passwords can be in non-Latin characters.
- ▶ To support non-Latin characters in BSM databases, the encoding for databases must be defined as UTF-8 or AL32UTF-8 (Oracle only), or set to the specific language.
- ▶ To support non-Latin characters in log files, set the log4j encoding property on the log4j configuration files.

To write a specific log in UTF-8 encoding, do the following:

- ▶ Search the specific log name in log4j configuration at **conf/core/Tools/log4j**.
- ▶ In the properties file where this log file is configured, add the following property:

log4j.appender.<appender name>.Encoding=UTF-8

For example, the jboss_server.log configuration follows:

```
#####
### define appender: jboss.appender ###
#####
# jboss.appender is set to be a FileAppender which outputs to log/jboss_server.log
log4j.appender.jboss.appender=org.apache.log4j.RollingFileAppender
log4j.appender.jboss.appender.File=${merc.home}/${log.file.path}/jboss_server.log
log4j.appender.jboss.appender.MaxFileSize=${def.file.max.size}
log4j.appender.jboss.appender.Encoding=UTF-8
log4j.appender.jboss.appender.MaxBackupIndex=${def.files.backup.count}
log4j.appender.jboss.appender.layout=org.apache.log4j.PatternLayout
log4j.appender.jboss.appender.layout.ConversionPattern=${msg.layout}
```

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 into BSM 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.

Report Issues

- BSM 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 BSM running on a Chinese Simplified operating system. To view Excel reports, select **Applications > User Reports > Report Manager**.
- Reports downloaded from BSM 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 BSM is installed on an English-language machine, set the **user.encoding** entry in the **<HPBSM root directory>\AppServer\resources\strings.properties** file to the correct encoding.

Business Process Monitor Issues

- If the Business Process Monitor (BPM) log files contain non-Latin-character 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.

- All BPM instances (application, scripts, parameters, etc.) should be named with Latin characters or BPM Server locale characters only.

SiteScope Issues

- ▶ In international version SiteScopes (supporting multilingual character sets), 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 the SiteScope Help.
- ▶ For a list of monitors that are tested for internationalization, see "Monitors Supported for Internationalization" in the SiteScope Help.

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 BSM databases must be defined as UTF-8, or set to the specific language. For further details, see "Database Environment Issues" on page 302.
- ▶ 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-Latin-character 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 discovery has 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 BSM uses SNMP version 1.0, which does not support multilingual data.
- ▶ Error messages in the Failed Transactions report do not display correctly when BSM 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.
- ▶ BSM 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 BSM is compatible with a multilingual version.

Multilingual User (MLU) Interface Support

The BSM 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 BSM can operate but the user interface of only Run-time Service Model (RTSM)-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 BSM. The language preference chosen affects only your local machine (the client machine) and not the BSM machine or any other user accessing the same BSM machine.

To set up and view BSM 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, BSM displays the characters as squares.
- 2** If you are logged into BSM, you must log out. Click **LOGOUT** at the top of the BSM window.

Close every open browser window or alternatively clear the cache (if BSM is running on Internet Explorer).

- 3** If BSM is running on Internet Explorer, configure the Web browser on your local machine to select the language in which you want to view BSM (**Tools > Internet Options**).
 - a** Click the **Languages** button and in the Language Preference dialog box, highlight the language in which you want to view BSM.
 - 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 BSM login window.
- f** From the Internet Explorer menu, select **View > Refresh**. BSM 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 BSM 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 BSM.
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 BSM 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 from the client locale and the package name contains non-Latin characters. For details, see "Package Manager" in the *RTSM 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 Creation and Deployment in a Non-English Locale" in the *RTSM 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 on creating new views, see "Modeling Studio" in *Modeling*.
- ▶ In Location Manager, all geographical locations are in English, regardless of the UI language selected. Logical locations may be named in any language you choose, and remain in that language even if the UI language is subsequently changed.
- ▶ The BSM 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.

13

HP Business Service Management Logs

Note: This chapter is not relevant for HP Software-as-a-Service customers.

This chapter includes:

Concepts

- ▶ BSM Logs — Overview on page 314
- ▶ Log File Locations on page 314
- ▶ Log Severity Levels on page 315
- ▶ Log File Size and Automatic Archiving on page 316
- ▶ JBoss and Tomcat Logs on page 316

Tasks

- ▶ How to Change Log Levels on page 318

Concepts

BSM Logs — Overview

BSM records the procedures and actions performed by the various components in log files. The log files are usually designed to serve HP Software Support when BSM does not perform as expected.

The default severity threshold level for log files differs per log, but is generally set to either **Warning** or **Error**. For a definition of log levels, see "Log Severity Levels" on page 315.

You can view log files with any text editor.

Log File Locations

Most log files are located in the `<HPBSM root directory>\log` directory and in subdirectories organized by component.

Log file properties are defined in files in the following directory and its subdirectories: `<HPBSM root directory>\conf\core\Tools\log4j`.

Log File Locations in a Distributed Deployment

In one-machine or compact installations, all BSM servers and their logs reside on the same machine. In the case of a distributed deployment of the servers among several machines, logs for a particular server are usually saved on the computer on which the server is installed. However, if it is necessary for you to inspect logs, you should do so on all machines.

When comparing logs on client machines to those on the BSM server machines, keep in mind that the date and time recorded in a log are taken from the machine on which the log was produced. It follows that if there is a time difference between the server and client machines, the same event is recorded by each with a different time stamp.

Log Severity Levels

Each log is set so that the information it records corresponds to a certain severity threshold. Because the various logs are used to keep track of different information, each is preset to an appropriate default level. For details on changing the log level, see "How to Change Log Levels" below.

Typical log levels are listed below from narrowest to widest scope:

- ▶ **Error.** The log records only events that adversely affect the immediate functioning of BSM. When a malfunction occurs, you can check if Error messages were logged and inspect their content to trace the source of the failure.
- ▶ **Warning.** The log's scope includes, in addition to Error-level events, problems for which BSM is currently able to compensate and incidents that should be noted to prevent possible future malfunctions.
- ▶ **Info.** The log records all activity. Most of the information is normally routine and of little use and the log file quickly fills up.
- ▶ **Debug.** This level is used by HP Software Support when troubleshooting problems.

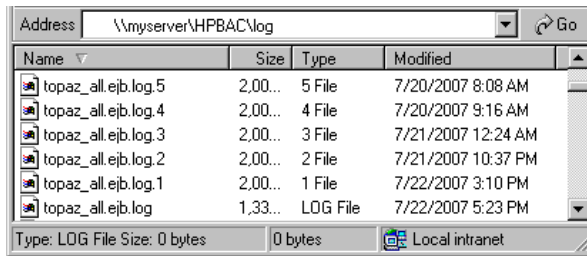
Note: The names of the different log levels may vary slightly on different servers and for different procedures. For example, **Info** may be referred to as **Always logged** or **Flow**.

Log File Size and Automatic Archiving

A size limit is set for each type of log file. When a file reaches this limit, it is renamed and becomes an archived log. A new active log file is then created.

For many logs, the number of archived log files saved can be configured. When a file reaches its size limit, it is renamed with the numbered extension **1**. If there is currently an archived log with the extension **1**, it is renamed with the extension **2**, **log.2** becomes **log.3**, and so on, until the oldest archived log file (with the number corresponding to the maximum number of files to be saved) is permanently deleted.

The following image shows an example of a log file, **topaz_all.ejb.log**, and its archived copies.



Name	Size	Type	Modified
topaz_all.ejb.log.5	2,00...	5 File	7/20/2007 8:08 AM
topaz_all.ejb.log.4	2,00...	4 File	7/20/2007 9:16 AM
topaz_all.ejb.log.3	2,00...	3 File	7/21/2007 12:24 AM
topaz_all.ejb.log.2	2,00...	2 File	7/21/2007 10:37 PM
topaz_all.ejb.log.1	2,00...	1 File	7/22/2007 3:10 PM
topaz_all.ejb.log	1,33...	LOG File	7/22/2007 5:23 PM

The maximum file size and the number of archived log files are defined in the log properties files located in **<HPBSM root directory>\conf\core\Tools\log4j**. An example is:

```
def.file.max.size=2000KB
def.files.backup.count=10
```

JBoss and Tomcat Logs

The following **<HPBSM root directory>\log** directory holds JBoss- and Tomcat-related log files:

- **jboss_boot.log.** Logs startup activities including running the JBoss process, deployment, and startup status, as well as the number of busy ports.
- **jboss_server.log.** Logs all JBoss activities including JBoss messages, deployment and startup status.
- **jboss_tomcat.log.** Logs the Tomcat messages.

Note: You can view the JMX Console at <http://<HPBSM server>:8080/jmx-console>.

Tasks

How to Change Log Levels

This task and the associated flowchart describe how to set up a system for delivering alerts to recipients.

If requested by HP Software Support, you may have to change the severity threshold level in a log, for example, to a debug level.

To change the severity threshold level:

1 Open the log properties file in a text editor. Log file properties are defined in files in the following directory: <HPBSM root directory>\conf\core\Tools\log4j.

2 Locate the **loglevel** parameter. For example,

```
loglevel=ERROR
```

3 Change the level to the required level. For example,

```
loglevel=DEBUG
```

4 Save the file.

14

Port Usage

This chapter includes:

Tasks

- ▶ How to Change Ports Manually on page 320

Reference

- ▶ Incoming HP Business Service Management Traffic on page 323
- ▶ Outgoing HP Business Service Management Traffic on page 325
- ▶ Local HP Business Service Management Traffic on page 326

Tasks

How to Change Ports Manually

This section contains information about how to change different ports manually. The procedure differs for each port.

Manually Changing Port 80

Port 80 is used by the BSM Web Server. To modify this port, you must reconfigure other components on the BSM server and restart BSM.

- 1** Modify the virtual Gateway Server settings
 - a** Navigate to **Administration Tab > Platform > Setup and Maintenance Tab > Infrastructure Settings** and locate the **Platform Administration - Host Configuration table**. If this table is not visible, set the **Select Context** option to **All**.
 - b** Modify the **Virtual Gateway Server for Application Users URL** to **http://<server name>:<new port>**
 - c** Modify the **Default Virtual Gateway Server for Data Collectors URL** to **http://<server name>:<new port>**.
- 2** Modify the direct Gateway Server settings
 - a** In the same table, modify the **Direct Gateway Server for Application Users Server URL** to include the new port.
 - b** Modify the **Direct Gateway Server for Data Collectors URL** to include the new port.
- 3** Modify the local virtual Gateway Server settings
 - a** In the same table, modify the **Local Virtual Gateway Server for Application Users URL** to include the new port.
 - b** Modify the **Local Virtual Gateway Server for Data Collectors URL** to include the new port.

4 Modify the Open BSM URL

- a** Remotely connect to the BSM Gateway server and select **Start > All Programs > HP Business Service Management**.
- b** Right-click **Open HP Business Service Management** and select **Properties**.
- c** In the **Web Document** tab, modify the **URL** field as follows:
http://<Gateway Server>:<new port>/topaz.

5 Modify the web server settings

Modify the web server settings. This procedure varies depending on your version of windows and web server type. They should all be performed in the BSM Gateway server. The following are examples for Windows Server 2008 using three different web servers:

For IIS 6.0 with Windows Server 2008:

- a** In the **Microsoft IIS Internet Services Manager**, right-click **Default Web Site** and select **Properties**.
- b** In the **Web Site** tab, modify the **TCP Port** value as required.

For IIS 7.x with Windows Server 2008:

- a** Open Microsoft's **Computer Management** tool by right-clicking **My Computer** and selecting **Manage**.
- b** Expand **Roles > Web Server** and select **Internet Information Services**.
- c** In the right-hand panel you can see the IIS Manager. In the left part of this panel (**Connections**), expand the connection of the current machine and expand the **Sites** node.
- d** Right-click **Default Web Site** and select **Edit Bindings**.
- e** Select the line that listens to port 80 and click **edit** to change the value to the new port.

For Apache with Windows Server 2008:

- a** Open the file **<BSM_Gateway_home>\WebServer\conf\httpd.conf** in a text editor.
- b** Go to the line that begins with **Listen**, and modify the port value as required.

- c** Go to the line that begins with **ServerName** and modify the port value as required.
- 6** Restart all BSM servers and update data collectors
Restart all BSM servers and update any data collectors that were configured before you modified the port (for example, RUM, BPM, SiteScope). Modify the Gateway Server address in each data collector to reflect the new port as follows: **BSM Gateway>:<new port>**.

Manually Changing Ports 1433 and 1521

These ports control the communication between HP BSM and Database Servers.

1 Modify the Management Database port

Run the Setup and Database Configuration Utility. Skip to the screen that specified the Management Database port and modify it as desired. For details about the Setup and Database Configuration Utility, see the *HP Business Service Management Deployment Guide PDF*.

Note: You can also perform this procedure manually as follows: On all BSM servers (Gateway and DPS), open `<BSM_home>\conf\TopazInfra.ini` in a text editor and modify the **dbPort** property as required.

2 Modify Profile Database port



Navigate to **Admin > Platform > Setup and Maintenance > Manage Profile Databases** and click the **Edit Database Properties** button to modify the desired database configuration to include the new port.

3 Restart all BSM servers

Reference

Incoming HP Business Service Management Traffic

Note: The ports listed here are those ports that BSM uses. If you need to change a port assignment, it is strongly recommended that you first consult with HP Software Support.

There are two categories of incoming BSM traffic:

Internal Traffic

Internal traffic is the traffic between two BSM servers. The following table lists the ports used to transmit data between two BSM servers:

Port Number	BSM Servers that Listen on Port	Port Usage
4444	Gateway Server, Data Processing Server	Remote Method Invocation (RMI) channel between BSM servers
4445	Gateway Server, Data Processing Server	RMI channel between BSM servers
9389	Gateway Server	TCP local LDAP connection for communication between Gateway Servers in a distributed deployment environment
2506	Data Processing Server	Bus domain manager for the connection between the Data Processing Server and the Gateway Server
2507	Gateway Server, Data Processing Server	Main bus processes for the connection between BSM servers

Port Number	BSM Servers that Listen on Port	Port Usage
383	Gateway Server, Data Processing Server	Events coming from HP Operations Manager into the Operations Management application

External Traffic

External traffic is the traffic coming into one of the BSM servers from a client that is not a BSM server. The following table lists the ports used to transmit data from an external BSM client machine to a BSM server:

Port Number	BSM Servers that Listen on Port	Port Usage
80/443	Gateway Server	<ul style="list-style-type: none"> ▶ 80. HTTP/S channel to Gateway Server applications ▶ 443. Port for reverse proxy

Outgoing HP Business Service Management Traffic

Note: The ports listed here are those ports that BSM uses. If you need to change a port assignment, it is strongly recommended that you first consult with HP Software Support.

The following table lists the ports used by the BSM servers to connect to external servers (non-BSM servers):

Port Number	BSM Servers that Connect to Port	Port Usage
25	Gateway Server, Data Processing Server	SMTP channel from the BSM servers to the SMTP mail server
123	Gateway Server	NTP channel from the Gateway Server to the NTP server
161	Data Processing Server	SNMP channel from the Data Processing Server to the SNMP manager
389	Gateway Server	Connection between the Gateway Server and LDAP server for authentication (optional). For more information, see "Authentication Strategies — Overview" on page 614.
1433	Gateway Server, Data Processing Server	Connection between the BSM servers and the Microsoft SQL Server. This is the default port. This port may be changed during installation or thereafter.
1434	Gateway Server, Data Processing Server	Connection between the BSM servers and the Microsoft SQL Browser Service. This port is in use only when a named instance is used.

Port Number	BSM Servers that Connect to Port	Port Usage
1521	Gateway Server, Data Processing Server	Connection between the BSM servers and the Oracle Server This is the default port. This port may be changed during installation or thereafter.
80/443	Gateway Server	<ul style="list-style-type: none"> ▶ 80. HTTP/S channel between the Gateway Server and data collectors for remote administration tasks ▶ 443. Port for reverse proxy

Local HP Business Service Management Traffic

Note: The ports listed here are those ports that BSM uses. If you need to change a port assignment, it is strongly recommended that you first consult with HP Software Support.

The table below lists the ports used for communication between components on all BSM server machine.

Port Number	BSM Servers that Connect to Port	Port Usage
1098	Gateway Server, Data Processing Server	Remote Method Invocation (RMI) management channel used by the jboss application server
1099	Gateway Server, Data Processing Server	Naming service used by the jboss application server
4504	Gateway Server	TCP local LDAP connection used by the Gateway Server

Port Number	BSM Servers that Connect to Port	Port Usage
5001	Gateway Server	Used to connect VuGen to Central Repository Service
8009	Gateway Server, Data Processing Server	Tomcat AJP13 connector
8010	Gateway Server, Data Processing Server	Tomcat AJP13 for WDE connector
8080	Gateway Server, Data Processing Server	HTTP channel for same machine components
8083	Gateway Server, Data Processing Server	RMI dynamic class loading
8093	Gateway Server, Data Processing Server	TCP JMS OIL/2 and UIL used by the jboss application server
11020	Gateway Server, Data Processing Server	RMI management channel for the BSM service
11021	Gateway Server, Data Processing Server	HTTP channel for the BSM service
21212	Data Processing Server	HTTP channel for the RTSM process
21301	Data Processing Server	RMI communication from backend to EPI server Admin services
21302	Gateway Server	RMI communication from console web-app to admin web-app
21303	Gateway Server	RMI communication from console web-app to custom action script server running on the same host
29601	Gateway Server, Data Processing Server	RMI management channel for the jboss application server
29602	Gateway Server, Data Processing Server	RMI management channel for the bus processes
29603	Gateway Server	RMI management channel for the DB Loader process

Port Number	BSM Servers that Connect to Port	Port Usage
29604	Gateway Server	RMI management channel for the Web Data Entry (WDE) process
29608	Data Processing Server	RMI management channel for the Offline BLE process
29610	Data Processing Server	RMI management channel for the Partition and Purging Manager
29612	Gateway Server, Data Processing Server	RMI management channel for the RTSM process
29616	Gateway Server	RMI management channel for the Scheduler process
29620	Data Processing Server	RMI management channel for the BPI repository
29622	Data Processing Server	RMI management channel for the Operations Manager backend process
29628	Data Processing Server	RMI for script execution for pipeline processing in OMi
29629	Gateway Server	RMI for script execution for customizable context menus in the event browser of OMi
29630	Data Processing Server	RMI
29700	Data Processing Server	RMI port for online BLE processes
29711,29712, 29713, 29714	Data Processing Server	RMI port for online BLE processes
29720	Data Processing Server	RMI port for online BLE processes
29800	Data Processing Server	HTTP port for online BLE processes
29807	Gateway Server, Data Processing Server	Shutdown of main bus processes
29811,29812, 29813	Data Processing Server	HTTP port for online BLE processes

Port Number	BSM Servers that Connect to Port	Port Usage
29820	Data Processing Server	HTTP port for online BLE processes
29903	Gateway Server	HTTP channel for the DB Loader process
29904	Gateway Server	HTTP channel for the Web Data Entry (WDE) process
29908	Data Processing Server	HTTP channel for the Offline BLE process
29910	Data Processing Server	HTTP channel for the Partition and Purging Manager
29916	Gateway Server	HTTP channel for the Scheduler process
29922	Data Processing Server	HTTP channel for the Operations Manager backend process
29928	Data Processing Server	HTTP port for script execution for pipeline processing in OMi
29929	Gateway Server	HTTP port for script execution for customizable context menus in the event browser of OMi
29930	Data Processing Server	HTTP
30020	Data Processing Server	HTTP port for online business logic engine processes
31000-31999; 32000-32999	Gateway Server, Data Processing Server	BSM service, uses the first available port in each range
Dynamic ports	Gateway Server, Data Processing Server	Some dynamic ports are used for inter-component channels

15

File Backup Recommendations

This chapter includes:

Reference

- ▶ Configuration and Data File Backup on page 332

Reference

Configuration and Data File Backup

BSM directories that contain key configuration and data files should be backed up on a daily basis as a precautionary measure.

The table below lists the BSM directories that contain such files and should therefore be backed up. All directories are under <HPBSM root directory>.

Resource	Comments
\HPBSM\BLE	Configuration of business rules. Back up if business rules have been created.
\HPBSM\conf	Assorted BSM configuration files.
\HPBSM\dat	Assorted BSM configuration files.
\HPBSM\dbverify\conf	Configuration files for dbverify. This directory does not have to be backed up if dbverify has not been run.
\HPBSM\EJBContainer\bin	Configuration files for the scripts used to run BSM, and environment settings.
\HPBSM\bin	BSM binary files. Back up if changes were made to any of the installation defaults.
\HPBSM\lib	BSM library files. Back up if changes were made to any of the installation defaults.
\HPBSM\AppServer\GDE	Configuration files for the Generic Reporting Engine, used for obtaining data for reports.
\HPBSM\odb\conf	RTSM main configuration directory
\HPBSM\odb\lib	RTSM library files. Back up if changes were made to any of the installation defaults.
\HPBSM\odb\classes	RTSM patch files. Back up if any patches were added.

Resource	Comments
\HPBSM\odb\runtime\fcmdb	RTSM adapter files.
\HPBSM_postinstall	Post-installation configuration files.
\HPBSM\opr\bin	Operations Management application binary files. Back up if changes were made to any of the installation defaults.
\HPBSM\opr\lib	Operations Management library files. Back up if changes were made to any of the installation defaults.
\HPBSM\opr\webapps	BSM Web application files. Back up if changes were made to any of the installation defaults.
\HPBSM\opr\newconfig	Assorted BSM configuration files and libraries.
\HPBSM\AppServer\webapps\site.war\WEB-INF\sam\hi-mapping-monitors.xml	Custom EMS monitor types. Back up if any customer EMS SiteScope monitors were configured.

Part III

Data Enrichment

16

Location Manager

This chapter includes:

Concepts

- ▶ Location Manager Overview on page 338
- ▶ Populating the Location Manager on page 339
- ▶ Creating and Working with the XML File on page 341

Tasks

- ▶ How to Populate the Location Manager on page 344
- ▶ How to Update Locations Using Mass Upload on page 345

Reference

- ▶ Location Manager User Interface on page 348

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 > RTSM Administration > Modeling > IT Universe Manager**). To see location CIs, select **Locations** view.

Location Manager is accessible to users who have Administrator or System Modifier 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 a 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 you assign geographical coordinates to a logical location, these coordinates can be changed or deleted.

Note: All geographical locations are in English, regardless of the UI language selected. Logical locations may be named in any language you choose, and remain in that language even if the UI language is subsequently changed.

- ▶ **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 349.
- ▶ **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 341.

- ▶ **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 359.

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; IPv4 address range 4.38.41.136 to 4.38.80.152 (ISP = Level 3 Communications); IPv6 address range 2002:0C19:8B00:0000:0000:0000:0000 to 2002:0C19:B28F: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 359.

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 344
- ▶ "Populate the Location Manager using an XML file" on page 344

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 349.

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 345.

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 341. For details on the XML file elements and attributes, see "XML Tag Reference" on page 359.
 - 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 34.)
- 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:

1. 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:

- ▶ No two locations on the same hierarchical level (having the same parent) may have the same name. A location directly under `customer_hierarchy` (that is, directly under the root location, `World`) and a location in another place in the hierarchy may not have the same name unless one instance refers to a geographical location and the other to a logical location; or they refer to different types (country, state or city) of geographical locations, such as the country Mexico and city Mexico, or the state New York and city New York.
- ▶ A maximum of seven levels of hierarchy can be defined.
- ▶ No two locations may have the same ID.
- ▶ All location ID values in the XML must match an existing location with that ID.
- ▶ No two overlapping IP ranges are allowed.

2. 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

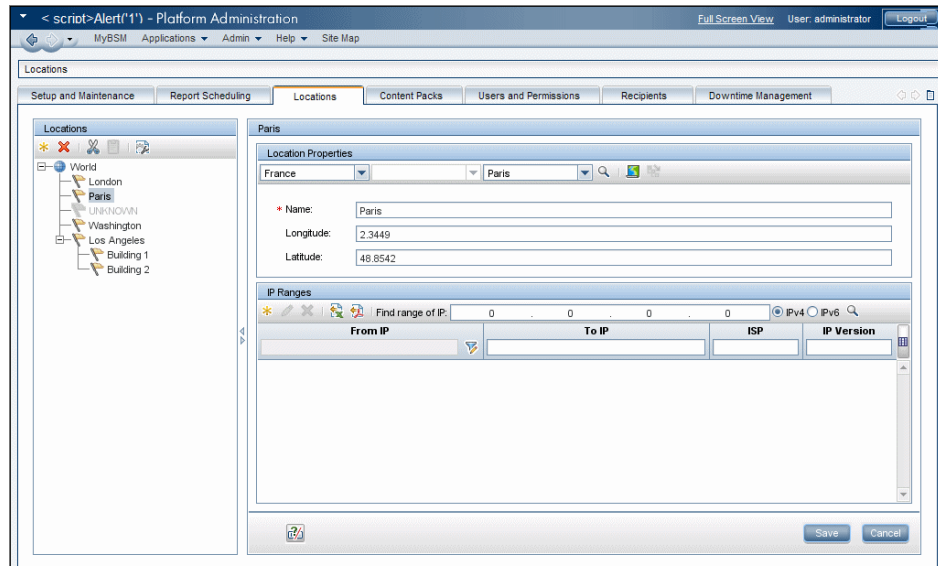
Location Manager User Interface

This section includes:

- ▶ Location Manager Page on page 349
- ▶ New/Edit IP Range Dialog Box on page 356
- ▶ Geographical Map Dialog Box on page 357

Location Manager Page

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








To access	Select Admin > Platform > Locations
Relevant tasks	"How to Populate the Location Manager" on page 344
See also	"Location Manager Overview" on page 338

Locations Area — Left Pane


In the Locations area, on the left pane of the Locations page, you can add, delete, and move locations, and set a location as the default container. Locations appear in a tree structure, with a maximum of seven hierarchical levels, whose root (level zero) 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 Element	Description
	<p>Add location. Click to add a new location below the selected location. Opens the Location Properties area.</p>
	<p>Delete location. Click to delete a location and its children locations.</p> <p>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.</p> <p>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.</p>
	<p>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.</p> <p>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.</p>




UI Element	Description
	<p>Paste location. Available when a location has been cut and the user has navigated to another part of the tree.</p> <p>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 sibling locations under the same parent is not permitted. A location under World and a location in another place in the tree may not have the same name unless one instance refers to a geographical location and the other to a logical location; or they refer to different types (country, state or city) of geographical locations, such as the country Mexico and city Mexico, or the state New York and city New York.</p>
	<p>Set as default container. Click to set a particular location as the default container. This is the parent location for all automatically discovered locations.</p> <p>For more information, see "Location Manager Overview" on page 338.</p>

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 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 Element	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 357.
	Get coordinates from nearest parent. Click to copy the geographical coordinates of the closest parent location with coordinates, to the selected location.







UI Element	Description
Name	<p>Enter the name of the location in the Name text box.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▶ The name field is mandatory. Assigning the same name to sibling locations under the same parent is not permitted. A location under World and a location in another place in the tree may not have the same name unless one instance refers to a geographical location and the other to a logical location; or they refer to different types (country, state or city) of geographical locations, such as the country Mexico and city Mexico, or the state New York and city New York. 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 should be changed. ▶ If you change the name of a geographical location, its association with the original geographical location is maintained.
Longitude/Latitude	<p>Enter the longitude and latitude of the location in the longitude and latitude text boxes.</p> <p>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.</p>


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 Element	Description
	<p>New IP Range. Click to create a new IP range. Opens the New IP Range dialog box.</p> <p>Note: A particular IP range can be assigned to only one location at a time.</p> <ul style="list-style-type: none"> ▶ 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.
	<p>Edit IP Range. Click to edit a selected IP range. Opens the Edit IP Range dialog box.</p>
	<p>Delete IP Range. Click to delete one or more selected IP ranges.</p>
	<p>Export to Excel. Click to export IP range information for the selected location to an Excel spreadsheet.</p>
	<p>Export to PDF. Click to export IP range information for the selected location to an Adobe Acrobat file.</p>
	<p>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.</p> <p>Note: Columns not displayed on screen are also not exported to Excel or Adobe Acrobat (PDF) files.</p>

UI Element	Description
Find Range of IP	<p>To find an existing range in which a particular IP address is located:</p> <ul style="list-style-type: none"> ▶ Select the appropriate radio button: <ul style="list-style-type: none"> ▶ 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 . <p>The range in which the IP address is found is highlighted.</p> <p>Note: This searches for the IP range in the currently selected location only.</p>
From IP/To IP, ISP, IP Version	<p>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.</p> <p>These boxes may be used in combination with each other. An asterisk (*) may be used as a wildcard to represent one or more characters.</p> <p>For example:</p> <ul style="list-style-type: none"> ▶ 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 Element	Description
IP version	<p>Choose IPv4 or IPv6 to select:</p> <ul style="list-style-type: none"> ▶ 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	<p>Use the From IP and To IP boxes to set the range of IP addresses for the location.</p> <ul style="list-style-type: none"> ▶ 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. <p>Note: The IPv4 range must not exceed 50,000,000 IP addresses.</p> <ul style="list-style-type: none"> ▶ 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 344
See also	"Location Manager Page" on page 349

User interface elements are described below:

UI Element	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 Element	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 format IPv6 – IPv6 regular expression	
end_ip	Upper limit of IP address range. For supported IPv4 and IPv6 notation formats, see start_ip, above. Note: IPv4 range must not exceed 50,000,000 IP addresses.	
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">
location_name	location	String. Mandatory. Not unique (several locations, if not siblings, 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: <ul style="list-style-type: none"> ▶ "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">
```

17

Content Packs

This chapter includes:

Concepts

- ▶ Content Packs Manager on page 364

Tasks

- ▶ How to Create and Manage Content Packs on page 375

Reference

- ▶ Content Pack Content Types on page 378
- ▶ Content Pack Manager Command-Line Interface on page 381
- ▶ Content Packs Manager User Interface on page 386

Troubleshooting and Limitations on page 403

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 378.

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 pack 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 Run-time Service Model (RTSM), you use Packages. For details, see "Package Administration Overview" in the *RTSM 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 367.
- Manage dependencies between content packs. For details, see "Dependencies in Content Packs" on page 367.
- 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 373.
- Import a content pack (definition and content) and the data it references. For details, see "Importing Content Packs" on page 374.

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.**

Importing Content Packs

Content can be imported as predefined or custom.

Automatic import of content packs during installation, BSM startup, or subsequent imports using the **Content -autoUpload** command imports the content of the selected content packs as predefined.

Imports made using the Content manager or using the **ContentManager -import <input_file>** command imports the content of the selected content packs as custom.

Note: Operations Manager *i* artifacts do not support the differentiation between predefined and custom artifacts.

Content Packs Manager Interfaces

The Content Packs manager has two interfaces:

► **BSM Content Packs user interface**

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 User Interface" on page 386.

► **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.

During BSM installation, all predefined Content Pack Definition files are automatically uploaded from the default content pack location:

<BSM Root Dir>/conf/opr/content/<locale>

These content packs are identified as **Predefined**, indicating that they are original and are not modified in any way.

If you want to load a new content pack and have it identified as **Predefined**, use the **-autoUpload** option.

For details, see "Content Pack Manager Command-Line Interface" on page 381.

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 and the relationships between them to be included in a content pack which you can export to another BSM installation.

Note: The content pack definition does not include the CI types themselves. To exchange CI types, use the features provided by the Run-time Service Model (RTSM).

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.

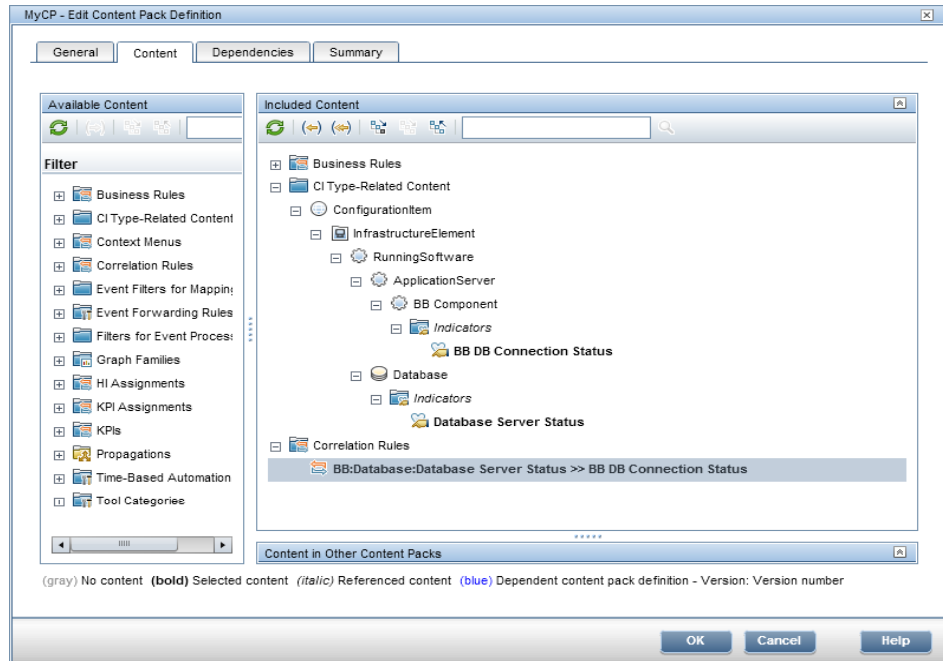
Dependencies in Content Packs

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 **BB DB Connection Status** requires two indicators: the BB Component indicator **BB DB Connection Status** and the Database indicator **Database Server Status**. If you include the correlation rule BB DB Connection Status in a content pack definition and the indicators **BB DB Connection Status** and **Database Server Status** are not included in other content packs, they are automatically included in this content pack definition.



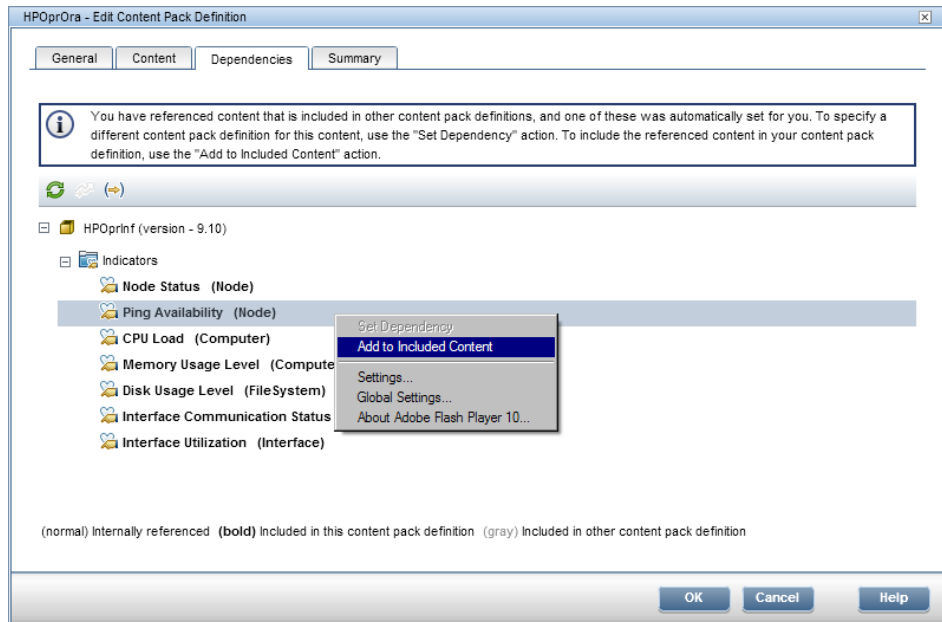
Referencing Dependent Content Included in Another Content Pack

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 **Ping Availability** and now you select the correlation rule **Database Affects WebApp** (which depends on **Ping Availability**) for inclusion in Content Pack B, Content Pack B references the inclusion of **Ping Availability** in Content Pack A.

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

Note: It is not recommended to have content in multiple content packs. It is preferable to set dependencies between content packs.



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.

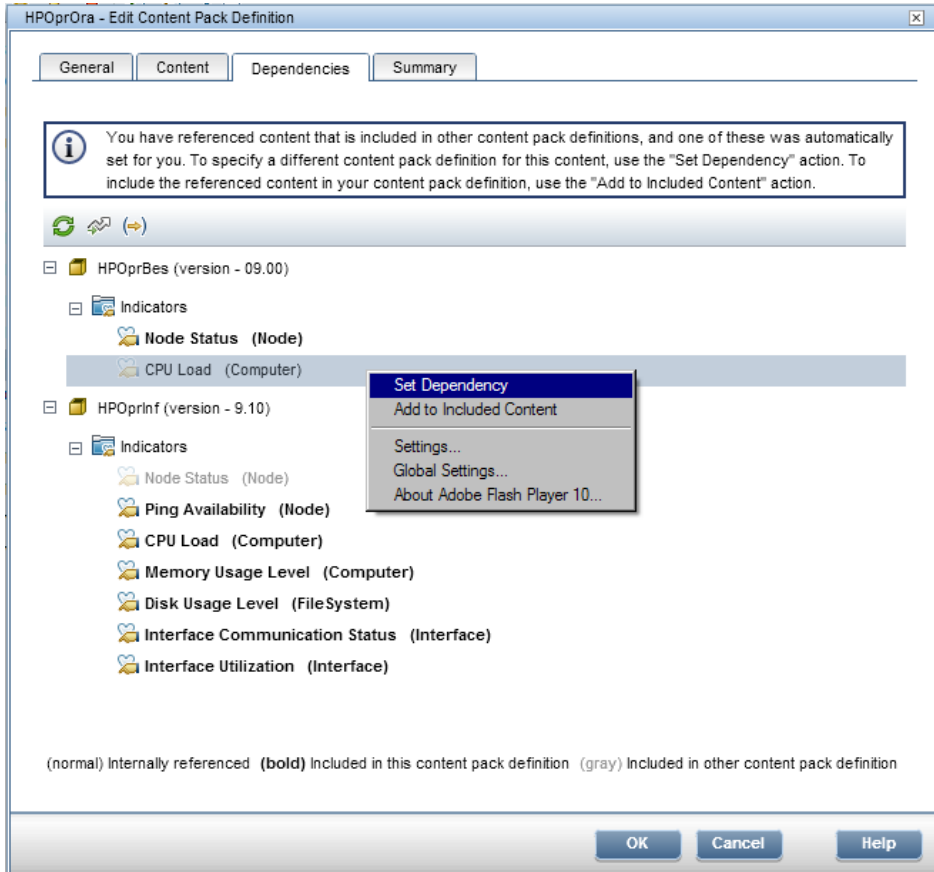
For example, if Content Pack B includes the correlation rule **Database Affects WebApp** and references the dependent indicator **Extend TS** in Content Pack A, and you delete Content Pack A, **Extend TS** is automatically included in Content Pack B.

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 **CPU Load** and you select the correlation rule **Database Affects WebApp** (which depends on **CPU Load**) for inclusion in Content Pack C, you can set dependency in Content Pack C to reference **CPU Load** 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 Run-time Service Model (RTSM) used by the system from which the content pack was exported. If these configuration items are not present in the RTSM 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 RTSM to export and import configuration items.

For details about exporting content packs, see "Export content packs" on page 376.

Importing Content Packs

When starting an import action, you can specify whether to overwrite any existing data or leave the existing data unchanged (**Create**), 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 376. For details about the user interface and the options available in the import operation, see "Import Content Pack Dialog" on page 401.

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 375
- "Export content packs" on page 376
- "Import content packs" on page 376

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, click 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 255 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 and all the available options, see "Create New Content Pack Definition Wizard" on page 392.

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\Content\<locale>`

In a distributed deployment, this directory is located on the Gateway 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.
-

Note: It is not possible to start an import if an import is already running.

For details about the Import Content Pack dialog box, see "Import Content Pack Dialog" on page 401.

Reference

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 Run Book Execution Rules	You can configure BSM to automatically execute Run Books on events that match a configured rule.
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.
Business Rules	<p>Business rules define the logic to be performed (by the Business Logic Engine) to calculate the measurement for a KPI or HI.</p> <p>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.</p> <p>Health indicator rules use sample data to calculate HIs; KPI rules use the results of HI calculations to calculate KPIs.</p>

Content Type	Description
CI Type-Related Content	<p>Configuration items (CIs) represent physical or logical entities in the system. For example, CIs can represent hardware, software, services, business processes, and so on.</p> <p>CI types are categories for each CI. Each CI type provides a template for creating the CI and its associated properties.</p> <p>The CI type tree organizes CI types into a hierarchical format based on the dependencies in your organization's IT environment.</p> <p>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.</p> <p>The CI Type tree includes a number of Content Types that have a reference to a CI Type, such as:</p> <ul style="list-style-type: none"> ➤ Indicators ➤ Mapping Rules ➤ Tool Definitions ➤ CI Type to Graph Families Mappings ➤ Configuration Item TQL View Mappings ➤ Graph Family to CI Type Assignments <p>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.</p>
Context Menus	<p>Menu settings define shortcut menus for CIs, for example to launch configuration tools, start custom tools for specific CI types, and display graphs.</p>
Correlation Rules	<p>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.</p>
Event Filters for Mapping Rules	<p>Filters designed to be use for mapping rules that search filtered events for strings and values which are then used to set an indicator value.</p>

Content Type	Description
Event Filters for User Group assignment	Filters designed to be use with configuring rules to automatically assign incoming events to available user groups.
Event Forwarding Rules	Event Forwarding rules select and forward events to external event managers such as another Operations Manager <i>i</i> instance, HP Operations Manager and or a Help Desk application. These external managers are also referred to as event forwarding targets.
Filters for Event Processing	Filters designed to be use for automated event handling.
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	<p>Health indicators (HIs) provide fine-grained information on the CIs that represent your monitored business elements and processes.</p> <p>HI assignments define which HIs are assigned to new CIs in the system, based on each CI's CI type (CIT).</p>
KPI Assignments	<p>Key performance indicators (KPIs) are high-level indicators of CI performance and availability.</p> <p>KPI assignments define which KPIs are assigned to new CIs in the system, based on each CI's CI type (CIT).</p>
Key Performance Indicators (KPIs)	<p>KPIs are high-level indicators of CI performance and availability, which apply calculation rules to the data provided by HIs to determine CI status.</p> <p>KPIs help you to monitor how well your business is achieving its objectives, and to track critical performance variables over time.</p>

Content Type	Description
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.
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.
Time-Based Automation Rules	Time-based event automation rules enable administrators to configure actions to be executed on events matching a user-defined set of criteria after a specified time.
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>]]
| -a [-uploadFolder <directory>] [-forceReload] [-f]
[-t]) ([[ -ssl] [-server <gateway_server>] [-p <port>] |
[-u <URL>]]) -username <login_name> [-password <password>] [-v]
```

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

Option	Description
-a,-autoUpload	<p>Automatically uploads the Content Pack Definition files from the default content pack directory.</p> <p><i><BSM Root Dir>/conf/opr/content/<locale></i></p> <p>Windows: <i>C:\HPBSM\conf\opr\content\<locale>\</i></p> <p>Linux: <i>/opt/HP/BSM/conf/opr/content/<locale>/</i></p> <p>If you want to upload content pack definitions from an alternative directory on the Gateway Server, specify the directory location using the <code>-uploadFolder <directory></code> option.</p> <p>All content pack definition files in the specified directory are imported in the order of their dependencies. If a content pack definition is already uploaded to the repository, it is not uploaded again.</p> <p>If you want to import new content using modified content packs, apply the <code>-forceReload</code> option. All content packs are assessed and new content is imported. Existing content is not changed.</p> <p>If you want to overwrite uploaded content pack definitions with the content pack definitions currently residing in the specified content pack directory, use the <code>-force-overwrite</code> option.</p> <p>The <code>-test</code> option can also be used with <code>autoUpload</code>.</p> <p>For information about import errors, see the following log file:</p> <p><i><BSM Root Dir>/log/EJBContainer/opr-admin.log</i></p> <p>Windows: <i>C:\HPBSM\log\EJBContainer\opr-admin.log</i></p> <p>Linux: <i>/opt/HP/BSM/log/EJBContainer/opr-admin.log</i></p>

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.
-forceReload	When using the autoUpload function, you want to import new content using modified content packs, apply the -forceReload option. All content packs are assessed and new content is imported. Existing content is not changed.
-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. The default behavior is to ignore any objects in the content pack, excluding the content pack definition, that currently exist on the target system.
-l,-list	Lists the content pack definitions.
-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.

Option	Description
-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 <gateway_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.
-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: <code>http://localhost:80/opr-admin-server</code> Do not specify this option in conjunction with the -server option.
-uploadFolder <directory>	If you want to upload content packs from an alternative directory, specify the directory location using the -uploadFolder <directory> option. For example: <code>ContentManager -a -uploadFolder c:\temp</code>
-username <login_name>	The name of the user, whose account is being used for authentication purposes.

Option	Description
-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.

Content Packs Manager User Interface

This section includes:

- ▶ Content Packs Page on page 387
- ▶ Create New Content Pack Definition Wizard on page 392
- ▶ Import Content Pack Dialog on page 401

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	Use one of the following: <ul style="list-style-type: none"> ▶ 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 375
See also	"Content Packs Manager" on page 364

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
	<p>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).</p>
	<p>New Item. Opens the Create New Content Pack Definition wizard. For details about the wizard, see "Create New Content Pack Definition Wizard" on page 392.</p>
	<p>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.</p> <p>Alternatively, double-click a section in the Details pane to open the appropriate tab in the Edit Content Pack Definition dialog box.</p> <p>For details, see "Create New Content Pack Definition Wizard" on page 392.</p>
	<p>Delete Item. Deletes the selected content pack definition (but not referenced content such as indicators and KPIs) from the list of definitions displayed.</p>

UI Elements	Description
	<p>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.</p> <p>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 401.</p>
	<p>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.</p>
	<p>Get Help. Displays help about the active window, pane, or dialog box.</p>

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	<p>Displays a summary of the selected content pack definition's contents, including:</p> <ul style="list-style-type: none"> ▶ 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	<p>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.</p>


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	Use one of the following: <ul style="list-style-type: none"> ▶ Admin > Platform > Content Packs ▶ Admin > Operations Management > Manage Content > Content Packs and then click 
Relevant tasks	"How to Create and Manage Content Packs" on page 375
Wizard map	This wizard contains: General Page > Content Page > Dependencies Page > Summary Page
See also	"Content Packs Manager" on page 364

General Page

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


Important information	<ul style="list-style-type: none"> ▶ General information about this wizard is available here: "Create New Content Pack Definition Wizard" on page 392. ▶ 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 364

User interface elements are described below:



UI Elements	Description
ID	<p>No action required. The content pack ID is assigned automatically when the content pack is first created.</p> <p>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.</p>
Display Name	<p>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.</p>
Name	<p>Name of the content pack definition. The name must be unique, and is limited to a maximum length of 255 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.</p> <p>When you export the content pack, this is the default file name for the XML file, with OMi Content Pack - as a prefix.</p>
Version	<p>Required, free text field. Use to control versions of your content packs. It is limited to a maximum length of 255 characters.</p>
Description	<p>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.</p>











Content Page





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

Important information	<ul style="list-style-type: none"> ▶ General information about this wizard is available here: "Create New Content Pack Definition Wizard" on page 392. ▶ This wizard page appears as the Content tab in the Edit Content Pack Definition dialog box that opens when you click  .
Wizard map	<p>The Create New Content Pack Definition Wizard contains:</p> <p>General Page > Content Page > Dependencies Page > Summary Page</p>
See also	"Content Packs Manager" on page 364

User interface elements are described below:

UI Elements	Description
	<p>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).</p>
	<p>Add to Included Content: Adds the selected item(s) to the list of included content.</p> <p>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.</p> <p>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.</p>

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
	<p>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.</p> <p>The search string must be at least three characters long. Searching is automatically 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 can be found by clicking on the  button.</p>
<p>Available Content</p>	<p>Hierarchical list representing the available content in your IT environment.</p> <p>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.</p> <p>Color coding:</p> <ul style="list-style-type: none"> ➤ Folder with no content: gray ➤ Selected content: bold ➤ Referenced content: italic ➤ Dependent content pack definition with version number: blue <p>For details, see "Content Pack Content Types" on page 378.</p>
<p>Filter: Show only CI types with assigned content</p>	<p>Filters the CI Types tree to display only CI types that have content assigned to them.</p>

UI Elements	Description
Included Content	<p>List of content selected for inclusion in a content pack, along with any dependent content.</p> <p>Tip: To exclude an item, select an item (or group of items) and select the Exclude button.</p> <p>Color coding:</p> <ul style="list-style-type: none"> ▶ Folder with no content: gray ▶ Selected content: bold ▶ Referenced content: italic ▶ Dependent content pack definition with version number: blue
Content in Other Content Packs	<p>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.</p>

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 user interface. 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	<ul style="list-style-type: none"> ▶ General information about this wizard is available here: "Create New Content Pack Definition Wizard" on page 392. ▶ This wizard page appears as the Dependencies tab in the Edit Content Pack Definition dialog box that opens when you click .
Wizard map	<p>The Create New Content Pack Definition Wizard contains:</p> <p>General Page > Content Page > Dependencies Page > Summary Page</p>
See also	<p>"Content Packs Manager" on page 364</p> <p>"Dependencies in Content Packs" on page 367</p>

User interface elements are described below:

UI Elements	Description
	<p>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).</p>
	<p>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.”</p> <p>To choose which content pack to reference, select the dependent content in that content pack and click Set Dependency.</p> <p>The dependent content in the referenced content pack is displayed in bold, indicating that dependency has been set on it.</p>
	<p>Add to Included Content. Adds the selected dependent content to the list of content included in this content pack.</p>

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	<ul style="list-style-type: none"> ▶ General information about this wizard is available here: "Create New Content Pack Definition Wizard" on page 392. ▶ This wizard page appears as the Summary tab in the Edit Content Pack Definition dialog box that opens when you click  .
Wizard map	<p>The Create New Content Pack Definition Wizard contains:</p> <p>General Page > Content Page > Dependencies Page > Summary Page</p>
See also	"Content Packs Manager" on page 364

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.
Referenced Content Included in This Content Pack	Displays a list of the referenced content, grouped by content type, included in the selected content pack definition.

UI Elements	Description
Referenced 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	Use one of the following: <ul style="list-style-type: none"> ▶ Admin > Platform > Content Packs ▶ Admin > Operations Management > Manage Content > Content Packs and then click  .
Relevant tasks	"Import content packs" on page 376

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	<p>Allows BSM to overwrite any existing content pack definition or the items it references during the import process.</p> <p>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.</p>
Create	Imports all objects contained within the content pack, including the content pack definition, and ignores any objects in the content pack, excluding the content pack definition, that currently exist on 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.

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 Create options are correctly specified before starting the import.

18

Downtime Management

This chapter includes:

Concepts

- ▶ Downtime Management — Overview on page 406

Tasks

- ▶ How to Create and Manage Downtimes for CIs on page 409

Reference

- ▶ Downtime REST Service on page 412
- ▶ Downtime Management User Interface on page 416

Troubleshooting and Limitations on page 431

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. BSM 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

This section includes the following topics:

- ▶ "Downtime Actions" on page 407
- ▶ "Events in Operations Management" on page 408
- ▶ "Downtime REST Service" on page 408

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" on page 553 in *Using Operations Management*.

Downtime REST Service

You can retrieve, update, create, and delete downtimes through a RESTful Web service running on the Gateway Server. For details, see "Downtime REST Service" on page 412.

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 409
- ▶ "Configure how events are handled in Operations Management — optional" on page 410
- ▶ "Run the Create Downtime wizard" on page 410
- ▶ "Results" on page 410

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 CI's that impact the CI's you selected. In some cases, these CI's are also affected by downtime. To understand the downtime impact model, see the BSMDowntime_topology TQL in the RTSM Modeling Studio. You can only select 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:
 - ▶ Take no actions
 - ▶ Suppress alerts and close events
 - ▶ Enforce downtime on KPI calculations; suppress alerts and close events
 - ▶ Enforce downtime on Reports and KPI calculations; suppress alerts and close events
 - ▶ Stop monitoring (BPM and SiteScope); enforce downtime on Reports & KPI calculations; suppress alerts and close events (affects all related SLAs)

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 Operations Management*.

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 421.

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 417.

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 REST Service

You can use a RESTful Web service running on the Gateway Server to retrieve, update, create, and delete downtimes. HTTP requests can be entered in your browser, and combinations of HTTP requests and XML commands in a REST client. Service authentication is based on basic authentication.

Supported HTTP Requests

The downtime REST service supports the following HTTP requests:

Note: CustomerID is always 1 except in the case of HP SaaS customers.

Action	HTTP Command
Retrieve all downtimes	http://<HPBSM server>/topaz/bsmservices/customers/[customerid]/downtimes
Retrieve a specific downtime	http://<HPBSM server>/topaz/bsmservices/customers/[customerid]/downtimes/[downtimeid]
Update a downtime using http PUT	http://<HPBSM server>/topaz/bsmservices/customers/[customerid]/downtimes/[downtimeid] + XML of the downtime (see "Downtime XML Example" on page 414)

Action	HTTP Command
Create downtime using http POST	<pre>http://<HPBSM server>/topaz/bsmservices/customers/[customerId]/downtimes + XML of the downtime (see "Downtime XML Example" on page 414) Note: Successful creation of the downtime causes a return of the newly created downtime in XML format, including the downtime ID.</pre>
Delete downtime using http DELETE	<pre>http://<HPBSM server>/topaz/bsmservices/customers/[customerId]/downtimes/[downti meld]</pre>

Allowed Downtime Actions

Use the XML commands listed for the following downtime actions:

Action Description	XML Command
Take no actions	<code><action name="REMINDER"/></code>
Suppress alerts and close events	<code><action name="SUPPRESS_NOTIFICATIONS"/></code>
Enforce downtime on KPI calculations; suppress alerts and close events (continue monitoring)	<code><action name="ENFORCE_ON_KPI_CALCULATION"/></code>
Enforce downtime on Reports and KPI calculations; suppress alerts and close events (continue monitoring)	<code><action name="ENFORCE_ON_REPORTS"/></code>
Enforce downtime on Reports and KPI calculations; suppress alerts and close events (continue monitoring), including all SLAs	<pre><action name="ENFORCE_ON_REPORTS"> <propGroup name="SLA" value="ALL"/> </action></pre>

Action Description	XML Command
Enforce downtime on Reports and KPI calculations; suppress alerts and close events (continue monitoring), including specific SLA	<pre><action name="ENFORCE_ON_REPORTS"> <propGroup name="SLA" value="SELECTED"> <prop>dda3fb0b20c0d83e078035ee1c005201 </prop> </propGroup> </action></pre>
Stop active monitoring (BPM and SiteScope); enforce downtime on Reports & KPI calculations; suppress alerts and close events	<pre><action name="STOP_MONITORING"/></pre>

Downtime XML Example

The following fields may not exceed the maximum lengths specified:

- Name: 200 characters
- Description: 2000 characters
- Approver: 50 characters

```
<downtime userId="1" planned="true"
id="8898e5a5dbcdc953e04037104bf5737c">

  <name>The name of the downtime</name>
  <action name="ENFORCE_ON_REPORTS">
</action>
  <approver>The approver name</approver>
  <category>1</category>
  <notification>
    <recipients>
      <recipient id="24"/>
      <recipient id="22"/>
      <recipient id="21"/>
    </recipients>
  </notification>
  <selectedCIs>
    <ci>
      <id>ac700345b47064ed4fbb476f21f95a76</id>
```

```

        <viewName>End User Monitors</viewName>
    </cj>
</selectedCIs>
    <schedule xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="WeeklyScheduleType">
        <type>WEEKLY</type>
        <startDate>2010-06-10T15:40:00+03:00</startDate>
        <timeZone>Europe/Zurich</timeZone>
        <days>
            <selectedDays>WEDNESDAY</selectedDays>
            <selectedDays>THURSDAY</selectedDays>
            <selectedDays>FRIDAY</selectedDays>
            <selectedDays>SATURDAY</selectedDays>
        </days>
        <startTimeInSecs>52800</startTimeInSecs>
        <durationInSecs>300</durationInSecs>
    </schedule>
</downtime>

```

Scheduling

Keep the following in mind when setting the downtime schedule:

- ▶ Retroactive downtime is not supported. You cannot:
 - ▶ Create a downtime that is scheduled in the past.
 - ▶ Delete a downtime that has started or that occurred in the past.
 - ▶ Modify a downtime that has started or that occurred in the past.
- ▶ The date format of startDate/endDate is: **yyyy-MM-dd'T'HH:mm:ssZ**
- ▶ For weekly and monthly downtimes, the startDate and endDate should be defined at midnight. For example:
 - ▶ <startDate>2010-07-24T00:00:00+03:00</startDate>
 - ▶ <endDate>2010-09-04T00:00:00+03:00</endDate>

Example of a Downtime Schedule with One Occurance

```

<schedule xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="OnceScheduleType">
    <type>ONCE</type>
    <startDate>2010-06-08T14:40:00+03:00</startDate>
    <endDate>2010-06-08T14:45:00+03:00</endDate>
    <timeZone>Asia/Tokyo </timeZone>

```

```
</schedule>
```

Example of a Weekly Downtime Schedule

```
<schedule xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="WeeklyScheduleType">
  <type>WEEKLY</type>
  <startDate>2010-06-10T15:40:00+03:00</startDate>
  <timeZone>Europe/Zurich</timeZone>
  <days>
    <selectedDays>WEDNESDAY</selectedDays>
    <selectedDays>THURSDAY</selectedDays>
    <selectedDays>FRIDAY</selectedDays>
    <selectedDays>SATURDAY</selectedDays>
  </days>
  <startTimeInSecs>52800</startTimeInSecs>
  <durationInSecs>300</durationInSecs>
</schedule>
```

Example of a Monthly Downtime Schedule

```
<schedule xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="MonthlyScheduleType">
  <type>MONTHLY</type>
  <startDate>2010-06-10T14:40:00+03:00</startDate>
  <timeZone>America/Montevideo</timeZone>
  <days>
    <selectedDays>WEDNESDAY</selectedDays>
    <selectedDays>THURSDAY</selectedDays>
    <selectedDays>FRIDAY</selectedDays>
    <selectedDays>SATURDAY</selectedDays>
  </days>
  <startTimeInSecs>52800</startTimeInSecs>
  <durationInSecs>300</durationInSecs>
</schedule>
```

Downtime Management User Interface

This section includes:

- ▶ Downtime Management Page on page 417
- ▶ New Downtime Wizard on page 421









Downtime Management Page

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

To access:	Select Admin > Platform > Downtime Management
Important information	<ul style="list-style-type: none"> ➤ 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 445. ➤ 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: <ul style="list-style-type: none"> ➤ 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 409
See also	"Downtime Management — Overview" on page 406

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 421.
	Edit downtime. Opens the Edit Downtime 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 421.
	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 426.
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.
Next Occurrence	The date and time of the next occurrence of the downtime. This field is updated automatically.

UI Element (A–Z)	Description
Scheduling	Displays the: <ul style="list-style-type: none"> ▶ Date, time, time zone, and duration For recurring downtimes, also displays: <ul style="list-style-type: none"> ▶ What day of the week or month the downtime is scheduled to recur ▶ Range of recurrence
Status	Displays whether the downtime is currently: <ul style="list-style-type: none"> ▶ 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
<p>Category</p>	<p>The category assigned to the downtime. Options include:</p> <ul style="list-style-type: none"> ➤ Application installation ➤ Application maintenance ➤ Hardware installation ➤ Hardware maintenance ➤ Network maintenance ➤ Operating system reconfiguration ➤ Other ➤ Security issue <p>You can also create your own customized categories using Infrastructure Settings.</p> <p>To add a custom downtime category, select Admin > Platform > Setup and Maintenance > Infrastructure Settings:</p> <ul style="list-style-type: none"> ➤ Select Foundations. ➤ Select Downtime. ➤ In the Downtime - General settings table, edit the Downtime categories 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.
<p>Planned</p>	<p>Indicates whether the downtime is planned or not.</p>

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 409
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 406

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 406

User interface elements are described below:

UI Element	Description
Downtime Name	Cannot exceed 200 characters.
Downtime Description	This description also appears in the "Downtime Information Area" in <i>Reports</i> .


UI Element	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	<p>Select a category from the drop-down menu. This category describes the reason for the downtime.</p> <p>You can also create your own customized categories using Infrastructure Settings.</p> <p>To add a custom downtime category, select Admin > Platform > Setup and Maintenance > Infrastructure Settings:</p> <ul style="list-style-type: none"> ➤ 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	<p>This New Downtime Wizard contains:</p> <p>Properties Page > Select CIs Page > Scheduling Page > Action Page > Notification Page > Preview Page</p>
See also	"Downtime Management — Overview" on page 406

User interface elements are described below:

UI Element (A-Z)	Description
Available CIs	<p>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.</p> <p>Highlight a CI from the view to move it to the Selected CIs list. Hold the Ctrl key for selecting multiple CIs.</p> <p>All views that the user has permission to see may be selected. You can select CIs only of the following CI types:</p> <ul style="list-style-type: none"> ➤ node ➤ running software ➤ business process ➤ business application ➤ ci collection ➤ infrastructure service ➤ business service
Selected CIs	<p>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.</p>

 **Scheduling Page**

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

<p>Important information</p>	<ul style="list-style-type: none"> ▶ 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 <p>To cancel a recurring downtime that has already occurred at least once, edit the downtime and modify this field.</p>
<p>Wizard map</p>	<p>This New Downtime Wizard contains:</p> <p>Properties Page > Select CIs Page > Scheduling Page > Action Page > Notification Page > Preview Page</p>
<p>See also</p>	<p>"Downtime Management — Overview" on page 406</p>

User interface elements are described below:

UI Element	Description
Time of occurrence	<ul style="list-style-type: none"> ▶ 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	<p>Select one of the following:</p> <ul style="list-style-type: none"> ▶ 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	<p>If you selected Weekly or Monthly:</p> <ul style="list-style-type: none"> ▶ 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 406

User interface elements are described below:

UI Element	Description
Take no actions	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 alerts and close events	<ul style="list-style-type: none"> ▶ No alerts or their associated notifications or actions are sent for any of the CIs associated with the downtime. ▶ By default, events are submitted as closed. If OMi is installed, event handling in downtime can be configured in Admin > Operations Management > Tune Operations Management > Downtime Behavior, and overrides the setting here. ▶ Monitoring continues, and reports, status in Service Health, and SLAs are updated. <p>Note: During the downtime period, the affected CI may change its status, and the status change may trigger the relevant CI Status alert.</p>

UI Element	Description
Enforce downtime on KPI calculations; suppress alerts and close events	<ul style="list-style-type: none"><li data-bbox="621 222 1259 314">▶ KPI calculations are not run and status in Service Health is not updated, and instead display the downtime for the CI.<li data-bbox="621 326 1259 418">▶ No alerts or their associated notifications or actions are sent for any of the CIs associated with the downtime.<li data-bbox="621 430 1259 586">▶ By default, events are submitted as closed. If OMi is installed, event handling in downtime can be configured in Admin > Operations Management > Tune Operations Management > Downtime Behavior, and overrides the setting here.<li data-bbox="621 598 1259 621">▶ Reporting and monitoring continue. SLAs are updated.

UI Element	Description
<p>Enforce downtime on Reports and KPI calculations; suppress alerts and close events</p>	<ul style="list-style-type: none"> ➤ 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 alerts or their associated notifications or actions are sent for any of the CIs associated with the downtime. ➤ By default, events are submitted as closed. If OMi is installed, event handling in downtime can be configured in Admin > Operations Management > Tune Operations Management > Downtime Behavior, and overrides the setting here. ➤ Monitoring continues.


UI Element	Description
<p>Stop active monitoring (BPM & SiteScope); enforce downtime on Reports & KPI calculations; suppress alerts and close events (affects all related SLAs)</p>	<ul style="list-style-type: none"> ▶ Business Process Monitor and SiteScope monitoring stops. ▶ Report data is not updated and the downtime is displayed for the associated CIs. ▶ 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 alerts or their associated notifications or actions are sent for any of the CIs associated with the downtime. ▶ By default, events are submitted as closed. If OMi is installed, event handling in downtime can be configured in Admin > Operations Management > Tune Operations Management > Downtime Behavior, and overrides the setting here. <p>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.</p>

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 406

User interface elements are described below:

UI Element	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 579.
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 406

User interface elements are described below:

UI Element	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 includes the following topics:

- "Editing Downtimes" on page 432
- "Downtime and Daylight Saving Time" on page 432

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 occurred at least once, edit the downtime's **End by** date in the Scheduling page.

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 436.

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
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

Example	Downtime as Set/With DST Change		Start Time	End Time	Duration
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
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

Part IV

Users, Permissions, and Recipients

19

User Management

This chapter includes:

Concepts

- ▶ User Management — Overview on page 443
- ▶ Permissions Overview on page 445
- ▶ Group and User Hierarchy on page 451
- ▶ Customizing User Menus on page 453

Tasks

- ▶ How to Configure Users and Permissions — Workflow on page 454
- ▶ How to Configure Users and Permissions — Use-Case Scenario on page 456
- ▶ How to Assign Permissions on page 466
- ▶ How to Configure Group and User Hierarchy on page 468
- ▶ How to Remove Security Officer Status Using the JMX Console on page 470
- ▶ How to Customize User Menus on page 471
- ▶ How to Customize User Menus — Use-Case Scenario on page 473
- ▶ How to Add a Custom Pager or SMS Service Provider on page 477

Reference

- ▶ User Management Roles Applied Across BSM on page 480
- ▶ User Management Roles Applied to Specific Contexts on page 519
- ▶ User Management Operations on page 525

- ▶ User Management User Interface on page 553

Concepts

User Management — Overview

You use the User Management interface to:

- ▶ **Configure BSM 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 BSM. 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 557.

For details on creating groups and users, see "Groups/Users Pane" on page 570.

- ▶ **Define a superuser.** One superuser is defined for every installation of BSM. This superuser's login name is **admin** and the initial password for this account is specified in the Setup and Database Configuration utility. 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 608.

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 466.

- ▶ **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 578.
- ▶ **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 445.
- ▶ **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 451.
- ▶ **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 453.

Permissions Overview

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

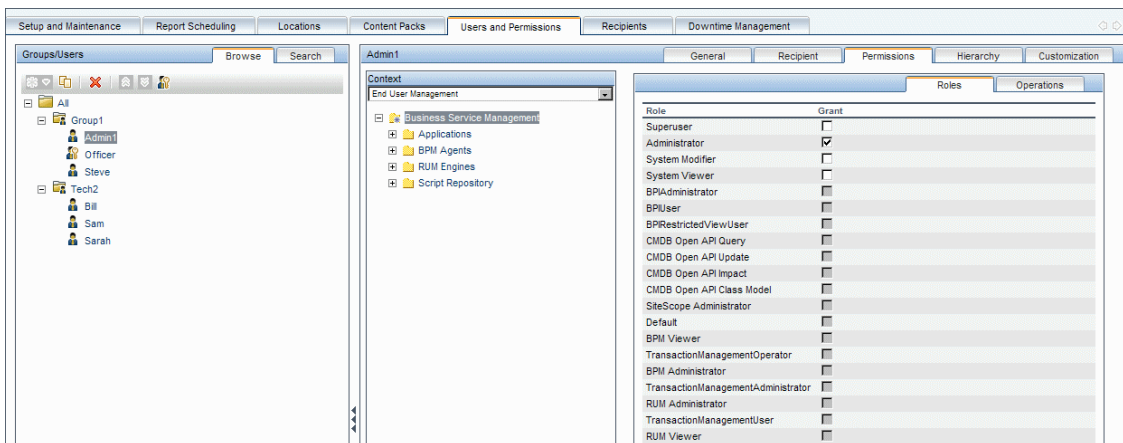
Granting permissions has the following components:

- ▶ 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 446.
- ▶ The roles and operations area on the right side of the page. For details on roles, see "Roles" on page 449. For details on operations, see "Operations" on page 450.

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



For details on assigning permissions, see "How to Assign Permissions" on page 466.

Note:

- ▶ If you have upgraded from a previous version of BSM 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 449.
 - ▶ You can export users and groups, together with their assigned roles, from one BSM machine to another. For details, contact HP Software Support.
-

Understanding Permissions Resources

BSM 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 BSM 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 446
- ▶ "Guidelines for Working with Resources" on page 449

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:

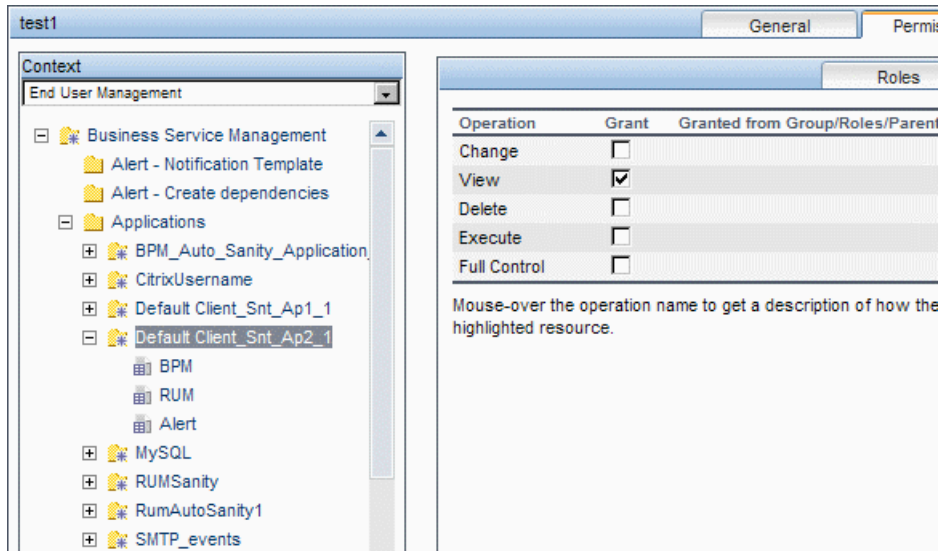
The Category resource includes all categories defined in End User Management Administration. **Change** permissions granted on the categories resource enables a user to modify all the categories defined in the system. You cannot grant or remove permissions for specific categories, only for every category 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.



Guidelines for Working with Resources

- The Business Service Management resource refers to all contexts in BSM.
- Only roles and not operations can be applied to the Business Service Management resource. For details, see "Roles" on page 449.
- 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

BSM 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 450.

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 480.

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 BSM, see "User Management Operations" on page 525.

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 *Using End User Management*.

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 570.

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 470.

Note: If you are working with SaaS and need to remove the Security Officer status, you need to enter the relevant customer ID at the top of the page. For assistance, please contact HP support.

Group and User Hierarchy

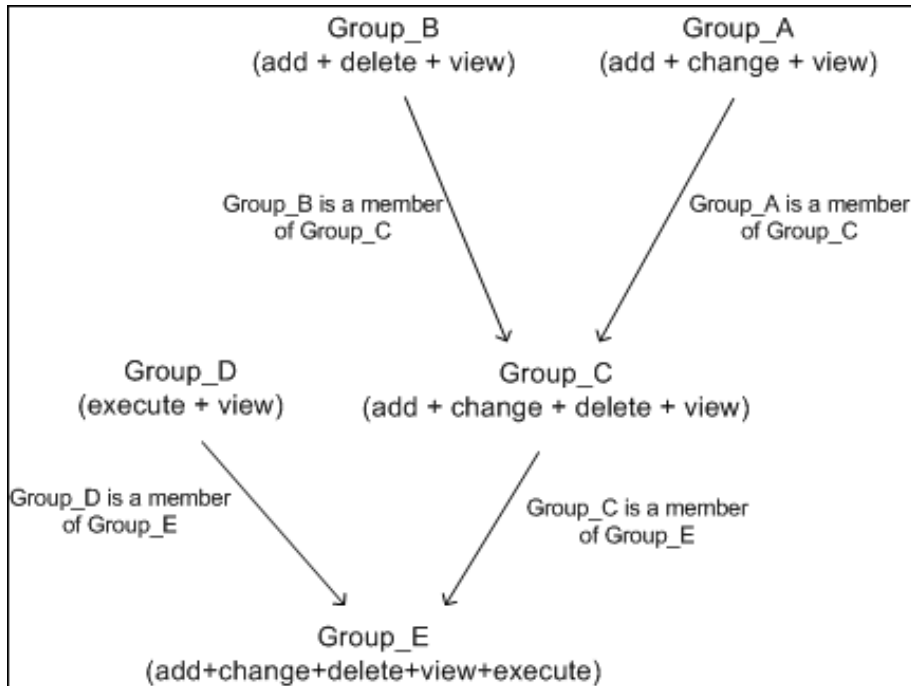
You can nest groups to make managing user and group permissions easier. Instead of assigning access permissions to each group one at a time, you can nest a group to inherit the permissions of its direct parent.

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.



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 468.

Customizing User Menus

You can customize user menus to:

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

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

For details on customizing user menus, see "How to Customize User Menus" on page 471.

You customize user menus on the Customization tab. For details on the Customization tab user interface, see "Customization Tab (User Management)" on page 555.

Note: For the Service Health and Operations Management applications, you cannot define user access to specific pages; you can only enable or disable user access at the application level.

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 456.

This task includes the following steps:

- "Prerequisites" on page 455
- "Create Groups" on page 455
- "Assign Permissions to Groups" on page 455
- "Create Users" on page 456
- "Configure User and Group Hierarchy" on page 456
- "Customize User Settings" on page 456
- "Configure and Manage Recipients" on page 456

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 BSM. 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 446.

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 553.

3 Assign Permissions to Groups

BSM 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 466.

4 Create Users

You create users and then place them into the appropriate groups. For user interface details, see "Groups/Users Pane" on page 570.

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 468.

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 471.

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 579.

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 454.

This scenario includes the following steps:

- ▶ "Mapping Out Users and Groups" on page 457

- "Creating Groups" on page 458
- "Assigning Permissions to Groups" on page 458
- "Creating Users" on page 459
- "Configuring User and Group Hierarchy" on page 460
- "Customizing User Settings" on page 464

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 BSM, 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.

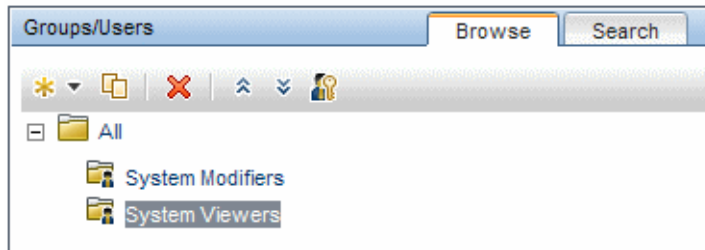
2 Creating Groups



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

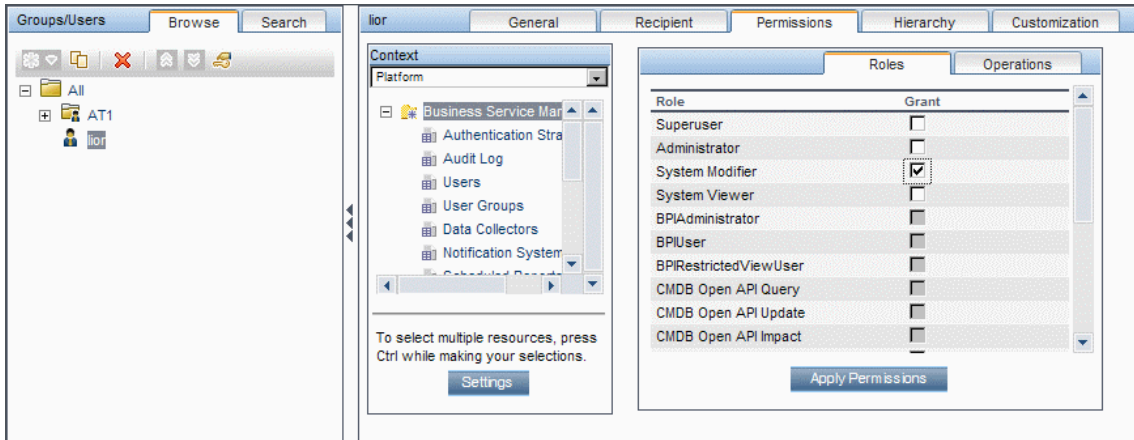
The **Groups/Users** pane appears as follows:



3 Assigning Permissions to Groups

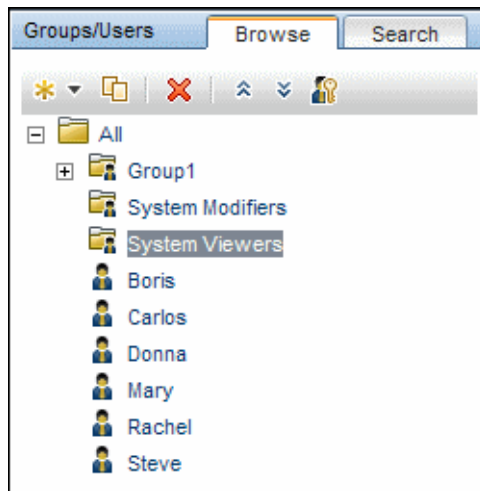
Once the groups have been created, Jane assigns the relevant permission levels to the groups. After selecting **System Modifiers** in the **Groups/Users** pane, she navigates to the **Permissions** tab in the **Information** pane, and chooses the Root instance (**Business Service Management**) from any 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:



4 Creating Users

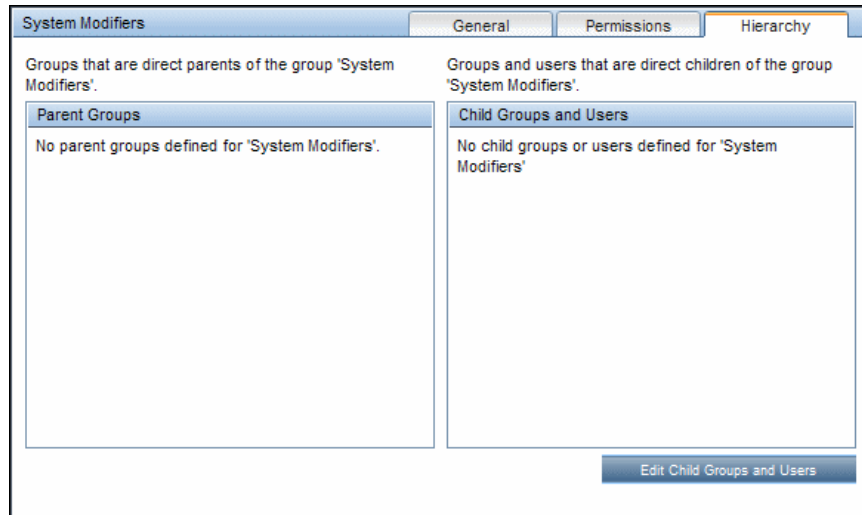
Jane must now create users to nest within the groups, in accordance with the desired permission levels of the individual users. She clicks the **New Group/User** button in the **Groups/Users** pane and while on the Root group, (**All**), she selects **Create User** and configures settings for each new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



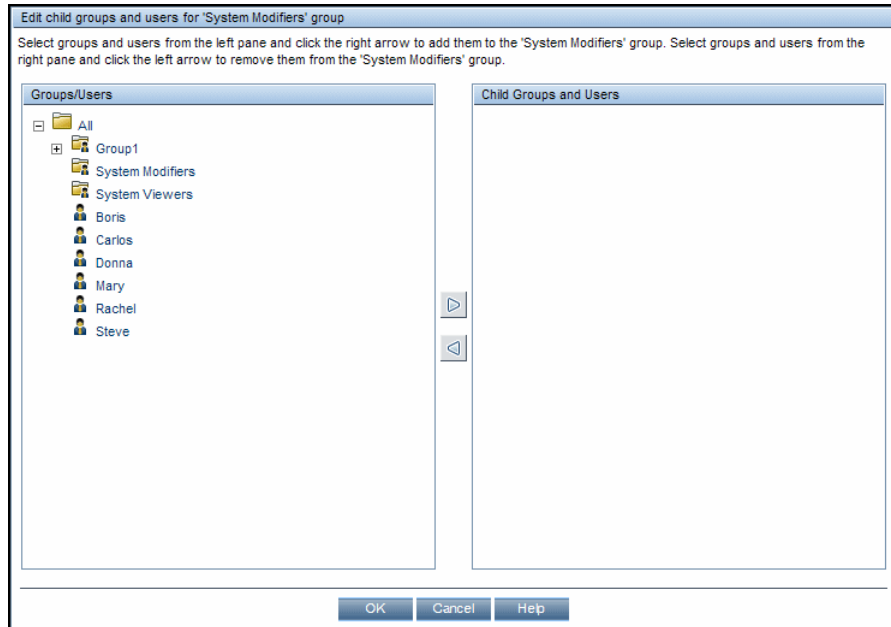
5 Configuring User and Group Hierarchy

Now that Jane has created users authorized to access BSM, she assigns their permission level by nesting them within the appropriate group.

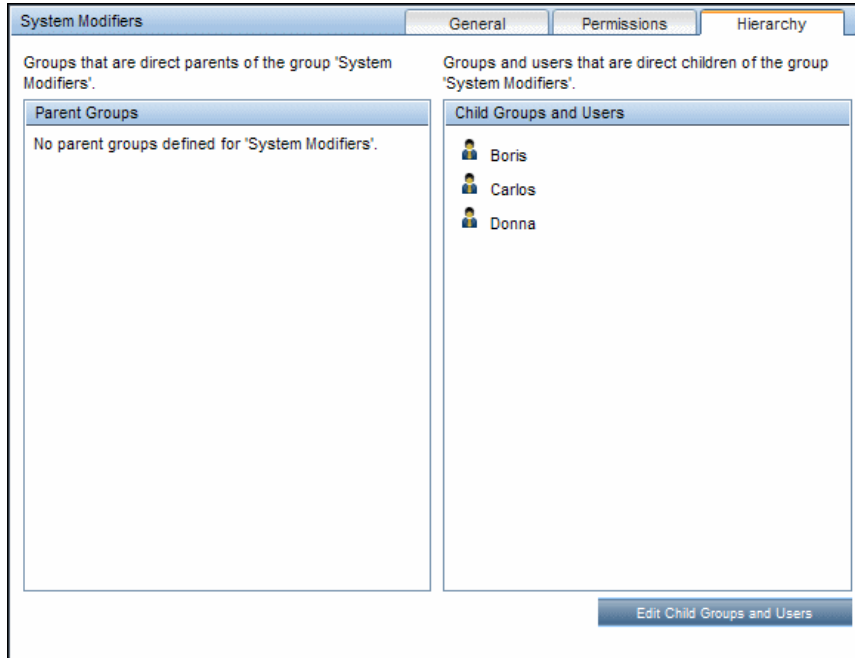
She selects the **System Modifiers** group from the **Groups/Users** pane to nest the appropriate users in this group. Jane then selects the **Hierarchy** tab from the **Information** pane on the right side of the page. The hierarchy tab indicates that the System Modifiers group has no child groups, as follows:



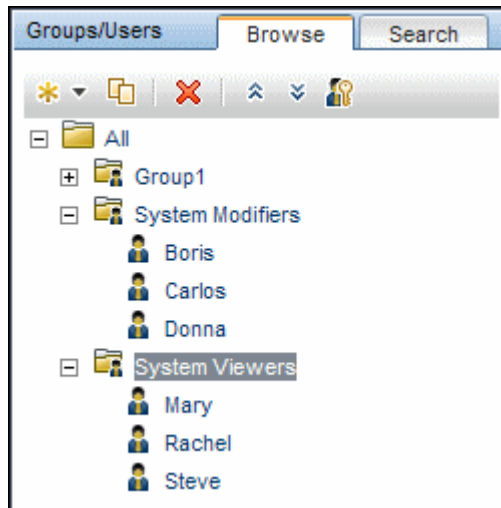
Jane clicks the **Edit Child Groups and Users** button to open the Edit Child Groups and Users dialog box:



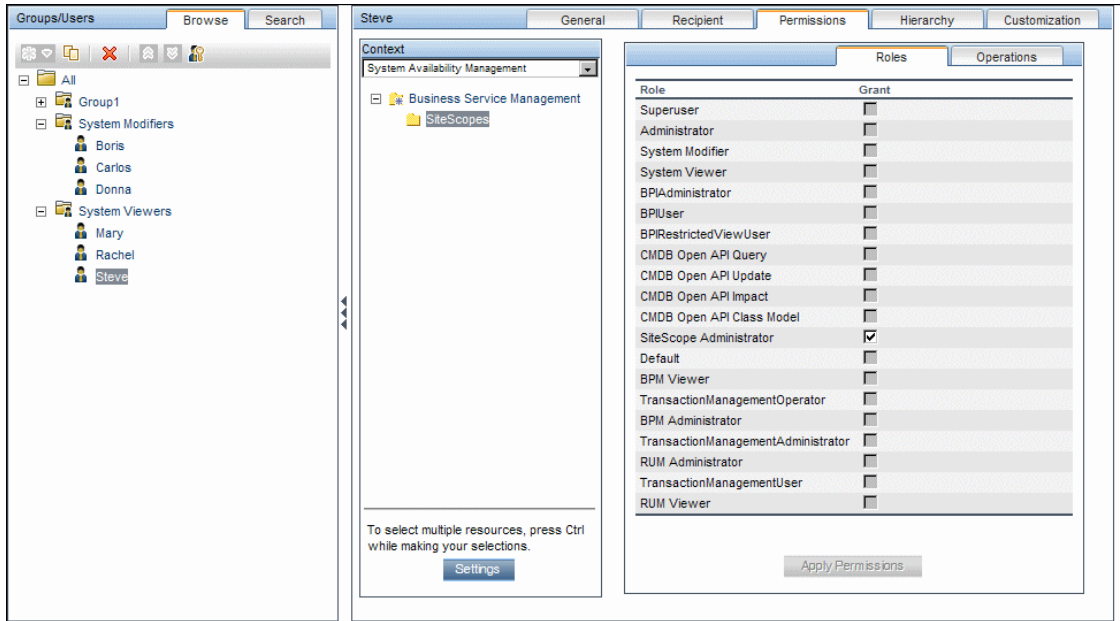
She then selects the relevant users from the **Groups/Users** pane and clicks the right arrow to move them to the **Child Groups and Users** pane. The Hierarchy tab indicates that these users are nested within the System Modifiers group, as follows:



After following the same procedure to nest the relevant users in the System Viewers group, the **Groups/Users** pane is displayed as follows:



Since Steve has the added permission level of SiteScope Administrator, Jane selects the username of the user in the **Groups/Users** pane whom she wants to give the added permission level of SiteScope Administrator, and in the Permissions tab, selects the **System Availability Management** context. After selecting a resource, she then selects **SiteScope Administrator** from the **Roles** tab, and clicks **Apply Permissions**. The resulting screen appears as follows:



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 BSM. 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 BSM 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:

The screenshot shows the 'Customization' tab for user 'Boris'. It is divided into two main sections: 'Contexts' and 'Pages and Tabs'.

Contexts: A list of 20 contexts with checkboxes. 'Applications - Transaction Management' is selected and highlighted.

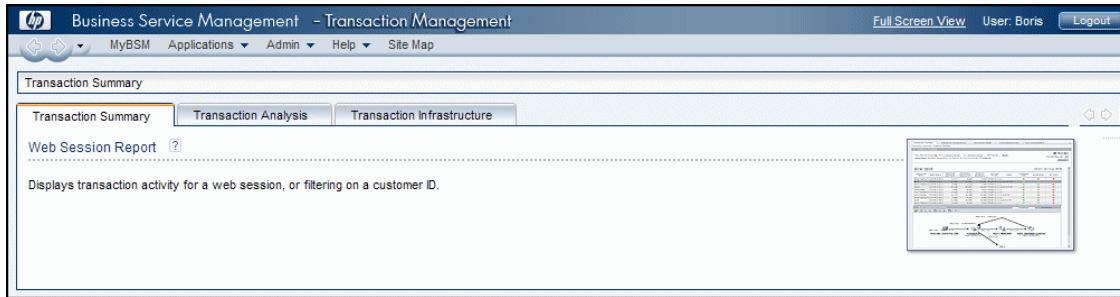
Context	Checked
Applications - MyBSM	<input checked="" type="checkbox"/>
Applications - Service Health	<input checked="" type="checkbox"/>
Applications - Service Level Management	<input checked="" type="checkbox"/>
Applications - End User Management	<input checked="" type="checkbox"/>
Applications - Transaction Management	<input checked="" type="checkbox"/>
Applications - System Availability Management	<input checked="" type="checkbox"/>
Applications - Business Service Management for Siebel	<input checked="" type="checkbox"/>
Applications - Application Management for SOA	<input checked="" type="checkbox"/>
Applications - User Reports	<input checked="" type="checkbox"/>
Admin - Service Health	<input checked="" type="checkbox"/>
Admin - Service Level Management	<input checked="" type="checkbox"/>
Admin - Operations Management	<input checked="" type="checkbox"/>
Admin - End User Management	<input checked="" type="checkbox"/>
Admin - System Availability Management	<input checked="" type="checkbox"/>
Admin - ODB Administration	<input checked="" type="checkbox"/>
Admin - Business Service Management for Siebel Administration	<input checked="" type="checkbox"/>
Admin - Platform	<input checked="" type="checkbox"/>
Admin - Integrations	<input checked="" type="checkbox"/>
Admin - Personal Settings	<input checked="" type="checkbox"/>
Help - Site Map	<input checked="" type="checkbox"/>

Pages and Tabs: A list of 11 pages and tabs with checkboxes. 'Transaction Summary' is selected and highlighted. 'Transaction Topology', 'Aggregated Topology', and 'Component Topology Analysis' are unchecked.

Page and Tab	Checked
Transaction Summary	<input checked="" type="checkbox"/>
Transaction Summary	<input checked="" type="checkbox"/>
Web Session Report	<input checked="" type="checkbox"/>
Transaction Analysis	<input checked="" type="checkbox"/>
Transaction Over Time	<input checked="" type="checkbox"/>
Transaction Tracking Report	<input checked="" type="checkbox"/>
Event Analysis	<input checked="" type="checkbox"/>
Transaction Topology	<input type="checkbox"/>
Aggregated Topology	<input type="checkbox"/>
Component Topology Analysis	<input type="checkbox"/>
Transaction Infrastructure	<input checked="" type="checkbox"/>
Application Server Statistics Report	<input checked="" type="checkbox"/>
User-created Reports	<input type="checkbox"/>

Buttons: OK, Cancel

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



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 BSM.

This task includes the following steps:

- "Prerequisites" on page 467
- "Select a Group or User" on page 467
- "Select a Context" on page 467
- "Assign a Role" on page 467
- "Assign Operations — Optional" on page 467
- "Configure Permissions Settings — Optional" on page 467

1 Prerequisites

Ensure that groups and users are configured in your system. For user interface details, see "Groups/Users Pane" on page 570.

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 565.

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 480.

5 Assign Operations — Optional

Optionally, you can assign individual operations in the **Operations** tab that the group or user can perform in BSM. For details on the available operations, see "User Management Operations" on page 525.

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 564.

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 560.

This task includes the following steps:

- "Prerequisites" on page 468
- "View Group and User Hierarchy" on page 468
- "Nest Groups and Users" on page 468
- "Results" on page 469

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 570.

2 View Group and User Hierarchy

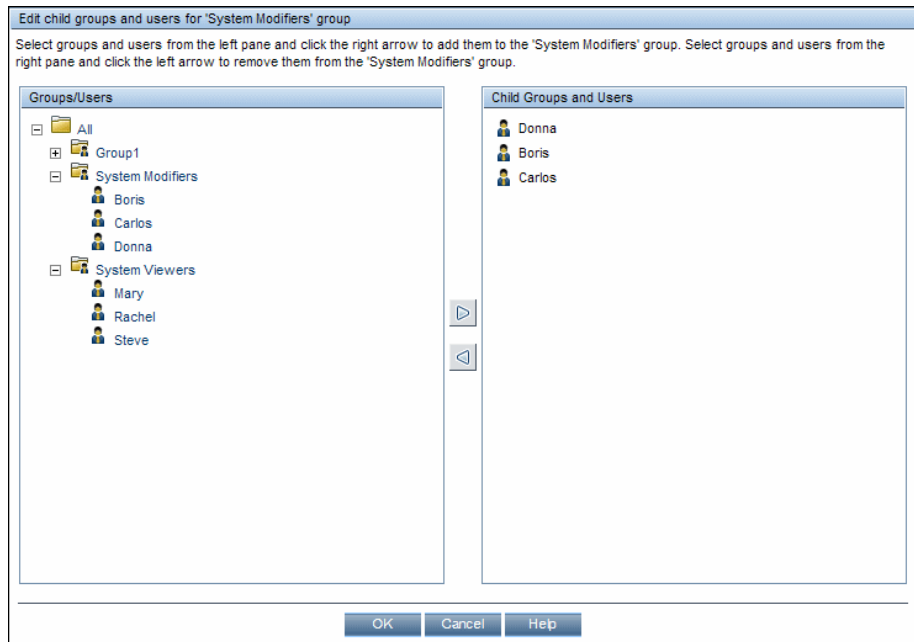
Select a group or user in the **Groups/Users** pane, and select the **Hierarchy** tab on the right side of the page to view the parent and child groups of the group or user, if applicable.

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.

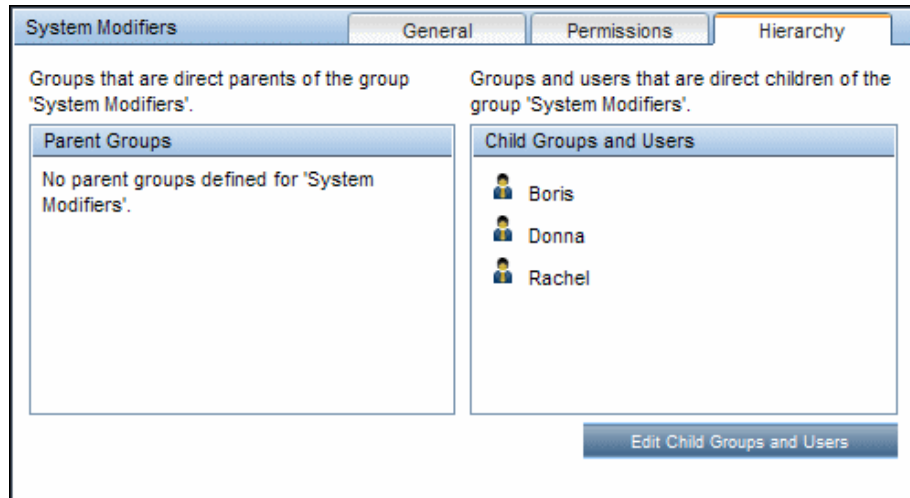


- d Assign users and nest groups by selecting the user or group in the **Groups/Users** pane, and clicking on the left-to-right arrow to move the group or user to the **Child Groups and Users** pane.
Unassign users and remove nested groups by selecting the group or user in the **Child Groups and Users**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



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 450.

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 BSM, and choose the menu items available on pages throughout BSM.

Tip: For a use-case scenario related to this task, see "How to Customize User Menus — Use-Case Scenario" on page 473.

This task includes the following steps:

- "Prerequisites" on page 472
- "Select a User" on page 472
- "Assign a Default Context" on page 472
- "Select Contexts and Applications to Hide/Display" on page 472
- "Select Context Pages and Tabs" on page 472
- "Assign a Default Entry Page" on page 472
- "Results" on page 473

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 570.

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 BSM, and click **Set as Default Entry Context**. For user interface details, see "Customization Tab (User Management)" on page 555.

4 Select Contexts and Applications to Hide/Display

In the **Contexts** 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.

Note: For the Service Health and Operations Management applications, you cannot define user access to specific pages; you can only enable or disable user access at the application level.

6 Assign a Default Entry Page

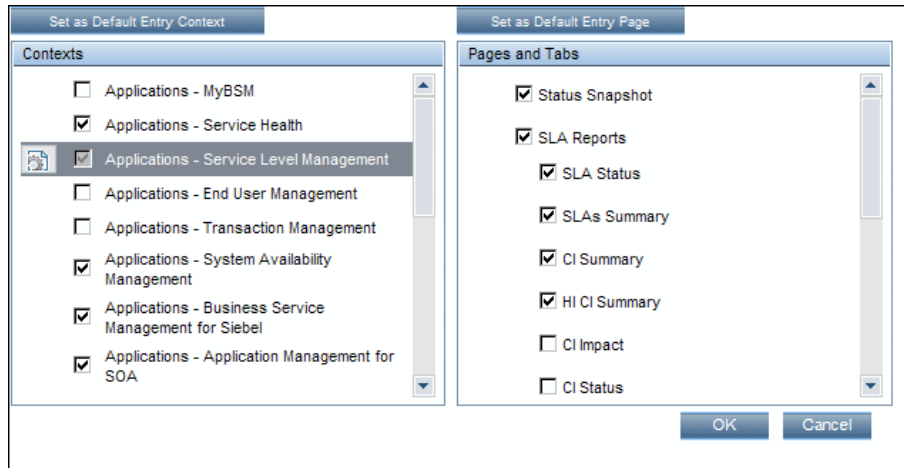
Select a page or tab to be the default entry page for the selected context, and click **Set as Default Entry Page**.

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:



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 471.

This scenario includes the following steps:

- "Choosing a User" on page 474
- "Assigning a Default Context" on page 474

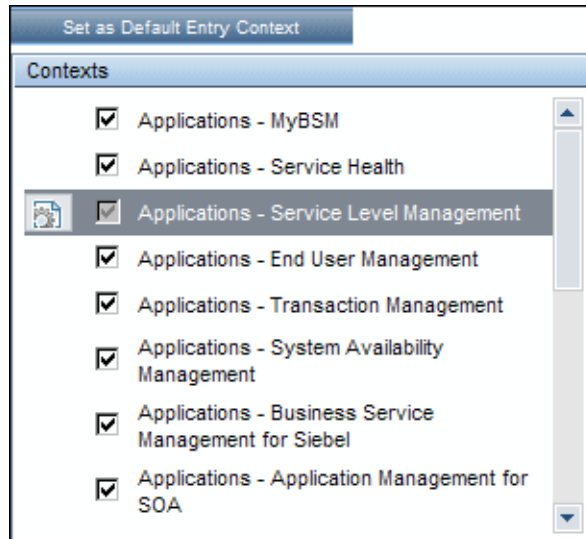
- ▶ "Selecting Context Pages and Tabs" on page 475
- ▶ "Results" on page 475

1 Choosing a User

Mary, the administrator of ABC Insurance Company, is creating several users in the User Management section of BSM. She decides that the user John Smith should be able to view only certain pages and tabs in BSM, and that a specific page should appear on his screen when he logs into BSM.

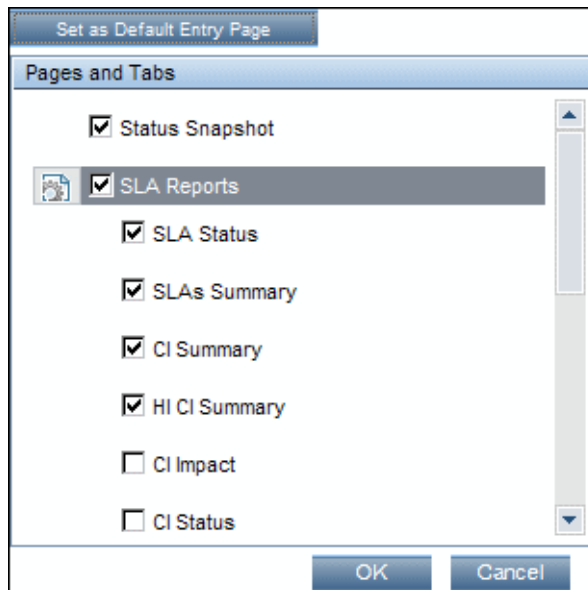
2 Assigning a Default Context

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:



3 Selecting Context Pages and Tabs

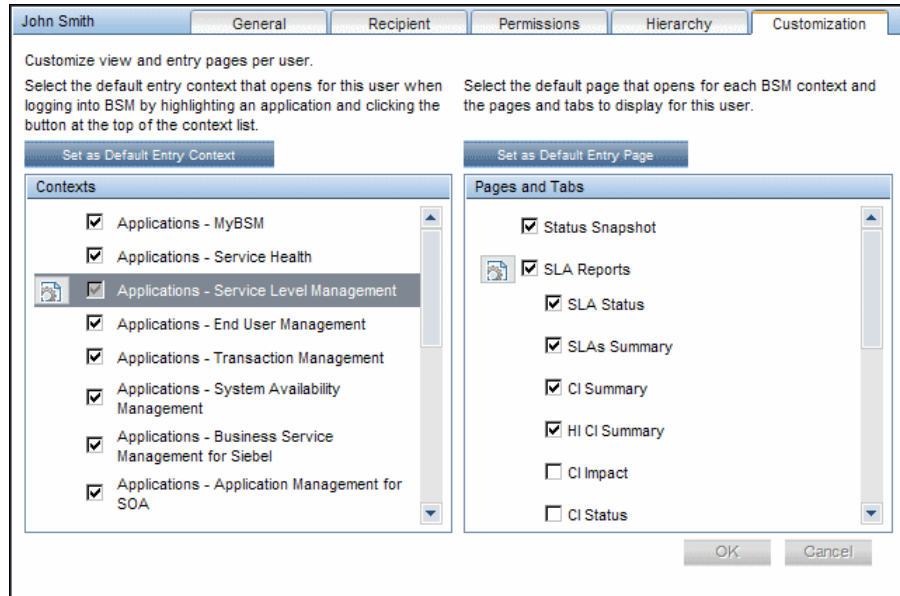
Since John is not authorized to view Outage Reports, that option is cleared in the Pages and Tabs pane, leaving the remaining pages and tabs checked to be visible when John logs into BSM. As SLA Reports are of the highest priority for ABC Insurance, Mary designates this as the first page for John to 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:



4 Results

The context that opens when John Smith logs into BSM 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:



The screenshot shows the 'SLA Reports' section of the HP Business Service Management interface. The page has a navigation bar with 'MyBSM', 'Applications', 'Admin', 'Help', and 'Site Map'. Below the navigation bar, there are tabs for 'Status Snapshot', 'SLA Reports', 'Alerts', 'Outage Reports', and 'SLA Management'. The 'SLA Reports' tab is active, displaying a grid of report cards. Each card includes a title, a brief description, and a small thumbnail image of the report's content. The reports include 'SLA Status', 'SLAs Summary', 'CI Summary', 'HI CI Summary', 'Time Range Comparison', 'CIs Over Time', and 'CI Time Comparison'.

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 BSM. 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 594.

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 477.
- 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 477.

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 BSM.

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 519.

This section describes the following roles:

- "Superuser" on page 480
- "Administrator" on page 481
- "System Modifier" on page 492
- "System Viewer" on page 498
- "Customer Superuser" on page 502
- "Customer Administrator" on page 509
- "BPM Viewer" on page 516
- "BPM Administrator" on page 517
- "RUM Administrator" on page 518
- "RUM Viewer" on page 518

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 520 and "CMDB Open API Update" on page 521.

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.

This section describes the following contexts:

- "Business Process Insight" on page 482
- "Diagnostics" on page 482
- "End User Management" on page 482
- "MyBSM" on page 483
- "MyBSM (Legacy)" on page 483
- "Operations Management" on page 484
- "Operations Orchestration Integration" on page 486
- "Platform" on page 486
- "RTSM" on page 488
- "Service Health Analyzer" on page 488
- "Service Level Management" on page 488
- "Sitescope On demand monitors" on page 489
- "System Availability Management" on page 489
- "Transaction Management" on page 490

► "User Defined Reports" on page 490

Business Process Insight

Resource	Allowed Operations
Business Process Insight Application	View
Business Process Insight Administration	Full Control

Diagnostics

Resource	Allowed Operations
Diagnostics	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

MyBSM

Resource	Allowed Operations
User Pages	Full Control
Predefined Pages	View
User Components	Full Control

MyBSM (Legacy)

Resource	Allowed Operations
Modules	Full Control
Portlet Definitions	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

RTSM

Resource	Allowed Operations
Views	Add
	Change
	View
	Delete
	Full Control
RTSM	Full Control
CI Search	Full Control
Data Modifier	Full Control
Get Related	Full Control
ITU Manager	Full Control
Modeling Studio	Full Control

Service Health Analyzer

Resource	Allowed Operations
Administration	Full Control
Application	Full Control

Service Level Management

Resource	Allowed Operations
SLAs	Add
	Change
	View
	Delete
	Full Control

Sitescope On demand monitors

Resource	Allowed Operations
Administration	Add
	Change
	View
	Delete
	Full Control
Execution	Execute
	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
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

Resource	Allowed Operations
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
	View
	Delete
	Full Control
Annotation	Change
	Delete
	Full Control
Service Report	Change
	Delete
	Full Control
Custom Query Reports	Add
	View
	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 BSM. 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 BSM.

This section describes the following contexts:

- "Business Process Insight" on page 492
- "Diagnostics" on page 493
- "End User Management" on page 493
- "MyBSM" on page 493
- "Operations Orchestration Integration" on page 494
- "Platform" on page 494
- "RTSM" on page 495
- "Service Health Analyzer" on page 495
- "Service Level Management" on page 495
- "Sitescope On demand monitors" on page 496
- "System Availability Management" on page 496
- "Transaction Management" on page 496
- "User Defined Reports" on page 497

Business Process Insight

Resource	Allowed Operations
Business Process Insight Application	View
Business Process Insight Administration	Full Control

Diagnostics

Resource	Allowed Operations
Diagnostics	Change
	View

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

MyBSM

Resource	Allowed Operations
User Pages	Full Control
Pre-defined Pages	View
User Components	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

Resource	Allowed Operations
Databases	Change
	View
System Recipient Template	Change
	View

RTSM

Resource	Allowed Operations
Views	Change
	View
CI Search	Full Control
Get Related	Full Control
ITU Manager	Full Control
Modeling Studio	Full Control

Service Health Analyzer

Resource	Allowed Operations
Administration	Full Control
Application	Full Control

Service Level Management

Resource	Allowed Operations
SLAs	Change
	View

Sitescope On demand monitors

Resource	Allowed Operations
Administration	Change
	View
Execution	Execute

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
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
	View
	Delete
Annotation	Change
	Delete
Service Report	Change
	Delete
Custom Query Reports	Add
	View

System Viewer

The System Viewer role can be applied only to the **Business Service Management** resource.

A system viewer can only view resources within BSM 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.

This section describes the following contexts:

- "Business Process Insight" on page 498
- "Diagnostics" on page 499
- "End User Management" on page 499
- "MyBSM" on page 499
- "Operations Orchestration Integration" on page 499
- "Platform" on page 499
- "RTSM" on page 500
- "Service Health Analyzer" on page 500
- "Service Level Management" on page 500
- "Sitescope On demand monitors" on page 501
- "System Availability Management" on page 501
- "Transaction Management" on page 501
- "User Defined Reports" on page 501

Business Process Insight

Resource	Allowed Operations
Business Process Insight Application	View

Diagnostics

Resource	Allowed Operations
Diagnostics	View

End User Management

Resource	Allowed Operations
Alert - Notification Template	View
Applications	View
BPM Agents	View
RUM Engines	View
Script Repository	View

MyBSM

Resource	Allowed Operations
Predefined Pages	View

Operations Orchestration Integration

Resource	Allowed Operations
Administration	View

Platform

Resource	Allowed Operations
Audit Log	View
Users	View
User Groups	View
Data Collectors	View

Resource	Allowed Operations
Scheduled Reports	View
Recipients	View
Custom Data Types	View
Downtime	View
Databases	View
System Recipient Template	View

RTSM

Resource	Allowed Operations
Views	View
CI Search	Full Control
Get Related	Full Control
ITU Manager	Full Control
Modeling Studio	Full Control

Service Health Analyzer

Resource	Allowed Operations
Administration	Full Control
Application	Full Control

Service Level Management

Resource	Allowed Operations
SLAs	View

Sitescope On demand monitors

Resource	Allowed Operations
Administration	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
Favorite Filter	View
Custom Query Reports	Add
	View

Customer Superuser

Note: This role can be applied to HP Software-as-a-Service customers only.

The **Customer Superuser** role can be applied only to the **Active Customer** resource instance. The **Active Customer** resource instance is available only to HP Software-as-a-Service customers and represents the customer level in the permissions resource tree. It is available in all contexts and applies to all contexts (like the **Business Service Management** resource).

The customer superuser is granted full control on all the resources and instances that belong to that customer. These include all resources, instances of those resources, and child resources under the customer resource.

This section describes the following contexts:

- "Business Process Insight" on page 503
- "Diagnostics" on page 503
- "End User Management" on page 503
- "MyBSM" on page 504
- "MyBSM (Legacy)" on page 504
- "Platform" on page 504
- "RTSM" on page 507
- "Service Health Analyzer" on page 507
- "Service Level Management" on page 507
- "System Availability Management" on page 508
- "User Defined Reports" on page 508

Business Process Insight

Resource	Allowed Operations
Business Process Insight Application	View
Business Process Insight Administration	Full Control

Diagnostics

Resource	Allowed Operations
Diagnostics	View
	Execute

End User Management

Resource	Allowed Operations
Alert - Create dependencies	Change
	Full Control
Applications	Add
	Change
	View
	Delete
	Execute
	Full Control
BPM Agents	View
RUM Engines	View

Resource	Allowed Operations
Script Repository	Add
	Change
	View
	Delete
	Full Control

MyBSM

Resource	Allowed Operations
User Pages	Full Control
Predefined Pages	View
User Components	Full Control

MyBSM (Legacy)

Resource	Allowed Operations
Modules	Full Control
Portlet Definitions	Full Control

Platform

Resource	Allowed Operations
Audit Log	View
	Full Control

Resource	Allowed Operations
Users	Add
	Change
	View
	Delete
	Full Control
User Groups	Add
	Change
	View
	Delete
	Full Control
Data Collectors	Change
	View
Central Repository Service	Add
	Change
	View
	Delete
	Execute
	Full Control
Notification System	View
	Execute
	Full Control
Package Work Manipulation	Change
	Full Control

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
Customer Recipient Template	Add
	Change
	View
	Delete
	Full Control
Downtime	View
	Full Control

RTSM

Resource	Allowed Operations
Views	Add
	Change
	View
	Delete
	Full Control
RTSM	Full Control
CI Search	Full Control
Data Modifier	Full Control
Get Related	Full Control
ITU Manager	Full Control
Modeling Studio	Full Control

Service Health Analyzer

Resource	Allowed Operations
Administration	Full Control
Application	Full Control

Service Level Management

Resource	Allowed Operations
SLAs	Add
	Change
	View
	Delete
	Full Control

System Availability Management

Resource	Allowed Operations
SiteScopes	Add
	Change
	View
	Delete
	Execute
	Full Control

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

Resource	Allowed Operations
Default Header/Footer	Change
	Full Control
Favorite Filter	Change
	View
	Delete
	Full Control
Annotation	Change
	Delete
	Full Control
Service Report	Change
	Delete
	Full Control
Custom Query Reports	Add
	View
	Full Control

Customer Administrator

Note: This role can be applied to HP Software-as-a-Service customers only.

The **Customer Administrator** role can be applied only to the **Active Customer** resource instance. The **Active Customer** resource instance is available only to HP Software-as-a-Service customers and represents the customer level in the permissions resource tree. It is available in all contexts and applies to all contexts (like the **Business Service Management** resource).

The customer administrator is granted full control on a selection of resources, as well as either view, execute, or both on other resources. This user can add profiles of any type, and has full control on the created profile. However, the user is not granted permissions for profiles that were created by other users, even if these profiles are for the same customer. In the case of the **MyBSM** resources, any user with this role can make changes to resources defined by other users.

This section describes the following contexts:

- "Business Process Insight" on page 510
- "Diagnostics" on page 511
- "End User Management" on page 511
- "MyBSM" on page 511
- "MyBSM (Legacy)" on page 511
- "Platform" on page 512
- "RTSM" on page 514
- "Service Health Analyzer" on page 514
- "Service Level Management" on page 514
- "System Availability Management" on page 515
- "User Defined Reports" on page 515

Business Process Insight

Resource	Allowed Operations
Business Process Insight Application	View
Business Process Insight Administration	Full Control

Diagnostics

Resource	Allowed Operations
Diagnostics	View
	Execute

End User Management

Resource	Allowed Operations
Alert - Create dependencies	Change
	Full Control
Applications	Add
	View
BPM Agents	View
RUM Engines	View

MyBSM

Resource	Allowed Operations
User Pages	Full Control
Predefined Pages	View
User Components	Full Control

MyBSM (Legacy)

Resource	Allowed Operations
Modules	Full Control
Portlet Definitions	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
Central Repository Service	Add
	Change
	View
	Delete
	Execute
	Full Control
Notification System	View
	Execute
	Full Control
Package Work Manipulation	Change
	Full Control

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
Customer Recipient Template	Add
	Change
	View
	Delete
	Full Control
Downtime	View
	Full Control

RTSM

Resource	Allowed Operations
Views	Add
	Change
	View
	Delete
	Full Control
RTSM	Full Control
CI Search	Full Control
Data Modifier	Full Control
Get Related	Full Control
ITU Manager	Full Control
Modeling Studio	Full Control

Service Health Analyzer

Resource	Allowed Operations
Administration	Full Control
Application	Full Control

Service Level Management

Resource	Allowed Operations
SLAs	Add
	Change
	View
	Delete
	Full Control

System Availability Management

Resource	Allowed Operations
SiteScopes	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 Header/Footer	Change
	Full Control
Favorite Filter	Change
	View
	Delete
	Full Control

Resource	Allowed Operations
Annotation	Change
	Delete
	Full Control
Service Report	Change
	Delete
	Full Control
Custom Query Reports	Add
	View
	Full Control

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 481).

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 480.

This section describes the following roles:

- "BPIAdministrator" on page 519
- "BPIUser" on page 520
- "BPIRestrictedViewUser" on page 520
- "CMDB Open API Query" on page 520
- "CMDB Open API Update" on page 521
- "CMDB Open API Impact" on page 521
- "CMDB Open API Class Model" on page 521
- "SiteScope Administrator" on page 522
- "Default" on page 522
- "TransactionManagementOperator" on page 523
- "TransactionManagementAdministrator" on page 524
- "TransactionManagementUser" on page 525

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 **RTSM Open API** resource in the **RTSM** context.

This role enables users to query the CMDB (Configuration Management Database) for communication with third-party applications.

Context	Resource	Allowed Operations
RTSM	RTSM Open API	View

CMDB Open API Update

The **CMDB Open API Update** role can be applied only to the **RTSM Open API** resource in the **RTSM** context.

This role enables users to update the CMDB (Configuration Management Database) for communication with third-party applications.

Context	Resource	Allowed Operations
RTSM	RTSM Open API	Change

CMDB Open API Impact

The **CMDB Open API Impact** role can be applied only to the **RTSM Open API** resource in the **RTSM** context.

This role enables users to impact operations on the CMDB.

Context	Resource	Allowed Operations
RTSM	RTSM Open API	View

CMDB Open API Class Model

The **CMDB Open API Class Model** role can be applied only to the **RTSM Open API** resource in the **RTSM** context.

This role enables users to perform operations on CITs.

Context	Resource	Allowed Operations
RTSM	RTSM 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 is automatically assigned if no other role was selected. It allows very limited permissions, mainly to enable adding and viewing custom and trend reports in the **User Defined Reports** context.

Note: To create meaningful reports, the user will likely need additional permissions to specific applications or configuration items.

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 BSM contexts, and the operations that can be applied to them:

- "Business Process Insight" on page 526
- "Diagnostics" on page 526
- "End User Management" on page 527
- "RTSM" on page 531
- "Operations Management" on page 532
- "Operations Orchestration Integration" on page 538
- "Platform" on page 539
- "Service Health" on page 545
- "Service Level Management" on page 546
- "System Availability Management" on page 547
- "Transaction Management" on page 549
- "User Defined Reports" on page 551

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

The **Diagnostics** context enables you to define operations permitted for the Diagnostics application.

Resources	Operation	Description
Diagnostics	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	Change	Enables editing the properties of a customer-specific notification template.
	View	Enables viewing the properties of 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.
Applications	Add	Enables adding applications.
	Change	Enables editing applications, or a specific instance of applications.
	View	Enables viewing applications, or a specific instance of applications.
	Delete	Enables deleting applications, or a specific instance of applications.
	Execute	Enables starting and stopping applications, or a specific instance of applications.
	Full Control	Enables performing all available operations on applications, or a specific instance of applications, and granting and removing permissions for those operations.

Resources		Operation	Description
Applications (specific instances)	BPM	Add	Enables creating a Business Process configuration for a specific instance of applications.
		Change	Enables editing a Business Process configuration for a specific instance of applications.
		View	Enables viewing a Business Process configuration for a specific instance of applications.
		Delete	Enables deleting a Business Process configuration for a specific instance of applications.
		Execute	Enables activating and disabling a Business Process configuration for a specific instance of applications.
		Full Control	Enables performing all available operations on a Business Process configuration for a specific instance of applications.

Resources		Operation	Description
Applications (specific instances) (cont.)	RUM	Add	Enables creating a Real User Monitor configuration for a specific instance of applications.
		Change	Enables editing a Real User Monitor configuration for a specific instance of applications.
		View	Enables viewing a Real User Monitor configuration for a specific instance of applications.
		Delete	Enables deleting a Real User Monitor configuration for a specific instance of applications.
		Execute	Enables activating and disabling a Real User Monitor configuration for a specific instance of applications.
		Full Control	Enables performing all available operations on a Real User Monitor configuration for a specific instance of applications.
	Alert	View	Enables viewing an Alert configuration for a specific instance of applications.
		Full Control	Enables performing all available operations on an Alert configuration for a specific instance of applications.
BPM Agents		View	Enables viewing BPM agents and managing monitors on those agents.
RUM Engines		View	Enables viewing Real User Monitor engines and managing RUM configurations on those engines.

Resources	Operation	Description
Script Repository	Add	Enables creating new folders in the script repository.
	Change	Enables renaming script repository folders and modifying scripts in those folders.
	View	Enables viewing script repository folders and scripts in those folders.
	Delete	Enables deleting folders in the script repository.
	Full Control	Enables performing all available operations on script folders and scripts in the script repository, and granting and removing permissions for those operations.

RTSM

The RTSM 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 RTSM, 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.
RTSM	Full Control	Enables administrative operations for all of the Run-time Service Model (RTSM), except ITU Manager and Modeling Studio.
CI Search	Full Control	Enables the CI Search option from any location in the RTSM.
Data Modifier	Full Control	Enables the Data Modifier option from any location in the RTSM.
Get Related	Full Control	Enables the Get Related CIs option from any location in the RTSM.

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.
RTSM Open API	Change	Enables running of updates in RTSM Open API.
	View	Enables running of queries in RTSM Open API.

Operations Management

Note: The **Operations Management** context is available only if you have installed OMi on your BSM machine. For details on the OMi context, see "User Context Pane" in *Using Operations Management*.

The Operations Manager *i* (OMi) context enables you to assign permissions to work with the Operations Manager context. For details on the operations available for the Operations Manager *i* (OMi) context, see "User Operations Tab" in *Using Operations Management*.

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/Update Annotations	Enables the user to create, modify and delete annotations for events not assigned to them.
	Add/Delete/Update 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	<p>Grants access to the Administration features in the Operations Management Administration, for example:</p> <ul style="list-style-type: none"> ▶ Correlation Rules manager ▶ Content Packs manager ▶ Performance Graphs manager ▶ View Mappings manager ▶ Event Processing Customization ▶ Custom Actions <p>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</p>
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.
Customer Recipient Template	Add	Enables adding a customer-specific recipient template.
	Change	Enables editing a customer-specific recipient template.
	View	Enables viewing the properties of a customer-specific recipient template.
	Delete	Enables deleting a customer-specific recipient template.
	Full Control	Enables performing all available operations on a customer-specific recipient template, and granting and removing permissions for those operations.

Resources	Operation	Description
Package Work Manipulation (HP Software-as-a-Service only)	Change	Enables modifying package locations, renaming packages, and selecting recipients for package notifications.
	View	Enables viewing package information.
	Delete	Enables removing packages from a location.
	Full Control	Enables performing all available operations on package information, 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 in 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 553
- ▶ Create User Dialog Box on page 554
- ▶ Customization Tab (User Management) on page 555
- ▶ General Tab (User Management) on page 557
- ▶ Recipient Tab (User Management) on page 560
- ▶ Hierarchy Tab (User Management) on page 560
- ▶ Permissions Tab (User Management) on page 563
- ▶ User Management Main Page on page 569

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  button, and select Create Group .
See also	"Group and User Hierarchy" on page 451

User interface elements are described below:

UI Element (A-Z)	Description
Group description	Description of the group. Note: This field is optional. Syntax Exceptions: <ul style="list-style-type: none"> ▶ Cannot exceed 99 characters
Group name	The name of the group. Syntax Exceptions: <ul style="list-style-type: none"> ▶ 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: <ul style="list-style-type: none"> ▶ User Account. For details, see "General Tab (User Management)" on page 557. ▶ Recipient. For details, see "Recipient Tab (User Management)" on page 560.
Relevant tasks	<ul style="list-style-type: none"> ▶ "How to Configure Users and Permissions — Workflow" on page 454 ▶ "How to Customize User Menus" on page 471
See also	"User Management — Overview" on page 443

Customization Tab (User Management)

This tab enables you to select the page users see when entering BSM, and choose the menu items available on pages throughout BSM.

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	<ul style="list-style-type: none"> ▶ "How to Configure Users and Permissions — Workflow" on page 454 ▶ "How to Customize User Menus" on page 471
See also	"Customizing User Menus" on page 453

User interface elements are described below:

UI Element (A-Z)	Description
Contexts	<p>Select a BSM context. You can perform the following actions on the context:</p> <ul style="list-style-type: none"> ▶ 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 BSM. <p>For details on BSM contexts, see "Resource Contexts" on page 565.</p>
Pages and Tabs	<ul style="list-style-type: none"> ▶ Select the pages and tabs you want to be visible for the BSM 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. <p>Note: For the Service Health and Operations Management applications, you cannot define user access to specific pages; you can only enable or disable user access at the application level.</p>
Set as Default Entry Context	<p>Sets the selected context in the Contexts pane as the entry context that is displayed when the specified user logs into BSM.</p> <p>Note: The Default Entry Context icon  appears next to the specified context.</p>
Set as Default Entry Page	<p>Assigns the specified page or tab as the default page that opens for the context selected in the Contexts pane.</p> <p>Note: The Default Entry Page icon  appears next to the specified page or tab.</p>

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	<ul style="list-style-type: none"> ▶ 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 454
See also	<ul style="list-style-type: none"> ▶ "User Management — Overview" on page 443 ▶ "Create Group Dialog Box" on page 553 ▶ "Create User Dialog Box" on page 554 ▶ "Groups/Users Pane" on page 570

User interface elements are described below when you select a user in the left pane:

UI Element (A-Z)	Description
Confirm password	Re-enter the edited password that you entered in the Password field.
Login name	<p>The name that the user uses to log into BSM.</p> <p>Syntax Exceptions:</p> <ul style="list-style-type: none"> ▶ Cannot exceed 99 characters ▶ The following characters are not supported: " \ / [] : < > + = ; , ? * % & <space> ▶ The name must be unique <p>Notes:</p> <ul style="list-style-type: none"> ▶ 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	<p>The password of the user used to log into BSM.</p> <p>Syntax Exceptions:</p> <ul style="list-style-type: none"> ▶ Cannot exceed 20 characters <p>Notes:</p> <ul style="list-style-type: none"> ▶ 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	<p>The time zone of the user's location as specified in the Create User dialog box.</p> <p>Note: When you modify the time zone, the linked recipient offset from GMT is also updated after you confirm the change.</p>

UI Element (A-Z)	Description
User mode	<p>The user mode, as configured in the Create User dialog box. Available options are:</p> <ul style="list-style-type: none"> ▶ Unspecified. Leaves the user without a particular mode. Select this option if: <ul style="list-style-type: none"> ▶ BSM is working with user modes and you want this user to see KPIs for both modes in Service Health 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	<p>The name of the user, as configured in the Create User dialog box.</p> <p>Syntax Exceptions:</p> <ul style="list-style-type: none"> ▶ 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 Element (A-Z)	Description
Group description	<p>The description of the group, as configured on the Create Group dialog box.</p> <p>Note: This field is optional.</p>
Group name	<p>The name of the group, as configured on the Create Group dialog box.</p>

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 578.

For user interface details, see "New or Edit Recipient Dialog Box" on page 586.



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.

<p>To access</p>	<p>Select Admin > Platform > Users and Permissions > User Management, select a group or user from the Groups/Users pane, and click the Hierarchy tab.</p> <p>The Hierarchy tab displays:</p> <ul style="list-style-type: none"> ▶ 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.
<p>Important information</p>	<ul style="list-style-type: none"> ▶ 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 BSM groups have been synchronized with groups on an external LDAP server, BSM users cannot be moved between groups, and only groups appear on the interface. For details on synchronizing groups, see "Synchronizing Users" on page 654.



Relevant tasks	<ul style="list-style-type: none"> ➤ "How to Configure Users and Permissions — Workflow" on page 454 ➤ "How to Configure Group and User Hierarchy" on page 468
See also	"Group and User Hierarchy" on page 451

User interface elements are described below:

UI Element (A-Z)	Description
	Denotes a group that the selected group or user is nested under.
	Denotes a user that is nested beneath the selected group.
Child Groups and Users	Displays the groups and users that are nested directly beneath the group selected in the Groups/Users pane.
Edit Child Groups and Users	<p>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 562.</p> <p>Note: This button is displayed only when selecting a group in the Groups/Users pane.</p>
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 Element (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	<p>Select Admin > Platform > Users and Permissions > User Management > Permissions tab.</p> <p>The Permissions tab is divided into the following areas:</p> <ul style="list-style-type: none"> ▶ Groups/Users pane on the left side of the page. For details, see "Groups/Users Pane" on page 570. ▶ Resource tree pane in the center of the page. For details, see "Resource Tree Pane" on page 564. ▶ Roles tab on the right side of the page. For details, see "Roles Tab" on page 567. ▶ Operations tab on the right side of the page. For details, see "Operations Tab" on page 567.
Important information	<ul style="list-style-type: none"> ▶ You can grant permissions to only one user or group at a time. ▶ Assigning Add permissions on the Operations tab does not automatically grant View permissions on the given resource. ▶ If you have many users for whom you have to grant permissions, it is recommended that you organize your users into logical groups using the Hierarchy tab. For details, see "Hierarchy Tab (User Management)" on page 560.
Relevant tasks	<ul style="list-style-type: none"> ▶ "How to Configure Users and Permissions — Workflow" on page 454 ▶ "How to Assign Permissions" on page 466
See also	"Permissions Overview" on page 445


Resource Tree Pane

This tab displays the instances and resources available within each BSM context for which you set permissions.

<p>To access</p>	<p>Select Admin > Platform > Users and Permissions > User Management > Permissions tab.</p> <p>The types of resources displayed in the Resource Tree pane are:</p> <ul style="list-style-type: none"> ➤ Resource with instances  ➤ Instances of a resource  <p>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.</p> <ul style="list-style-type: none"> ➤ Resource without instances 
<p>Important information</p>	<ul style="list-style-type: none"> ➤ The Business Service Management resource refers to all contexts in BSM 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 446.
<p>Relevant tasks</p>	<p>"How to Assign Permissions" on page 466</p>
<p>See also</p>	<ul style="list-style-type: none"> ➤ "Understanding Permissions Resources" on page 446 ➤ "Resource Contexts" on page 565

User interface elements are described below:

UI Element (A-Z)	Description
	<p>An instance of a resource.</p>
	<p>A resource without instances.</p>

UI Element (A-Z)	Description
	A resource that has instances (a resource collection).
Select Context	Select a BSM context for which to configure permissions. For details on BSM contexts, see "Resource Contexts" on page 565.
Settings	<p>Applies specific permissions settings for configurations in your User Management session. Select from the following options:</p> <ul style="list-style-type: none"> ➤ 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. <p>Note: When you select the settings for applying permissions, the options selected apply only to the current BSM session.</p>

Resource Contexts

The following contexts are included:

UI Element (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 Element (A-Z)	Description
End User Management	Includes all the resources relating to operating and administering the End User Management application.
MyBSM	Includes resources needed to administer user pages, predefined pages, and user components.
MyBSM (Legacy)	Includes resources needed to administer modules and portlet definitions.
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.
RTSM	Includes all the resources for the Run-time Service Model (RTSM).
Service Health Analyzer	Includes all the resources relating to the Service Health Analyzer application.
Service Level Management	Includes the SLA resource.
SiteScope On Demand Monitors	
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 BSM.

To access	Select Admin > Platform > Users and Permissions > User Management > Permissions tab
Relevant tasks	"How to Assign Permissions" on page 466
See also	<ul style="list-style-type: none"> ▶ "Understanding Permissions Resources" on page 446 ▶ "User Management Roles Applied Across BSM" on page 480

User interface elements are described below:

UI Element (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 480.

Operations Tab

Displays the predefined operations configurable for groups and users in BSM.

To access	Select Admin > Platform > Users and Permissions > User Management > Permissions tab
Relevant tasks	"How to Assign Permissions" on page 466
See also	<ul style="list-style-type: none"> ▶ "Understanding Permissions Resources" on page 446 ▶ "User Management Operations" on page 525

User interface elements are described below:

UI Element (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.
Granted from Group/Roles/Parent	<p>Displays those permissions that have been granted from either a group, a role, or a parent resource.</p> <p>Note:</p> <ul style="list-style-type: none"> ➤ 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	<p>Select the check box in the Inherit column for the operation to be inherited to all the child resources within the selected resource.</p> <p>Note:</p> <ul style="list-style-type: none"> ➤ 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 525.

User Management Main Page

This page displays information on the groups and users configured to access BSM, including their respective permission levels.

To access	Select Admin > Platform > Users and Permissions > User Management
Important information	<p>When you first access the User Management page or the cursor is located on the All node, the page includes:</p> <ul style="list-style-type: none"> ▶ the Groups/Users pane. For details, see "Groups/Users Pane" on page 570. ▶ the workflow pane. The Workflow page displays introductory information about the User Management application, and a suggested workflow for configuring groups and users. <p>When you select a user, the page includes the following tabs:</p> <ul style="list-style-type: none"> ▶ General. For details, see "General Tab (User Management)" on page 557. ▶ Recipient. For details, see "Recipient Tab (User Management)" on page 560. ▶ Permissions. For details, see "Permissions Tab (User Management)" on page 563. ▶ Hierarchy. For details, see "Hierarchy Tab (User Management)" on page 560. ▶ Customization. For details, see "Customization Tab (User Management)" on page 555. <p>When you select a group, the page includes the following tabs:</p> <ul style="list-style-type: none"> ▶ General. For details, see "General Tab (User Management)" on page 557. ▶ Permissions. For details, see "Permissions Tab (User Management)" on page 563. ▶ Hierarchy. For details, see "Hierarchy Tab (User Management)" on page 560.

Relevant tasks	"How to Configure Users and Permissions — Workflow" on page 454
See also	<ul style="list-style-type: none"> ➤ "User Management — Overview" on page 443 ➤ "Groups/Users Pane" on page 570





Groups/Users Pane







This pane displays the list of users and groups of users configured to access BSM.

To access	<p>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.</p> <p>The Groups/Users pane contains the following tabs:</p> <ul style="list-style-type: none"> ➤ 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: <ul style="list-style-type: none"> ➤ Group name ➤ Login name ➤ User name ➤ User last login <p>You can sort the columns by clicking on the column headers above the boxes.</p> <p>You can include wildcards (*) in your search.</p>
Important information	<ul style="list-style-type: none"> ➤ 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 454
See also	"User Management Main Page" on page 569


User interface elements are described below:

UI Element	Description
	<p>Creates a user or group.</p> <p>Depending on whether you choose to create a user or group, the Create User or Create Group window opens.</p> <p>When you create a new group or user, the Groups/Users pane refreshes and the newly created group or user is selected.</p> <p>Note: In Firefox, after refresh, the All node is selected.</p> <p>For details, see "Create User Dialog Box" on page 554 or "Create Group Dialog Box" on page 553.</p>
	<p>Clones the settings of an existing user or group to a new user or group</p>
	<p>Deletes the selected user or group.</p> <p>Note: When you delete a user, the linked recipient is also deleted.</p>
	<p>Collapses or expands the groups selected in the hierarchy tree.</p> <p>Note: Only previously loaded nodes are expanded.</p>

UI Element	Description
	<p>Click and select Group Mappings to map local groups to groups configured on the LDAP server, or Delete Obsolete Users to delete BSM users no longer configured on the LDAP server. After selecting Delete Obsolete Users, you can remove multiple users at once by holding the Ctrl button while selecting users.</p> <p>For details, see "Group Mappings Dialog Box" on page 573.</p> <p>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 619.</p>
	<p>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).</p> <p>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 450.</p>
	<p>A configured user</p>
	<p>A configured group</p>
	<p>Security officer</p>
	<p>Root node</p>


Group Mappings Dialog Box

This dialog box enables you to map groups configured in BSM to groups configured on the LDAP server.

<p>To access</p>	<p>Select Admin > Platform > Users and Permissions > User Management. In the Groups/Users pane, click the LDAP Configuration button  and select Group Mappings.</p> <p>The Group Mappings dialog box consists of the following panes:</p> <ul style="list-style-type: none"> ▶ Corporate Directory Pane. For details, see "Corporate Directory Pane" on page 574. ▶ BSMLocal Repository For Remote Group Pane: <group name>. For details, see "BSM Local Repository for Remote Group: <group name> Pane" on page 575. ▶ 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.
<p>Important information</p>	<p>Note: This dialog box is accessible only if LDAP mode has been enabled in the Authentication Wizard. For details, see "Authentication Wizard" on page 619.</p> <p>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.</p>


Corporate Directory Pane

This pane enables you to assign BSM groups to LDAP groups, and to list the users in the LDAP groups.

<p>Description</p>	<p>Select Admin > Platform > Users and Permissions; in the Groups/Users pane, click the LDAP Configuration button  and select Group Mappings.</p>
<p>Important information</p>	<ul style="list-style-type: none"> ▶ To synchronize LDAP groups with BSM 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. <p>You can also select either of these options by right clicking on the group.</p> <ul style="list-style-type: none"> ▶ Once the LDAP groups have been mapped to the BSM groups, the BSM groups are managed only from the LDAP interface. This means that the following are fields are affected on the Users and Permissions interface: <ul style="list-style-type: none"> ▶ 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 BSM mapped to the LDAP group selected in the Corporate Directory Pane, and enables you to remove the mapped BSM 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	<ul style="list-style-type: none"> ▶ To remove groups, select the group you want to remove and click Remove Groups. ▶ You can remove multiple groups at once by holding the Ctrl button while selecting groups.

20

Recipient Management

This chapter includes:

Concepts

- ▶ Recipient Management Overview on page 578

Tasks

- ▶ How to Configure and Manage Recipients on page 579
- ▶ How to Add a Custom Pager or SMS Service Provider on page 579

Reference

- ▶ Recipient Management User Interface on page 582

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 684.
- ▶ **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 678.

For details on where to configure and manage recipients, see "Recipients Page" on page 583.

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 583.

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**.

How to Add a Custom Pager or SMS Service Provider

If you are configuring alerts to be sent by 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 BSM. 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 594.

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 580.
- 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 580.

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 BSM.

Reference


Recipient Management User Interface

This section includes:

- ▶ Attach Recipient to a User Dialog Box on page 582
- ▶ Recipients Page on page 583
- ▶ New or Edit Recipient Dialog Box on page 586

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 451

User interface elements are described below:



UI Element	Description
User Login	The name used to log into BSM.
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	<ul style="list-style-type: none"> ▶ 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 563. ▶ 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 579
See also	"Recipient Management Overview" on page 578

User interface elements are described below:


UI Element (A-Z)	Description
	Add new recipient. Opens the New Recipient dialog box. For details, see "New or Edit Recipient Dialog Box" on page 586.
	Edit selected recipient. Opens the Edit Recipient dialog box. For details, see "New or Edit Recipient Dialog Box" on page 586.

UI Element (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 582.
	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: <ul style="list-style-type: none"> ➤ The following characters are not supported: @ & " ' ... ➤ The following special characters are allowed: () - _ + = [] { } ; < > . ,





UI Element (A-Z)	Description
Recipient Name	<p>The name of the recipient.</p> <p>Important: Cannot exceed 49 characters.</p> <p>Syntax Exceptions: The following characters are not supported: ' ~ ! @ # \$ % ^ & * - + = [] { } \ / ? . , " ' : ; < ></p>
SMS	<p>The SMS numbers of the recipient.</p> <p>Syntax Exceptions:</p> <ul style="list-style-type: none"> ▶ 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	<p>You can also access this page from:</p> <ul style="list-style-type: none"> ▶ 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 <i>Using Service Health</i>. ▶ 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 <i>Using Service Level Management</i>. ▶ Click the Create Recipient button in the Attach Recipient dialog box for event-based alerts. For details, see "Attach Recipients Dialog Box" in <i>Using End User Management</i>. ▶ Click the New Recipient button in the Report Manager Main page. For details, see "Report Manager Main Page" in <i>Reports</i>.
Important information	<ul style="list-style-type: none"> ▶ 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 563. ▶ 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 579
See also	"Recipient Management Overview" on page 578

User interface elements are described below:

UI Element (A-Z)	Description
	<p>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 582.</p> <p>Note: This button is displayed only when you access the dialog box from Admin > Platform > Users and Permissions > User Management.</p>
	<p>Detach user from selected recipient. Detaches the current recipient from the corresponding user (listed in the page). A confirmation message is issued.</p> <p>Note: This button is displayed only when you access the dialog box from Admin > Platform > Users and Permissions > User Management.</p>
	<p>Delete the recipient attached to the selected user. Detaches the recipient from the user and deletes the recipient.</p> <p>Note: This button is displayed only when you access the dialog box from Admin > Platform > Users and Permissions > User Management.</p>
	<p>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.</p>

UI Element (A-Z)	Description
<p>EUM Alert notification template</p>	<p>Select the template you want to use for the EUM alert notification, or any custom template already created.</p> <p>Note: When you change the selection in the EUM 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 EUM 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 EUM 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.</p> <p>For details on EUM alert notification templates and creating custom templates, see "How to Configure EUM Alerts Notification Templates" on page 714.</p> <p>Note: This field is relevant only for event-based alerts.</p> <p>For details on alert notification templates and creating custom templates, see "Notification Templates Page" on page 723.</p> <p>Note:</p> <ul style="list-style-type: none"> ➤ The default template is LONG. ➤ For details on the parameters displayed in each template, see "Default Notification Templates" on page 598. ➤ 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.

UI Element (A-Z)	Description
Link to user	<p>This field is displayed only when you access this page from:</p> <ul style="list-style-type: none">▶ Admin > Platform > Users and Permissions > User Management, select a user in the tree and click the Recipient tab.▶ Admin > Personal Settings > Recipient.
Recipient name	<p>The name of the recipient.</p> <p>Important: Cannot exceed 49 characters.</p> <p>Syntax Exception: The following characters are not supported: ` ~ ! @ # \$ % ^ & * - + [] { } \ / ? " ' < ></p>

UI Element (A-Z)	Description
<p>Schedule for receiving alerts</p>	<p>Enabled if you selected the Per notification method scheduling option for the recipient in the Schedule for Receiving Alerts in the General tab.</p> <p>Select:</p> <ul style="list-style-type: none"> ▶ Mixed value. When you change the selection in the EUM 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 EUM 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 EUM 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. <p>The time range is calculated based on the GMT offset selected for the recipient.</p> <p>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 <i>Reports</i>.</p>

UI Element (A-Z)	Description
Time zone	<p>Select the time zone for the recipient. Business Service Management uses the time zone to send alert notices and HP Software-as-a-Service notifications to the selected recipient.</p> <p>Note:</p> <ul style="list-style-type: none">▶ The 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 time zone selected for the recipient is also the time zone that BSM 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. <p>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 <i>Reports</i>.</p> <ul style="list-style-type: none">▶ 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

<p>Important information</p>	<p>This area includes the following tabs:</p> <ul style="list-style-type: none"> ➤ "Email Tab" on page 592 ➤ "SMS Tab" on page 594 ➤ "Pager Tab" on page 596
-------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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.

<p>To access</p>	<p>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.</p>
<p>Important information</p>	<p>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.</p> <p>Note: The text displayed in email messages can only be in Latin characters except for the contents of fields inserted by the user that can be in any supported and relevant language. Those fields can include, for example, Alert Name, Alert description, and KPI name.</p>

User interface elements are described below:

UI Element (A-Z)	Description
<p>Email Addresses</p>	<p>Enter one or more email addresses. Separate multiple entries with a semi-colon (;).</p>

UI Element (A-Z)	Description
<p>Enable secure mail</p>	<p>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.</p> <p>Note:</p> <ul style="list-style-type: none"> ▶ The encrypted mail option is supported only for alerts. Encrypted mail is not supported for scheduled reports or subscription notification (HP Software-as-a-Service customers only). ▶ The encrypted mail option is supported only when the BSM Data Processing Server is installed on a Windows machine.
<p>EUM Alert notification template</p>	<p>Select the template you want to use. For details, see "EUM Alerts Notification Templates" on page 712.</p> <p>Note: When you change the selection in the EUM 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 EUM 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 EUM 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.</p>
<p>Schedule for receiving Email messages</p>	<p>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 586.</p>

 **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	<p>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.</p> <p>Note: You can use a pager or an SMS service provider that does not appear on the default list. For details, see "How to Add a Custom Pager or SMS Service Provider" on page 579.</p>

User interface elements are described below:

UI Element (A-Z)	Description
EUM Alert notification template	<p>Select the template you want to use. For details, see "EUM Alerts Notification Templates" on page 712.</p> <p>Note: When you change the selection in the EUM 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 EUM 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 EUM 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.</p>
Provider	<p>Select an SMS service provider from the list:</p> <ul style="list-style-type: none"> ➤ Genie-UK ➤ Itineris ➤ SFR-France ➤ GoSMS-Israel ➤ MtnSMS-Global <p>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 BSM. For details, see "How to Add a Custom Pager or SMS Service Provider" on page 579.</p>
Schedule for receiving SMS messages	<p>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 586.</p>
SMS numbers	<p>Type one or more SMS access numbers in the box. Separate multiple entries with a semi-colon (;).</p>

 **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	<p>You can use a pager that does not appear on the default list. For details, see "How to Add a Custom Pager or SMS Service Provider" on page 579.</p> <p>Note: The text displayed in pager messages can only be in Latin characters 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.</p>

User interface elements are described below:

UI Element (A-Z)	Description
EUM Alert notification template	<p>Select the template you want to use. For details, see "EUM Alerts Notification Templates" on page 712.</p> <p>Note: When you change the selection in the EUM 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 EUM 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 EUM 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.</p>
Pager Numbers	<p>Enter one or more pager access numbers. Separate multiple entries with a semi-colon (;).</p> <p>Note: If your pager is numeric only, when creating an alert scheme in the Alert Wizard, you can only type a numeric user message.</p>
Schedule for receiving pager message	<p>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 586.</p>
Type	<p>Select a pager service provider. The following providers are supported:</p> <ul style="list-style-type: none"> ➤ MetroCall ➤ Arch ➤ AirTouch ➤ PageMci ➤ SkyTel ➤ PageNet ➤ PageMart ➤ AmeriPage ➤ Nextel ➤ PageOne

Default Notification Templates

Important information	<p>Each template enables you to display, in the notification, selected information that corresponds to specific parameters.</p> <p>For details on the parameters displayed in each template, see "Notification Template Properties Dialog Box" on page 716.</p>
------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

The following default notification templates are available:

UI Element (A-Z)	Description
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 715.
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.

21

Personal Settings

This chapter includes:

Concepts

- Personal Settings Overview on page 600

Tasks

- How to Customize Your BSM Menus and Pages — Workflow on page 602
- How to Customize Your BSM Menus and Pages — Use-Case Scenario on page 604

Reference

- Personal Settings User Interface on page 608

Concepts

Personal Settings Overview

Personal settings enable customization of the way BSM presents information to individual users.

Individual users can configure personal settings to customize their specific user-related behavior of BSM.

The Personal Settings tab contains the following options:

- ▶ **General Settings.** For details, see "User Account" on page 600.
- ▶ **Menu Customization.** For details, see "Menu Customization" on page 601.

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 608.

Menu Customization

On the Menu Customization tab, you can:

- Specify the default context that is displayed when logging into BSM.
- Specify the first page that is displayed in each of the different parts of BSM.
- Specify the tabs and options that are available on pages throughout BSM.

Customizing your entry page, menu items, and tabs enables your interface to display only the areas of BSM that are relevant to you. For details on the Menu Customization User Interface, see "Menu Customization Page" on page 610.

Tasks

How to Customize Your BSM Menus and Pages — Workflow

This task describes how to customize the page you see when entering BSM, and choose the menu items available on pages throughout BSM.

Tip: For a use-case scenario related to this task, see "How to Customize Your BSM Menus and Pages — Use-Case Scenario" on page 604.

This task includes the following steps:

- "Assign a Default Context" on page 602
- "Select Context Pages and Tabs" on page 602
- "Assign a Default Entry Page" on page 603
- "Results" on page 603

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 BSM, and click **Set as Default Entry Context**. For user interface details, see "Menu Customization Page" on page 610.

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.

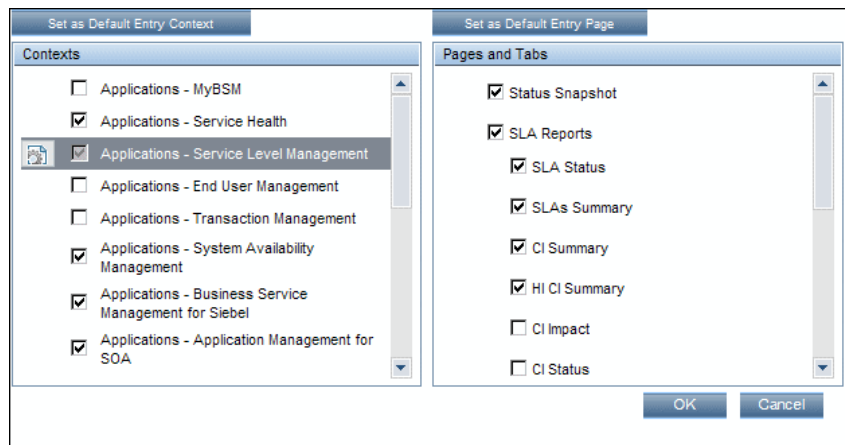
3 Assign a Default Entry Page

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:



How to Customize Your BSM Menus and Pages — Use-Case Scenario

This use-case scenario describes how to customize user menus for individual users.

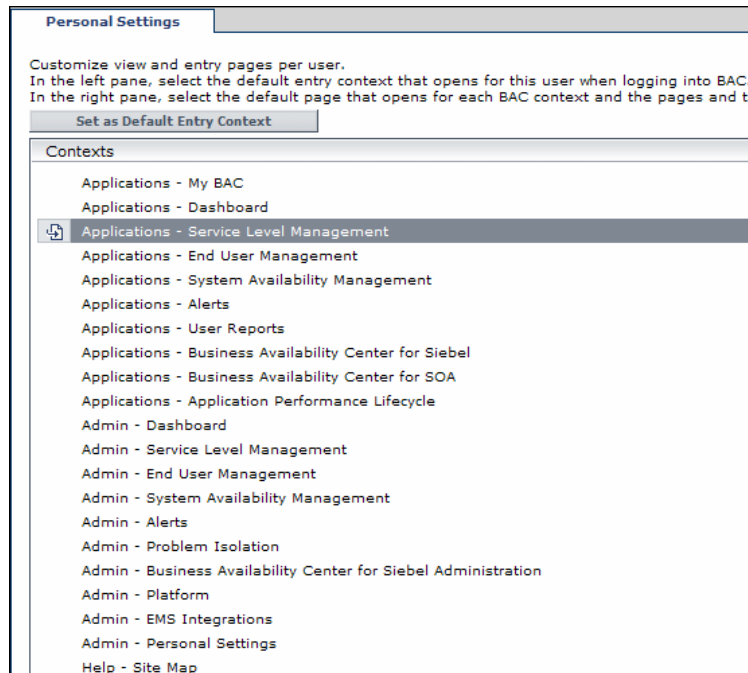
Note: For a task related to this scenario, see "How to Customize Your BSM Menus and Pages — Workflow" on page 602.

This task includes the following steps:

- ▶ "Assigning a Default Context" on page 605
- ▶ "Selecting Context Pages and Tabs" on page 606
- ▶ "Results" on page 607

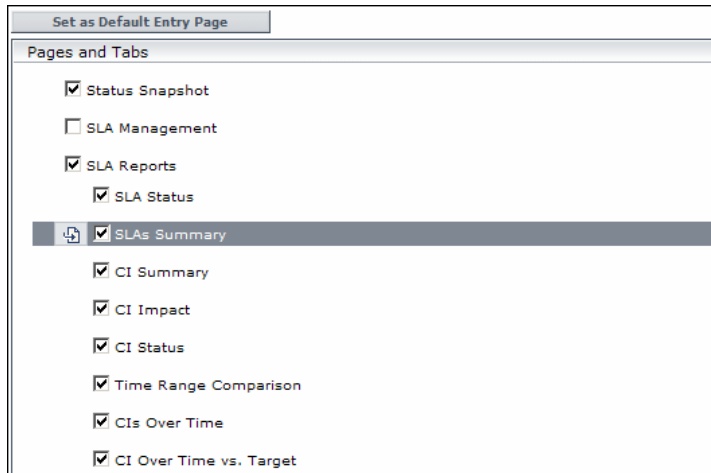
1 Assigning a Default Context

John Smith is a registered BSM 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:



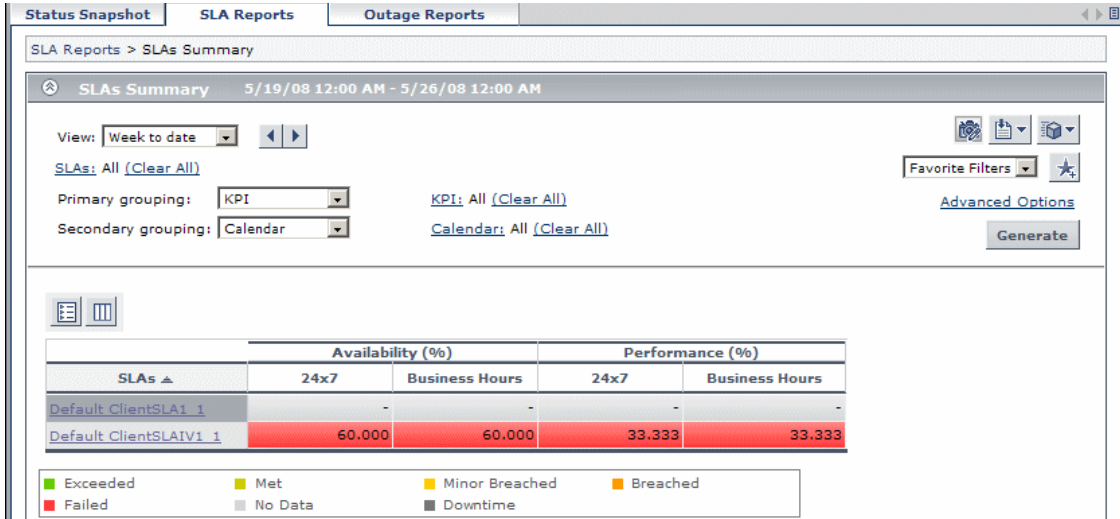
2 Selecting Context Pages and Tabs

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 into BSM. 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 into BSM:



3 Results

The context that opens when John Smith logs into BSM is the **Service Level Management** context on the Applications menu. The **SLAs Summary Report** page is displayed on the SLA Reports tab:



SLA Reports > SLAs Summary

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 KPI: All (Clear All)

Secondary grouping: Calendar Calendar: All (Clear All)

Generate

SLAs	Availability (%)		Performance (%)	
	24x7	Business Hours	24x7	Business Hours
Default ClientSLA1_1	-	-	-	-
Default ClientSLAIV1_1	60.000	60.000	33.333	33.333

■ Exceeded ■ Met ■ Minor Breached ■ Breached
■ Failed ■ No Data ■ Downtime

Reference

Personal Settings User Interface

This section includes:

- ▶ User Account Page on page 608
- ▶ Menu Customization Page on page 610
- ▶ Recipient Tab on page 611

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	BSM 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 600

User interface elements are described below:

UI Element (A-Z)	Description
Confirm Password	Re-enter the password specified in the Password field.
Login name	The name used to log into BSM. Note: You cannot change the entry in this field.
Password	Enter a password to be used when accessing BSM.

UI Element (A-Z)	Description
Select auto-refresh rate	<p>Select the rate at which you want BSM to automatically refresh the browser and load the most up-to-date data from the database.</p> <p>Note: This setting is active only when in the Past day or Past hour time resolution in reports.</p>
Time zone	<p>Select the appropriate time zone, according to the user's location.</p>
User mode	<p>Select the user mode for the user, from the following options:</p> <ul style="list-style-type: none"> ▶ Unspecified. Leaves the user without a particular mode. Select this option if: <ul style="list-style-type: none"> ▶ BSM is working with user modes and you want this user to see KPIs for both modes in Service Health 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. <p>Note: For details on user modes, see "KPIs for User Modes" in <i>Using Service Health</i>.</p>
User name	<p>The user name for the user.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▶ 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 BSM.
- ▶ The first page displayed in each of the different parts of BSM.
- ▶ The tabs and options available on pages throughout BSM.

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 602
See also	"Personal Settings Overview" on page 600

User interface elements are described below:

UI Element (A-Z)	Description
Contexts	Select a BSM context. You can perform the following actions on the context: <ul style="list-style-type: none"> ▶ 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 BSM.
Pages and Tabs	<ul style="list-style-type: none"> ▶ Select the pages and tabs you want to be visible for the BSM 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 Element (A-Z)	Description
Set as Default Entry Context	<p>Click to set the selected context in the Contexts pane as the entry context that is displayed when the specified user logs into BSM.</p> <p>Note: The Default Entry Context icon  appears next to the specified context.</p>
Set as Default Entry Page	<p>Click to assign the specified page or tab as the default page that opens for the context selected in the Contexts pane.</p> <p>Note: The Default Entry Page icon  appears next to the specified page or tab.</p>

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 586.

22

Set Up the Authentication Strategies

This chapter includes:

Concepts

- ▶ Authentication Strategies — Overview on page 614
- ▶ Setting Up an SSO Authentication Strategy on page 614
- ▶ Setting Up LDAP Authentication on page 615

Reference

- ▶ Authentication Modes in BSM on page 616
- ▶ Authentication Strategy User Interface on page 617

Concepts

Authentication Strategies — Overview

BSM 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 BSM at any given time.

The default authentication strategy for logging into BSM is the BSM internal authentication service. You enter your BSM user name and password from the login page, and your credentials are stored and verified by the BSM database. For a description of the authentication process in BSM, see "BSM Login Flow" on page 35.

You can choose to configure authentication using the Lightweight Directory Access Protocol (LDAP). BSM uses the LDAP server to verify a user's credentials. For details on LDAP, see "LDAP Authentication and Mapping" on page 651.

Authentication strategies are configured in the Authentication Management Wizard. For details on the Authentication Management Wizard, see "Authentication Wizard" on page 619.

Setting Up an SSO Authentication Strategy

Single Sign-On (SSO) 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 BSM is Lightweight Single Sign-On (LW-SSO). LW-SSO is embedded in BSM and does not require an external machine for authentication. For details on LW-SSO, see "LW-SSO Strategy — Overview" on page 636.

If the applications configured outside of BSM 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 BSM, 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 630.

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 "IDM-SSO — Overview" on page 646.

Setting Up LDAP Authentication

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 BSM in one of the following ways:

- As an authentication mechanism for users logging into BSM.
- To map groups and synchronize BSM users with users configured on the external LDAP server, thereby simplifying the process of managing users for BSM administrators. For details, see "How to Map Groups and Synchronize Users" on page 659.

You enable and disable LDAP using the Authentication Management Wizard. For details, see "Authentication Wizard" on page 619.

Reference

Authentication Modes in BSM

The following table displays the Authentication Strategy used by BSM, 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	BSM Internal
	Enabled	LDAP
LW-SSO	Disabled	BSM 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 617
- Authentication Wizard on page 619

Authentication Strategy Page

This page displays the current authentication strategy and Single Sign-on configurations for logging into BSM.

To access	Select Admin > Platform > Users and Permissions > Authentication Management
Important information	<p>Access to the Authentication Management page is dependent on the following permission levels:</p> <ul style="list-style-type: none"> ➤ View. Enables viewing the Authentication Management Page. ➤ Change. Enables you to access the Authentication Management Wizard and change configurations. The Configure button is enabled. <p>You configure permissions on the Users and Permissions interface. For details, see "How to Assign Permissions" on page 466.</p>
See also	<ul style="list-style-type: none"> ➤ "Authentication Strategies — Overview" on page 614 ➤ "Infrastructure Settings" on page 127

User interface elements are described below:

UI Element (A-Z)	Description
Configure	<p>Click to open the Authentication Wizard and configure an authentication strategy. For details on the Authentication Wizard, see "Authentication Wizard" on page 619.</p> <p>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.</p>
Lightweight Directory Access Protocol Configuration	<p>The section displays:</p> <ul style="list-style-type: none"> ▶ 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	<p>The section displays:</p> <ul style="list-style-type: none"> ▶ 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 Element (A-Z)	Description
Configure	<p>Click to open the Authentication Wizard and configure an authentication strategy. For details on the Authentication Wizard, see "Authentication Wizard" on page 619.</p>
Name	<p>The name of the Single Sign-On or Lightweight Directory Access Protocol parameter.</p>
Value	<p>The value of the specified Single Sign-On or Lightweight Directory Access Protocol parameter.</p>

Authentication Wizard

This wizard enables you to create an authentication strategy for logging into BSM.

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 BSM (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: <ol style="list-style-type: none"> 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 619.
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.

<p>Important information</p>	<ul style="list-style-type: none"> ▶ General information about this wizard is available here: "Authentication Wizard" on page 619. ▶ 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: <ul style="list-style-type: none"> ▶ Hover over the error icon to display a tooltip with the error message. ▶ Access the log file <code><HPBSM>/log/EJBContainer/login.log.</code>
<p>Wizard map</p>	<p>The Authentication Wizard contains:</p> <p>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</p>


User interface elements are described below:

UI Element (A-Z)	Description
<p>Disabled</p>	<p>Select to disable the Single Sign-On (SSO) authentication strategy.</p>

UI Element (A-Z)	Description
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 "IDM-SSO — Overview" on page 646. 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 "LW-SSO Strategy — Overview" on page 636.




Identity Management Single Sign-On (IDM-SSO) Configuration

User interface elements are described below:

UI Element (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.
Header Name	Enter the header name for the token name passed by the Identity Management Single Sign-On. Example: sso_user Note: Ensure that the Identity Management Single Sign-On strategy is securing BSM 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 BSM. Example: \<alternativeLogoutURL>.jsp Note: This field is optional.

Lightweight Single Sign-On (LW-SSO) Configuration

User interface elements are described below:

UI Element	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 BSM 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
Parse automatically	Click to parse the BSM domain automatically.
Trusted Hosts/Domains	Displays the list of trusted hosts and domains that are participating in an 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  .

UI Element	Description
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	<p>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.</p> <p>The SAML Configuration dialog box consists of the following sections:</p> <ul style="list-style-type: none"> ▶ SAML2 Creation. Modify the SAML2 Authentication parameters for sending SAML authentication requests from BSM. ▶ SAML2 Validation. Modify the SAML2 Authentication parameters for decrypting SAML requests received by BSM.
Important information	<ul style="list-style-type: none"> ▶ General information about this wizard is available here: "Authentication Wizard" on page 619. ▶ BSM comes with SAML enabled by default. If you want to disable SAML authentication, clear the Enable SAML2 authentication schema check box.
Wizard map	<p>The Authentication Wizard contains:</p> <p>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</p>

User interface elements are described below:

UI Element	Description
Restore	Restores the SAML2 configuration attributes to their state upon logging into the current session of BSM.

SAML2 Creation Section

User interface elements are described below:

UI Element (A-Z)	Description
Keystore filename	<p>The filename of the keystore in BSM.</p> <ul style="list-style-type: none"> ▶ 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.
Look for keystore in classpath	<p>Select for the Lightweight Single Sign-On framework to search for the keystore in the classpath.</p> <p>Note: When this option is selected, you enter only the name of the actual keystore file in the Keystore filename field.</p>
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 Element (A-Z)	Description
Keystore filename	<p>The filename of the keystore in BSM.</p> <ul style="list-style-type: none"> ▶ 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	<p>The password of the public key used for decryption during the SAML authentication request.</p>
Look for keystore in classpath	<p>Select for the Lightweight Single Sign-on framework to search for the keystore in the classpath.</p> <p>Note: When this option is selected, you enter only the name of the actual keystore file in the Keystore filename field.</p>


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 BSM users.

<p>To access</p>	<p>Select Admin > Platform > Users and Permissions > Authentication Management, and click Configure. Navigate to the LDAP General Configuration page. The available LDAP modes are:</p> <ul style="list-style-type: none"> ▶ Enabled ▶ Disabled <p>Note: LDAP cannot be used for authentication when you choose IdentityManagement on the Single Sign-On Configuration page of the wizard.</p>
<p>Important information</p>	<ul style="list-style-type: none"> ▶ General information about this wizard is available here: "Authentication Wizard" on page 619. ▶ When configuring LDAP parameters, consult your LDAP Administrator for assistance.
<p>Wizard map</p>	<p>The Authentication Wizard contains:</p> <p>Introduction Page > Single Sign-On Page > (SAML2 Configuration Dialog Box) > LDAP General Configuration Page > LDAP Users Synchronization Configuration Page > Summary Page</p>

LDAP General Configuration Section

User interface elements are described below:

UI Element (A-Z)	Description
	<p>Indicates that the value in the specified field is empty or invalid.</p> <p>You can view a description of the error in one of the following ways:</p> <ul style="list-style-type: none"> ▶ 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	<p>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 630.</p>
Distinguished Name (DN) Resolution	<p>Select to enable entering LDAP search user credentials.</p> <p>Note: If your LDAP requires user credentials to verify connection to LDAP server, you will need to use the users-remote-repository service in the JMX console to enter these credentials, because this UI will not let you past LDAP server URL without valid user credentials.</p>
Distinguished Name of Search-Entitled User	<p>Defines the Distinguished Name (DN) of a user with search privileges on the LDAP directory server.</p> <p>Note: Leave this entry blank for an anonymous user.</p>

UI Element (A-Z)	Description
<p>LDAP server URL</p>	<p>Enter the URL of the LDAP (or, for Active Directory users, Global Catalog [AD GC]) server.</p> <p>To represent different trees in the same forest, enter multiple DNs, separated by semicolons.</p> <p>To allow failover, enter multiple LDAP (AD GC) server URLs, separated by semicolons.</p> <p>The required format is: ldap://machine_name:port/[??scope]</p> <ul style="list-style-type: none"> ▶ LDAP servers typically use port 389; AD GC servers typically use port 3268 or secure port 3269. ▶ 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. <ul style="list-style-type: none"> ▶ Default port number for regular communication: 389 ▶ Default port number for SSL communication: 636 ▶ Default scope value: sub <p>Examples:</p> <p>Single DN, single LDAP server: ldap://my.ldap.server:389/ou=People,o=myOrg.com??sub</p> <p>Multiple DNs: ldap://my.ldap.server:389/ou=People,o=myOrg.com??sub;ld ap://my.ldap.server:389/ou=Staff,o=my2ndOrg.net??sub</p> <p>Multiple LDAP servers: ldap://my.ldap.server:389/ou=People,o=myOrg.com??sub;ld ap://my.2ndldap.server:389/ou=People,o=myOrg.com??sub</p>

UI Element (A-Z)	Description
LDAP vendor type	Enter the LDAP vendor you are using. Select from: <ul style="list-style-type: none"> ▶ Common LDAP ▶ Microsoft Active Directory ▶ Other <p>Note: If you click Advanced and modify the LDAP Vendor Attribute settings, the value of this field automatically changes to Other.</p>
Password of Search Entitled User	Defines the password of the user entitled to search the LDAP server entities for groups. <p>Note: Leave this entry blank for an anonymous user.</p>

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 Element (A-Z)	Description
Password	The password of the user whose credentials are entered in the UUID field. <p>Note: This field is optional. If left empty, anonymous user is used.</p>
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 dialog 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	<ul style="list-style-type: none"> ▶ General information about this wizard is available here: "Authentication Wizard" on page 619. ▶ 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 Element (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 BSM.
Users filter	Defines which LDAP users are enabled to log into BSM.


UI Element (A-Z)	Description
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 log into BSM 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 BSM users.

To access	Select Admin > Platform > Users and Permissions > Authentication Strategy , and click Configure . Navigate to the LDAP Users Synchronization Configuration page.
Important information	<ul style="list-style-type: none"> ▶ General information about this wizard is available here: "Authentication Wizard" on page 619. ▶ 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 Element (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 BSM, to synchronize LDAP users with BSM users. Important: Ensure that you have mapped LDAP groups to BSM groups before selecting this check box. 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 659.
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.
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 BSM.
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 BSM 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 619.
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 Element (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.

23

Lightweight Single Sign-On Strategy

This chapter includes:

Concepts

- ▶ LW-SSO Strategy — Overview on page 636
- ▶ LW-SSO Configuration for Multi-Domain and Nested Domain Installations on page 636

Tasks

- ▶ How to Configure Unknown User Handling Mode on page 638
- ▶ How to Modify LW-SSO Parameters Using the JMX Console on page 639
- ▶ How to Secure User Access to BSM Using Client-Side Authentication Certificates on page 640
- ▶ How to Secure User Access to BSM Using an External Authentication Point on page 641

Reference

Troubleshooting and Limitations on page 643

Concepts

LW-SSO Strategy — Overview

The default single sign-on authentication strategy for BSM is Lightweight Single Sign-On (LW-SSO). LW-SSO is embedded in BSM and does not require an external machine for authentication. BSM currently uses version 2.4 of LW-SSO.

For an overview of Single Sign-On strategies, see "Setting Up an SSO Authentication Strategy" on page 614.

You configure LW-SSO in BSM using the Authentication Wizard. For details on the Authentication Wizard, see "Authentication Wizard" on page 619.

LW-SSO can be configured using 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 Secure User Access to BSM Using Client-Side Authentication Certificates" on page 640.

For details on limitations of working with LW-SSO, see "LW-SSO Authentication – General Reference" on page 665.

LW-SSO Configuration for Multi-Domain and Nested Domain Installations

LW-SSO configuration, set in the Authentication Wizard (for details, see "Authentication Wizard" on page 619), depends on the architecture of your BSM installation.

If you log into BSM through a man-in-the-middle, such as reverse proxy, a load balancer, or NAT, the BSM domain is the domain of the man-in-the-middle.

If you log in directly to the BSM Gateway, the BSM domain is the domain of the BSM Gateway.

For LW-SSO to work with another application in a domain different from the BSM domain, all of these domains must be listed in the **Trusted Hosts/Domains** list of the LW-SSO configuration.

If your BSM domain and integrating application are located in nested domains, then the suffix of the domain should be the defined as the LW-SSO domain for both applications. In addition, you should disable automatic domain calculation (**Parse automatically** in the Authentication Wizard) and explicitly state the domain suffix.

Example 1:

BSM gateway server is located in emea.hp.com

TransactionVision server is located in cnd.hp.com

Disable automatic domain calculation and set domain name = hp.com

Example 2:

BSM gateway server is in corp.ad.example.com

NNMi server is in sdc.example.com

Load balancer is in example.com

Disable automatic domain calculation and set domain name = example.com

Tasks

How to Configure Unknown User Handling Mode

This task describes how to handle unknown users trying to log into BSM -- users that were authenticated by the hosting application but do not exist in the BSM 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 BSM 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 BSM, and is directed to the login page.

The changes take effect immediately.

Note: When User Synchronization is enabled between BSM and the LDAP server, unknown users are always denied entry into BSM.

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.

You can also use the JMX console if you are locked out of BSM and must change SSO parameters to gain access.

To modify Lightweight Single Sign-On (LW-SSO) parameters using the JMX console:

- 1** Enter the URL of the JMX console (**http://<server name>:8080/jmx-console/**) in a web browser.
- 2** Enter your JMX console authentication credentials. If you do not know your authentication credentials, contact your system administrator.
- 3** Locate the Lightweight Single Sign-On context, as follows:
 - a** Domain name: **Topaz**
 - b** Service: **LW-SSO Configuration**
- 4** Modify parameters accordingly.

The changes take effect immediately.

How to Secure User Access to BSM Using Client-Side Authentication Certificates

You can secure user access to BSM using client-side authentication certificates. You configure LW-SSO using the JMX console to accept such certificates. Once a certificate is accepted, the user is logged into BSM. Client-side authentication certificates provide a secure alternative to entering user credentials in the login screen.

To configure LW-SSO to work with client-side authentication certificates:

- 1** Determine which field and which attribute in the client-side certificate will be used for authentication (example: **EMAILADDRESS** in **SubjectDN**). To do this, view your client certificate details and look at the **Subject** or **SubjectAlternativeName** field. Decide which attribute you are going to use.
- 2** Enter the URL of the JMX console (**http://<Gateway or Data Processing Server name>:8080/jmx-console/**) in a web browser.
- 3** Enter your JMX console authentication credentials.
- 4** Under the domain name **Topaz**, locate **service=LW-SSO Configuration**.
- 5** 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**.

- 6** 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**.
- 7** 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**.

- 8 To define the part of the User Identifier Retrieve field that contains the User Identifier, locate the 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.

- 9 Click **Apply Changes**.
- 10 In the BSM UI, select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**. Click **Foundations** and select **Single Sign-On** from the drop-down list box.
- 11 Set **Unknown User Handling Mode** to **Deny**.

How to Secure User Access to BSM Using an External Authentication Point

LW-SSO 2.4 enables the use of an external authentication point, allowing customers to plug in their own credential validation for whatever authentication technology they wish to use: LDAP, a proprietary user/password database, a custom SSO solution, etc.

The external authentication point is an external URL that does the actual user authentication. It obtains the user credentials (usually the user name and password, but it could be something else, such as the user's class-B certificate, or a proprietary SSO token), validates these credentials, and then creates an "authentication assertion" — a token that states who the authenticated user is, and usually also provides information about how the user was authenticated.

To use an external authentication solution with LW-SSO 2.4:

- 1** If using LDAP, ensure that the same user repository is being used by BSM and the authentication point server. If not using LDAP, create the users manually in BSM.
- 2** Set LW-SSO configuration on the authentication point server side to use the same `initString` as in BSM.
- 3** In LW-SSO configuration on the BSM side, use the JMX Console to:
 - a** Specify `AuthenticationPointServer` URL
 - b** Set `validationPoint enabled = true`
 - c** Click **Apply Changes**, then restart BSM.
- 4** Make sure you can log into BSM through the external authentication point. If you are unable to log in, see "Unable to Log into BSM when Using an External Authentication Point" on page 644.
- 5** If you do not want particular URLs to use this feature, use the JMX Console to add them to the list of non-secure URLs in the LW-SSO configuration.

Reference

Troubleshooting and Limitations

This section describes troubleshooting and limitations for Lightweight Single Sign-On.

This section includes:

- ▶ "Unable to Access BSM Due to Changes in LW-SSO Parameters" on page 643
- ▶ "Synchronizing Users When Using LW-SSO" on page 644
- ▶ "Unable to Log into BSM when Using an External Authentication Point" on page 644

Unable to Access BSM Due to Changes in LW-SSO Parameters

If you are locked out of BSM, you can update selected Lightweight Single Sign-On (LW-SSO) parameters remotely using the JMX console on the application server that is embedded in BSM.

For details on how to change LW-SSO parameters outside the BSM interface, see "How to Modify LW-SSO Parameters Using the JMX Console" on page 639.

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 659.

Unable to Log into BSM when Using an External Authentication Point

If you enabled an external authentication point (AP) and are unable to log in through it, make sure that the user whose credentials you are entering is defined as a user in BSM.

24

Identity Management Single Sign-On Authentication

This chapter includes:

Concepts

- ▶ IDM-SSO — Overview on page 646

Reference

- ▶ Securing BSM Resources Under IDM-SSO on page 647

Troubleshooting and Limitations on page 649

Concepts

IDM-SSO — Overview

You implement Identity Management Single Sign-On (IDM-SSO) if you want a more secure connection than that offered by LW-SSO, or if the applications configured outside of BSM 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.

BSM 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 619.

Before configuring IDM-SSO in BSM, make sure you see your IDM login dialog before the BSM login screen.

If you do not see it, work with your IDM administrator. If the same LDAP was defined in BSM as used by IDM, you should be able to authenticate through both the IDM and BSM login screens using the same credentials. If not, verify that LDAP settings in BSM match those used by IDM. Now you are ready to configure IDM-SSO in BSM. If you need help dumping headers in order to determine the correct IDM header to use in configuration, you can return to the BSM login screen without closing the session and append **/DumpSession.jsp** to the login URL. Look for your user login ID in the resulting list. Before it should be the header name supplied by IDM. You can verify it using **http://<HPBSM server>/topaz/verifyIDM.jsp** in the same user session. Once it is verified as correct, you should be able to use it in the Authentication Management wizard.

Reference

Securing BSM Resources Under IDM-SSO

When using IDM-SSO as a Single Sign-On strategy, BSM resources may be protected with form or basic authentication schemes, or left unprotected.

Resources accessed by application users

If you want to use IDM-SSO to secure BSM resources accessed by application users, use **form authentication** on the following resources:

- /filters/*
- /hpbsm/*
- /mam-images/*
- /mcrcs/*
- /MercuryAM/*
- /odb/*
- /opal/*
- /opr-admin-server/*
- /opr-console/*
- /opr-gateway/*
- /ovpm /*
- /topaz/*
- /topazSettings/*
- /tv/*
- /tvb/*
- /ucmdb-ui/*
- /uim/*

- /utility_portlets/*
- /webinfra/*

Resources accessed by data collectors

If you want to use IDM-SSO to secure BSM resources accessed by data collectors in machine-to-machine communication, use an authentication method that allows passing credentials, or basic authentication.

The following resources are used by data collectors:

- /ext/* — used by RUM
- /mam/* — used by RTSM
- /topaz/topaz_api/* — used by all data collectors to get BSM version, server time, etc.

Resources accessed by web services (required)

If you use IDM-SSO with BSM, you must protect the following resources with **basic authentication** as they are used by various BSM web services:

- /axis2/service/*
- /cm/rest/*
- /opr-admin-server/rest/*
- /opr-console/rest/*
- /opr-gateway/rest/*
- /topaz/bam/*
- /topaz/bsmservices/*
- /topaz/eumopenapi/*
- /topaz/servicehealth/*
- /topaz/slm/*

Additional resources to be protected with basic authentication

- /topaz/rfw/directAccess.do — used with published URL to a report
- /topaz/sitescope/* — used for SAM Admin embedded in BSM UI

Unprotected

The following resources should remain **unprotected**:

- /mam-collectors
- /topaz/Charts
- /topaz/images
- /topaz/Imgs/chartTemp
- /topaz/js
- /topaz/rfw/static
- /topaz/static
- /topaz/services/technical/time
- /topaz/stylesheets
- /tvb/rest
- /ucmdb-api

If you are using a Load Balancer, you should also **unprotect** the following resources:

- /topaz/topaz_api/loadBalancerVerify_centers.jsp
- /topaz/topaz_api/loadBalancerVerify_core.jsp

Troubleshooting and Limitations

This section provides troubleshooting help related to IDM-SSO.

Errors When Entering IDM-SSO Header in Authentication Wizard

Make sure the correct header is used. Ask your Siteminder administrator to dump all headers and look for one that matches what you expect to use. For example, if you want to use an email address as your login username, look for a field containing only an email address. Or, for example, if it looks like **HTTP_SEA**, remove **HTTP_** from the name and give **sea** as the header name.

Verifying Correct User ID

To verify that you get the correct user ID with the header you provided, go to <https://<HPBSM server>/topaz/verifyIDM.jsp?headerName=sea> (if **sea** is your header).

25

LDAP Authentication and Mapping

This chapter includes:

Concepts

- ▶ LDAP Authentication — Overview on page 652
- ▶ Mapping Groups on page 652
- ▶ Synchronizing Users on page 654
- ▶ Achieving Finer Control over Default User Permission Assignments on page 657

Tasks

- ▶ How to Map Groups and Synchronize Users on page 659
- ▶ How to Synchronize Users After Upgrading from a Previous Version of BSM on page 662
- ▶ How to Modify the Attribute Used to Log into BSM on page 663
- ▶ How to Delete Obsolete Users on page 663

Reference

Troubleshooting and Limitations on page 664

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 BSM service. You can also use the LDAP server to synchronize BSM and LDAP users. For optimal performance, it is recommended that the LDAP server be in the same subnet as the rest of the BSM servers. For optimal security, it is recommended to either configure an SSL connection between the BSM Gateway Server and the LDAP server, or to have BSM 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 BSM 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 619.

For details on securing communication between an LDAP server and your BSM 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 BSM 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 manually assign users to groups using the Hierarchy tab.

Note: Users who are not assigned to any group will appear at the Root (All) level, with the role defined in **Automatically Created User Roles**, in **Infrastructure Settings**, under **LDAP Configuration**. In this does not give you sufficient control of user permissions, see "Achieving Finer Control over Default User Permission Assignments" on page 657.

Note: Some customers like the concept of automatic user creation but prefer to put users into the appropriate BSM groups manually. However, as noted above, with user synchronization enabled, manual group assignment is disabled in BSM.

To assign users manually to the appropriate BSM group when LDAP User Synchronization is enabled, do the following:

- 1) Disable User Synchronization in **Group Mappings**.
- 2) Assign users to groups manually using the **Hierarchy** tab.
- 3) Re-enable User Synchronization in **Group Mappings**.

You can optionally map an LDAP group to multiple BSM groups, or multiple LDAP groups to a BSM group.

When enabling the Group Mapping feature, you can log into BSM 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 BSM" on page 663.

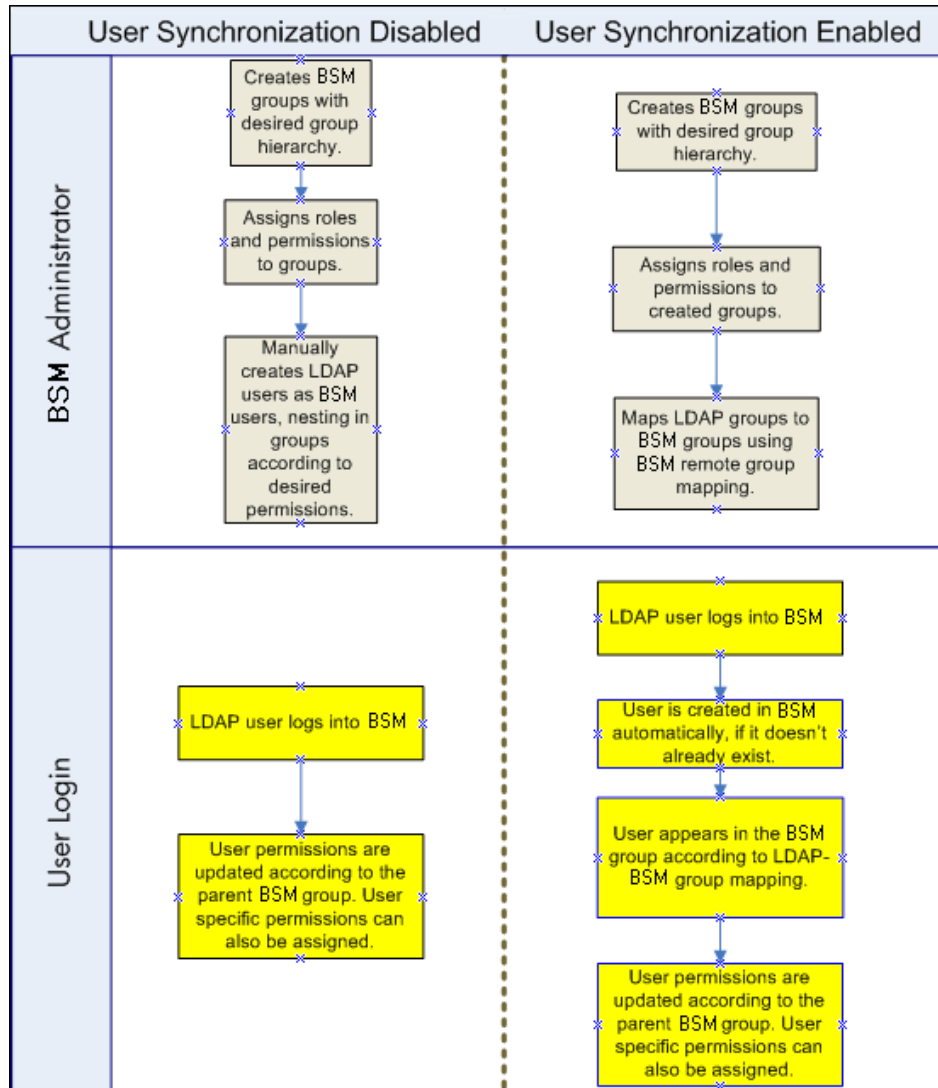
Synchronizing Users

The user synchronization feature maps users on an LDAP server to users in BSM. This simplifies the process of managing users for BSM 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 BSM, 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 BSM server after logging into BSM.

LDAP users who do not exist in, and log into, BSM, are created as BSM users. Their status is determined as follows:

- ▶ If the user belongs to a mapped LDAP group, she is automatically assigned to the BSM group that is mapped to their LDAP group.
- ▶ If their group is not mapped to a BSM group, or if they do not belong to an LDAP group, they are nested under the **Root** group and created as a BSM 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 BSM administrator and BSM itself when the user logs in:



For an LDAP user to log into BSM, he 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 630.

Note: Be aware that any new LDAP user who satisfies the user filter will be created as a BSM user on first login. Ask your LDAP administrator to help you narrow down the filter definition so that only appropriate users can gain access to BSM.

Users that have been removed from the LDAP server are still displayed as BSM users, even though they are no longer registered as LDAP users and cannot log into BSM. These users are called **Obsolete Users**. For details on removing Obsolete Users from BSM, see "How to Delete Obsolete Users" on page 663.

For details on synchronizing LDAP users with BSM users, see "How to Map Groups and Synchronize Users" on page 659.

For details on synchronizing groups after upgrading from a previous version of BSM, see "Synchronizing Users After Upgrading from a Previous Version of BSM" on page 656.

Synchronizing Users After Upgrading from a Previous Version of BSM

When upgrading from a previous version of BSM, 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 BSM using the **LDAP Configuration** button on the Users and Permissions interface. If you do not map the groups at this time, all BSM groups are nested under the Root directory.

Once the LDAP and BSM 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 BSM.

For details on performing this task, see "How to Synchronize Users After Upgrading from a Previous Version of BSM" on page 662.

Achieving Finer Control over Default User Permission Assignments

If you need a default group mapping for all users who do not fit into any of the currently mapped groups, and the default BSM user role (as defined in the infrastructure setting **Automatically Created User Roles** under **LDAP Configuration**) provides insufficient granularity, use the the Dynamic LDAP group feature in BSM.

Request that your corporate LDAP server administrator create a dynamic LDAP group based on the same user filter that you specified in the BSM LDAP configuration.

This user filter automatically populates and maintains members of the dynamic group in your corporate LDAP.

In BSM, create a local group with the roles and permissions that you require by default. Map the dynamic group created in your corporate LDAP to the BSM local group. Any user who is allowed to enter BSM but does not belong to any other mapped group will belong to the default group. Without such a default group, these users would be created at the root level in the User Management tree and their permissions would need to be handled individually.

To enable dynamic LDAP groups in BSM, go to **Infrastructure Settings**, select the **LDAP Configuration** context and set **Enable Dynamic Groups** to true. The change takes effect immediately.

Before dynamic groups are enabled, **List Users**, in the Group Mappings dialog box under **Users and Permissions**, will not display members of the dynamic group.

Note: Because corporate LDAP groups can be very large, **List Users** will display only up to the first 100 users. To see the whole user list or search for specific users, use a standard LDAP browser.

Tasks

How to Map Groups and Synchronize Users

This task describes how to map LDAP groups to BSM groups, and how to synchronize LDAP users with BSM users:

This task includes the following steps:

- "Configure the LDAP Server for Mapping Groups" on page 659
- "Create BSM Groups and Hierarchy" on page 659
- "Map LDAP Groups to BSM Groups" on page 659
- "Enable User Synchronization" on page 661

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 619.

2 Create BSM Groups and Hierarchy

You create local groups in BSM 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 570.

3 Map LDAP Groups to BSM Groups

You map user groups on the LDAP server to groups in BSM.

Caution: Administrators must do one of the following, to avoid being locked out of BSM when logging out after enabling the LDAP server but before configuring group mapping and user synchronization:

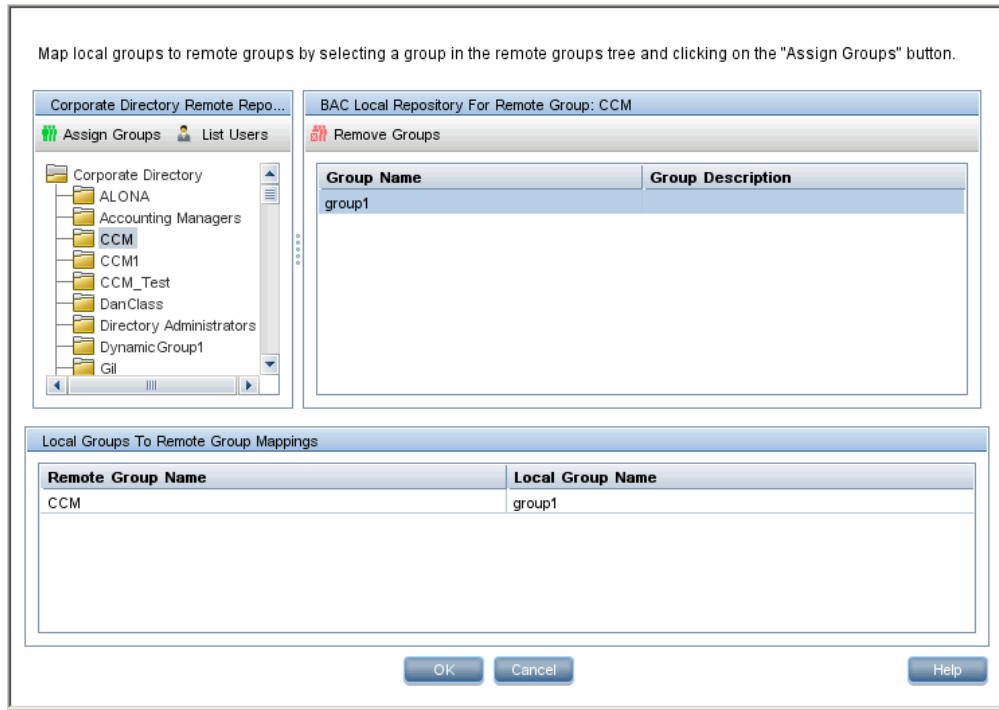
- Ensure that they have mapped their own group, to enable logging into BSM after enabling User Synchronization.
 - Create an account in BSM with superuser permissions.
-



- 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 BSM 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.



4 Enable User Synchronization

You enable synchronization of user groups on the LDAP server with user groups in BSM 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 BSM that matches your own LDAP user login, or mapped an appropriate LDAP group to a BSM group that has the **superuser** role assigned to it. If you have not done so, and log out of BSM after enabling LDAP but before group mapping is completed and user synchronization is enabled, the designated BSM superuser account will be locked out of BSM.
 - ▶ To disable user synchronization and enable management of users through the User Management interface in BSM, clear the **Enable User Synchronization** check box 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 631.

How to Synchronize Users After Upgrading from a Previous Version of BSM

To synchronize LDAP and BSM users after upgrading from a previous version of BSM:

- 1** If you have upgraded from a version prior to BSM 7.50, ensure that the **Enable User Synchronization** check box on the **LDAP Users Synchronization** page of the Authentication Wizard is cleared.
- 2** Ensure that LDAP groups have been mapped to BSM groups. For details on performing this task, see "How to Map Groups and Synchronize Users" on page 659.
- 3** Navigate to the LDAP Users Synchronization page in the Authentication Wizard, and select the **Enable User Synchronization** check box.

How to Modify the Attribute Used to Log into BSM

This task describes how to modify the LDAP attribute with which you want to log into BSM.

To modify the LDAP attribute with which you want to log into BSM:

- 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 BSM 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 BSM to use LDAP Authentication and are unable to log into BSM, 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.
- ▶ When BSM is installed with an Oracle database and User Synchronization is enabled with an LDAP Active Directory server, ensure that you log into BSM with the correct-case UID (uppercase or lowercase), as configured on the LDAP server. This is because while the Oracle database is case sensitive, the LDAP Active Directory is case insensitive, and logging in with an incorrect case UID can create undesirable results.

For example, if a user called **testuser** exists on the LDAP Active Directory server and logs into BSM, he is automatically created as BSM user **testuser**, who can be assigned permissions in the BSM User Management interface. If you then log into BSM as **Testuser**, the LDAP Active Directory server sends an acknowledgement that the user exists (because Active Directory is case insensitive) and he is allowed entry to BSM. However, since the Oracle database does not identify this user as **testuser** (because the Oracle database is case sensitive), the user **Testuser** is treated as a new user, without the permissions that were assigned to **testuser**.

26

LW-SSO Authentication – General Reference

This chapter includes:

Concepts

- ▶ LW-SSO Authentication Overview on page 666

Reference

- ▶ LW-SSO System Requirements on page 668
- ▶ LW-SSO Security Warnings on page 669

Troubleshooting and Limitations on page 671

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 2.4.

This section includes the following topics:

- ▶ “LW-SSO Token Expiration” on page 666
- ▶ “Recommended Configuration of the LW-SSO Token Expiration” on page 666
- ▶ “GMT Time” on page 667
- ▶ “Multi-domain Functionality” on page 667
- ▶ “Get SecurityToken for URL Functionality” on page 667

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 `lwssso` 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 `lwssso` 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 6.0.29 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 log on manually 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.

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.companymain.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, an 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.

To solve this issue, add the launched application (or a DNS domain subset as *.mydomain.com) to the Intranet/Trusted zone on your computer (for example, 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.

Part V

Report and Alert Admin

27

Report Schedule Manager

This chapter includes:

Concepts

- ▶ Report Schedule Manager — Overview on page 678

Reference

- ▶ Report Schedule Manager User Interface on page 679

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 Report Manager" in *Reports*.

Reference

Report Schedule Manager User Interface

This section includes:








- ▶ Report Schedule Manager Main Page on page 679

Report Schedule Manager Main Page

This page enables you to manage schedules configured on favorite filter reports and some of the user reports in the Report Manager.

To access	Select Admin > Platform > Report Scheduling
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 Report Manager" in <i>Reports</i> .
Relevant tasks	"How to Create and Manage User Reports Using Report Manager" in <i>Reports</i> .

User interface elements are described below:

UI Element (A–Z)	Description
	<p>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 <i>Reports</i>.</p> <p>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 Report Manager" in <i>Reports</i>.</p>
	<p>Deletes the selected schedule.</p>
	<p>Resumes the selected schedule.</p>
	<p>Pauses the selected schedule.</p>
	<p>Refreshes the Report Schedule Manager page.</p>
	<p>Resets the width of the columns to the default setting.</p>
	<p>Enables you to select columns to be visible in the table.</p>
<p>Generation Time</p>	<p>The time (in the indicated time zone) that the schedule is to be generated.</p>
<p>Recipients</p>	<p>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 <i>Reports</i>.</p>
<p>Recurrence</p>	<p>The recurrence pattern for the selected schedule.</p>
<p>Report Name</p>	<p>The name of the report for which the schedule is configured.</p>

UI Element (A-Z)	Description
Report Type	The type of report for which the schedule is configured.
Status	The status of the schedule. Possible values are: <ul style="list-style-type: none"><li data-bbox="621 319 725 343">▶ Active<li data-bbox="621 355 729 380">▶ Paused

28

Setting Up an Alert Delivery System

This chapter includes:

Concepts

- ▶ Alerts Overview on page 684
- ▶ Alerts and Downtime on page 687
- ▶ Planning for Effective Alert Schemes on page 688

Tasks

- ▶ How to Set Up an Alert Delivery System on page 689
- ▶ How to Customize Alerts on page 694

Reference

- ▶ Alert Logs on page 706
- ▶ Alert Details Report on page 708

Troubleshooting and Limitations on page 709

Concepts

Alerts Overview

BSM 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 689.

This section includes the following topics:

- ▶ "Alert Recipients" on page 684
- ▶ "Notification Template" on page 684
- ▶ "Alert Schemes" on page 684
- ▶ "Open Events in OM" on page 685
- ▶ "Alert History" on page 686
- ▶ "Delivery of Alerts" on page 686

Alert Recipients

Alerts can be configured to send notification to specified recipients. For task details on configuring recipients, see "Recipient Management" on page 577.

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 714.

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 "Planning for Effective Alert Schemes" on page 688.

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 BSM. 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 alert is triggered in BSM. 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 alerts that were triggered 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 alerts that were triggered 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 the details for the EUM alerts sent by BSM 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" on page 406.

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 actions**
- **Suppress alerts and close events**
- **Enforce downtime on KPI calculations; suppress alerts and close events**
- **Enforce downtime on Reports and KPI calculations; suppress alerts and close events**
- **Stop active monitoring (BPM & SiteScope); enforce downtime on Reports & KPI calculations; suppress alters and close events (affects all related SLAs)**

CI Status or EUM alerts for CIs that are in a scheduled downtime are not sent for all the options listed above apart from the **Take no action** option.

The CI alert is sent even if one of the options listed above is selected (apart from the **Take no action** option), 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 689.

For user interface details, see "Downtime Management Page" on page 417.

Planning for 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 BSM 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.

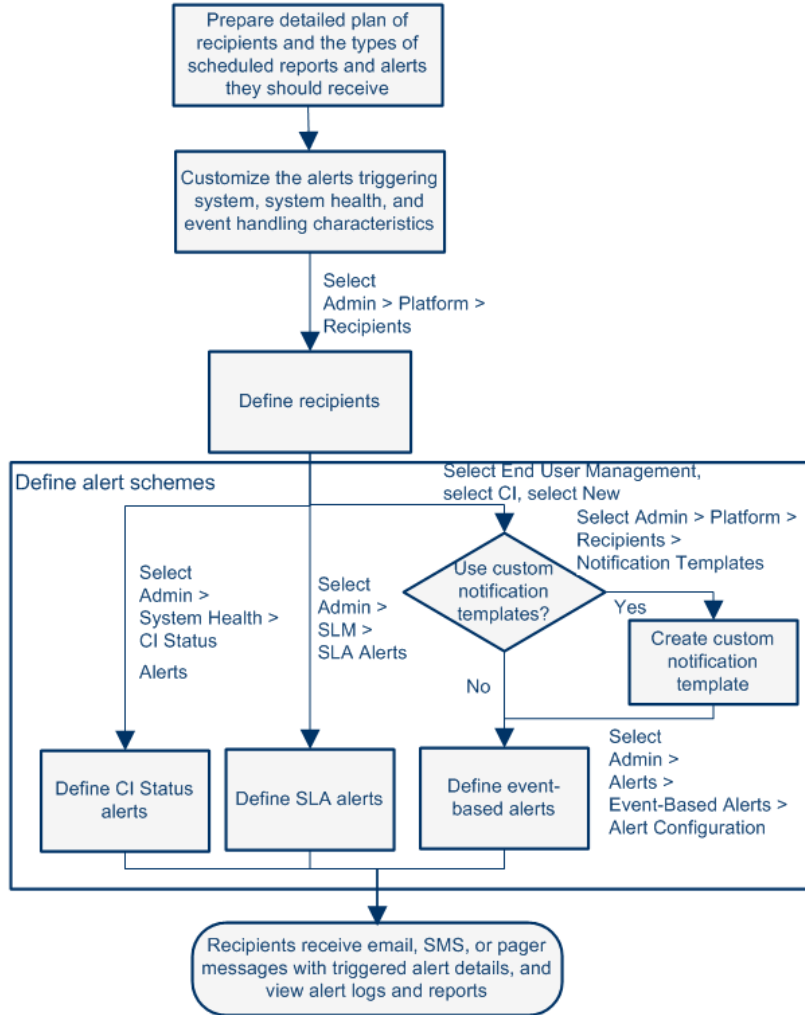
Tasks

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 691
- "Specify the appropriate user permissions" on page 691
- "Specify how alerts are triggered during downtime" on page 692
- "Customize the alerts triggering system, alerts system health, and event handling characteristics – optional" on page 692
- "Define recipients" on page 693
- "Create custom notification templates – optional" on page 693
- "Set up to open an event in HP Operations Manager and Operations Management when an alert is triggered in BSM" on page 693
- "Result - define the alerts schemes" on page 693



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 "Planning for Effective Alert Schemes" on page 688.
- ▶ 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 693.

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 Management** 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 **RTSM** 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" on page 450.

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 687.

For user interface details, see "Downtime Management Page" on page 417.

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 694.

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 560.

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 714.

7 Set up to open an event in HP Operations Manager and Operations Management when an alert is triggered in BSM

You can set up to open events in HP Operations Manager and Operations Management when an alert is triggered in BSM. 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, SLA, and EUM alerts.

- ▶ "Modify the way events are handled" on page 694
- ▶ "Modify the Alerting System Health parameters" on page 695
- ▶ "Modify the alerts triggering defaults" on page 696
- ▶ "Modify the way alerts are sent by email" on page 701
- ▶ "Modify the way alerts are sent by pager" on page 701
- ▶ "Modify the way alerts are sent by SMS" on page 702
- ▶ "Modify the way notifications are handled" on page 702

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:
 - **Acceptable event delay (minutes)**. Used to specify the default delay for alerts. Modify the default delay (60 minutes) after which alerts are discarded.
 - **Calculation persistency**. Used to enable/disable 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

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:
 - ▶ **Error threshold for the notification queue monitor.** Used to specify when the notification queue status changes to error. Enter the maximum number of messages that can wait in the alert queue of the notification queue monitor. When the maximum is reached the notification queue monitor status changes to **error**.
 - ▶ **Warning threshold for the notification queue monitor.** Used to specify when the notification queue status changes to warning. Enter the maximum number of messages that can wait in the alert queue of the notification queue monitor. When the maximum is reached the notification queue monitor status changes to **warning**.
 - ▶ **Error threshold for the alert queue monitor.** Used to specify when alert queue status changes to error. Enter the maximum number of messages that can wait in the alert queue of the alert queue monitor. When the maximum is reached the alert queue monitor status changes to **error**.
 - ▶ **Warning threshold for the alert queue monitor.** Used to specify when alert queue status changes to warning. Enter the maximum number of messages that can wait in the alert queue of the alert queue monitor. When the maximum is reached 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:
 - ▶ **Command line execution timeout (seconds).** You can modify the default timeout for an action (30 seconds) after which a command line alert action is not executed.

- ▶ **Default SNMP Target Address or Default SNMP Port.** You can 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 traps 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.

- ▶ **Command line substitution pairs.** When specifying a command in the Executable Files action of an EUM alert, you can use special tokens that are replaced with actual values when the command is prepared for execution. Those values might include a double quote (") or other tokens that may cause the resulting command line to be inappropriately interpreted by the operating system. To avoid this misinterpretation, you can modify the default value of the **Command line substitution pairs** infrastructure setting, as follows:
 - ▶ Each pair is written using the **|a|b|** format.
 - ▶ The **a** character is replaced by **b**.

- ▶ Multiple pairs are separated by a comma (,).
For example: |a|b|,|c|d|, |e|f|.
- ▶ **Enable alert dependencies across CIs.** Use to enable alert dependencies between CIs. Select:
 - ▶ **false.** (Default) Alert dependencies are not allowed between CIs.
 - ▶ **true.** Alert dependencies are allowed between CIs.
- ▶ **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 logging to DB.** Enable logging alerts and notifications in the 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.For details about the logs, see "Alert Logs" on page 706.
- ▶ **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.

- ▶ **Legacy SNMP Target Address or Legacy SNMP Port.** Used to modify the default SNMP Trap host address for EUM alerts. 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.

- ▶ **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.
- ▶ **Notification URL.** Use to customize the URL embedded in the notifications.
- ▶ **Symphony request timeout (seconds).** Use to specify the number of seconds until an alert action times out.
- ▶ **Wait interval between retries (seconds).** Use to specify the number of seconds between each attempt to execute a notification.
- ▶ **Default EXE path.** Use to specify the default path to the default executable for EUM alerts.
- ▶ **Default URL.** Use to specify the default URL address for EUM alerts.
- ▶ **Recipient information format in template.** Use to modify how to display the recipient list in Emails or SMSs. You can assign the following values:
 - ▶ **Address.** To display the complete email of the recipients in the **To** field of Emails and SMS notifications. For example, if you set **Recipient information format in template** to **Address** and the template includes the following parameters: **To:**<<Recipients>>, **Profile Name:** <<Profile Name>>, **Severity:** <<Severity>>, then the Email is as follows:

To:gaz@devlab.ad;shifv@devlab.ad;aahhh.hhheee@hp.com
Profile Name: forAlert
Severity: Major
 - ▶ **Logical Name.** To display the logical name of the recipients in the **To** field of Emails and SMS notifications. For example, if you set **Recipient information format in template** to **Logical Name** and the template includes the same parameters as the example above, then the Email is as follows:

To:aa;bac admins
Profile Name: forAlert
Severity: Major

Modify the way alerts are sent by email

To modify the way email alerts are handled, select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**:

- ▶ Select **Foundations**.
- ▶ Select **Platform Administration**.
- ▶ In the **Platform Administration - Alerts E-Mail Settings** table, locate and modify the following parameters:
 - ▶ **Password for authorized email setting**. Used to modify the default password for authorized sending of email alerts.
 - ▶ **SMTP server (Windows only)**. Used to specify the primary SMTP server used. In windows NT, set as <SMTPSVC> if you want to send using the SMTP service.
 - ▶ **SMTP server port (Windows only)**. Used to specify the SMTP server port.
 - ▶ **User for authorized email sending**. Used to modify the default user for authorized sending of email alerts. If not set, email alerts are sent without authorization.

Modify the way alerts are sent by pager

To modify the way pager alerts are handled, select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**:

- ▶ Select **Foundations**.
- ▶ Select **Platform Administration**.
- ▶ In the **Platform Administration - Alerts Pager Settings** table, locate and modify the following parameters:
 - ▶ **Password for authorized pager setting**. Used to modify the default password for authorized sending of pager alerts.
 - ▶ **SMTP server (Windows only)**. Used to specify the primary SMTP server used. In windows NT, set as <SMTPSVC> if you want to send using the SMTP service.

- **SMTP server port (Windows only).** Used to specify the SMTP server port.
- **User for authorized pager sending.** Used to modify the default user for authorized sending of pager alerts. If not set, pager alerts are sent without authorization.

Modify the way alerts are sent by SMS

To modify the way SMS alerts are handled, select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**:

- Select **Foundations**.
- Select **Platform Administration**.
- In the **Platform Administration - Alerts SMS Settings** table, locate and modify the following parameters:
 - **Password for authorized SMS setting.** Used to modify the default password for authorized sending of SMS alerts.
 - **SMTP server (Windows only).** Used to specify the primary SMTP server used. In windows NT, set as <SMTPSVC> if you want to send using the SMTP service.
 - **SMTP server port (Windows only).** Used to specify the SMTP server port.
 - **User for authorized SMS sending.** Used to modify the default user for authorized sending of SMS alerts. If not set, SMS alerts are sent without authorization.

Modify the way notifications are handled

To modify the way notifications are handled, select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**:

- Select **Foundations**.
- Select **Platform Administration**.
- In the **Platform Administration - Recipient Notification Service** table, locate and modify the following parameters:

- **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 BSM sends alerts is set when you install the Data Processing Server.
- **Alternate SMTP server port (Windows only), and Alternate SMTP server (Windows only).** Used to modify the alternate SMTP server:
 - **A designated server with a defined port number.** Enter a server name for sending SMTP emails as the value in the **Alternate SMTP server** field and enter a port number for the server in the **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: _ . -

- **Email notification 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:
 - **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.

- **Email sender.** Use to specify the name of the sender of alert emails.
- **Enable recipient notifications.** Set to **false** to prevent notifications from being sent to recipients. Set to **true** to send notifications to recipients.

- **Pager notifications charset.** Defines the character set used to send pager notification messages. You can select one of the following character sets:
 - **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.

- **Password for authorized message sending.** Use the parameter to specify a default password for authorized message sending. If not set, messages are sent without authorization.
 - **SMS notifications charset.** Defines the character set used to send SMS notification messages. You can select one of the following character sets:
 - **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 (Windows only).** Used to specify the primary SMTP server used. In windows NT, set as <SMTPSVC> if you want to send using the SMTP service.
- **SMTP server port (Windows only).** Used to specify the SMTP server port.
- **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.

- **User for authorized message sending.** Use the parameter to specify a default user for authorized message sending. If not set, messages are sent without authorization.

Note: This is for Windows operating systems only.

Reference

Alert Logs

You can use the following logs to debug the CI Status, SLA, and EUM alerts.

Alert Type	Path to Log and to Properties File for Log Level Setup	Description
All alerts	Log: <BSM_data_processing_server>\log\alerts\alerts.ejb.log Setup: <BSM_data_processing_server>\conf\core\Tools\log4j\EJB\alerts.properties	Alerts and notifications handling in the MercuryAs process
	Log: <BSM_Gateway_server>\log\alerts\alerts.reports.log Setup: <BSM_Gateway_server>\conf\core\Tools\log4j\EJB\alerts.properties	For all alert reports
CI Status alerts and SLA alerts	Log: <BSM_data_processing_server>\log\marble_worker_1\status.alerts.log Setup: <BSM_data_processing_server>\conf\core\Tools\log4j\marble_worker\cialerts.properties	Alert init and calculation in the MAR Business Logic Engine worker process
	Log: <BSM_data_processing_server>\log\marble_worker_1\status.alerts.downtime.log Setup: <BSM_data_processing_server>\conf\core\Tools\log4j\marble_worker\acialerts.properties	Alert downtime handling in the MAR Business Logic Engine worker process
	Log: <BSM_Gateway_server>\log\alerts\alertui.log Setup: <BSM_Gateway_server>\conf\core\Tools\log4j\EJB\alerts.properties	Alert administration

Alert Type	Path to Log and to Properties File for Log Level Setup	Description
EUM alerts	Log: <BSM_data_processing_server>\log\alerts\alert.rules.log Setup: <BSM_data_processing_server>\conf\core\Tools\log4j\marble_worker\alerts-rules.properties	Alert calculation in the MAR Business Logic Engine worker process
	Log: <BSM_data_processing_server>\log\alerts\alerts.rules.init.log Setup: <BSM_data_processing_server>\conf\core\Tools\log4j\marble_worker\alerts-rules.properties	Alert initialization in the MAR Business Logic Engine worker process
	Log: <BSM_data_processing_server>\log\alerts\alerts.downtime.log Setup: <BSM_data_processing_server>\conf\core\Tools\log4j\marble_worker\alerts-rules.properties	Alert downtime handling in the MAR Business Logic Engine worker process


Note: When you modify a log properties file on one of the BSM processing servers, it affects only the logs on this BSM processing server.

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	<p>For CI Status Alerts, see details about the Alert Details page in "Configuration Item Status Alert Notifications Report" in <i>Using Service Health</i>.</p> <p>For SLA Status Alerts, see details about the Alert Details page in "SLA Status Alert Notifications" in <i>Using Service Level Management</i>.</p> <p>For EUM alerts, see details about the Alert Details page in "Alert Details" in <i>Using End User Management</i>.</p>

Troubleshooting and Limitations

This section describes troubleshooting and limitations for alerts.

Emails Are Not Received by Recipients When an Alert Should Have Been Triggered

If emails are not received by recipients, check the following possibilities:

- ▶ The alert definition is not as expected. Check the alert definition in the relevant alert administration.
- ▶ The data does not behave as expected so the alert triggering condition might not exist. Check the alert calculation log or check the specific data origin logs and reports. For details, see "Alert Logs" on page 706.
- ▶ There might be a connection problem with the SMTP email server. To check if the server works, **run telnet <smtp_server_host_name_or_IP_nbr> 25**.
- ▶ The email address of the recipient might not be valid. Examine the recipient definition in the user interface, and manually send an email to the recipient to check the address's validity.
- ▶ The recipient considers the alert email as spam. You might have to ask the recipient's administrator to reconfigure the spam filter.

29

Configure EUM Alerts Notification Templates

This chapter includes:

Concepts

- ▶ EUM Alerts Notification Templates on page 712
- ▶ Clear Alert Notification Templates on page 713

Tasks

- ▶ How to Configure EUM Alerts Notification Templates on page 714
- ▶ How to Configure a Template for Clear Alert Notifications on page 715

Reference

- ▶ EUM Alerts Notification Templates User Interface on page 716

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 723.

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 723.

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 531.

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 715.

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 712.

This task includes the following steps:

- ▶ "Create custom templates" on page 714
- ▶ "Manage existing templates" on page 714

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 716.

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 723.

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 713.

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 716. 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 723.

Reference


EUM Alerts Notification Templates User Interface

This section describes:

- ▶ Notification Template Properties Dialog Box on page 716
- ▶ Notification Templates Page on page 723

Notification Template Properties Dialog Box

This dialog box enables you to define a new alerts notification template.

To access	<ul style="list-style-type: none">▶ 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 .
------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p>Important information</p>	<p>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 your 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 <code>_FOLLOWUP</code> (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.</p> <p>Example: If you are creating a clear alert template based on the LONG default template, you would call the clear alert template <code>LONG_FOLLOWUP</code>. If the clear alert template is based on a user-defined template called MyTemplate, name the clear alert template <code>MyTemplate_FOLLOWUP</code>.</p> <p>Default: The <code>_FOLLOWUP</code> string is the default string recognized by BSM as the template name for a clear alert message.</p> <p>Customization: You can customize the <code>_FOLLOWUP</code> string. For details, see "How to Configure a Template for Clear Alert Notifications" on page 715.</p>
<p>Relevant tasks</p>	<p>"How to Configure a Template for Clear Alert Notifications" on page 715</p>

General Information Area

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

UI Element (A-Z)	Description
<Insert>	<p>Select a parameter to add to the section. Repeat to add as many text parameters as you want from the list.</p> <p>Add free text before or after the text parameters. The text parameters available for this section are:</p> <ul style="list-style-type: none"> ▶ 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 BSM 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	<p>Enter a name for the template.</p> <p>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.</p>
Subject	<p>Specify the information that you want BSM to include in the subject of the email, pager message, or SMS message.</p> <p>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.</p>

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>	<p>Select a parameter to add to the section. Repeat to add as many text parameters as you want from the list.</p> <p>Add free text before or after the text parameters. The text parameters available for this section are:</p> <ul style="list-style-type: none"> ▶ 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 BSM 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. <ul style="list-style-type: none">▶ 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>	<p>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:</p> <ul style="list-style-type: none"> ▶ 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>	<p>Select a parameter to add to the section. Repeat to add as many text parameters as you want from the list.</p> <p>Add free text before or after the text parameters. The text parameters available for this section are:</p> <ul style="list-style-type: none"> ➤ 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 BSM 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	<p>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 715.</p> <p>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.</p> <p>BSM uses the clear alert notification template that you create under the following circumstances:</p> <ul style="list-style-type: none"> ▶ 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 714

User interface elements are described below:

UI Element (A-Z)	Description
	<p>Click to duplicate notification template. Clones the selected notification template. The Notification Template Properties dialog box opens where you can edit the cloned notification. For details, see "Notification Template Properties Dialog Box" on page 716.</p>
	<p>Click to modify notification template properties. Click to edit the selected template. For details, see "Notification Template Properties Dialog Box" on page 716.</p>
	<p>Click to delete notification template. Delete the selected templates simultaneously.</p> <p>To delete multiple templates simultaneously, select their check boxes, and click the  button located at the bottom of the templates list.</p>
<p>New Template</p>	<p>Click the New Template button to open the Notification Template Properties dialog box. For details, see "Notification Template Properties Dialog Box" on page 716.</p>

UI Element (A-Z)	Description
Notification Template Name	<p>Lists the default templates and the custom templates. The default templates are:</p> <ul style="list-style-type: none"> ▶ 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 715. ▶ 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. <p>Note: For details on the parameters displayed in each template, see "Notification Template Properties Dialog Box" on page 716.</p>

Part VI

Troubleshooting

30

Platform Administration Troubleshooting

This chapter includes:

Troubleshooting and Limitations on page 729

Troubleshooting and Limitations

This section describes common problems that you may encounter when working in the Platform Administration area of BSM.

For additional troubleshooting information, use the HP Software Self-solve knowledge base (h20230.www2.hp.com/selfsolve/documents).

This section includes the following topics:

- ▶ "Need to change password for access from data collectors (RUM, TV, BPI, Diagnostics) to RTSM" on page 730
- ▶ "RTSM Administration pages do not load" on page 731
- ▶ "Java applets fail to load with "class not found" error" on page 731
- ▶ "Java applets fail to load" on page 731
- ▶ "Intermittent UI failures after connecting through Load Balancer" on page 731
- ▶ "BSM Login page does not appear when connecting through Load Balancer" on page 731
- ▶ "BSM dialog boxes and applets, such as the Authentication Wizard, do not load properly" on page 732
- ▶ "BSM has been installed, but the Downloads page is empty" on page 732
- ▶ "General connectivity problems related to ports" on page 732

- ▶ "BSM connectivity is down, but the Tomcat servlet engine and jboss application server appear to be working" on page 733
- ▶ "Inability to log into BSM, and jboss application server fails to initialize" on page 734
- ▶ "Browser unable to reach BSM and an error about insufficient heap space" on page 734
- ▶ "Browser unable to reach BSM or the .jsp source code appears in the browser window" on page 735
- ▶ "BSM is sitting behind a proxy and the server name is not recognized by the proxy" on page 736
- ▶ "Host names of Gateway or Data Processing Server has changed" on page 736
- ▶ "Processes do not resume restart automatically after automatic failover" on page 737

Need to change password for access from data collectors (RUM, TV, BPI, Diagnostics) to RTSM

During deployment, you can optionally set an **Access to RTSM password** to secure communication between BSM data collectors (such as Real User Monitor, Business Process Insight, and TransactionVision), and the Runtime Service Model. This password can be changed later using the JMX console.

To modify the password for RTSM access using 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. (For detailed instructions, see "Using the JMX Console" on page 34.)
- 2** Enter your JMX console authentication credentials. If you do not know your authentication credentials, contact your system administrator.
- 3** In the **Foundations** domain, select the service **RTSM passwords manager**.
- 4** Modify **changeDataCollectorsOdbAccessPwd**. The operation gets customer ID and new password as parameters and changes all data collector passwords to the new one.

RTSM Administration pages do not load

If the links from RTSM Administration do not work, this may be caused by one of the following:

- ▶ Make sure that the BSM Gateway Server is able to access the Default Virtual Server for Application Users URL. This URL can be found in **Admin > Platform > Setup and Maintenance > Infrastructure Settings**. In the **Foundations** field, specify **Platform Administration**. The URL is located in the **Host Configuration** table.
- ▶ If you are using a reverse proxy or load balancer, make sure you log in through the URL specified above.

Java applets fail to load with "class not found" error

Make sure that you created a Profile Database. This database must be created manually in Platform Administration. For more information, see "Database Administration" in *Platform Administration*.

Java applets fail to load

Open **Control Panel > Java > Temporary Internet Files > Settings** and make sure **Keep temporary files on my computer** is checked. If the problem persists, clear the Java cache by clicking **Delete Files** in the same location.

Intermittent UI failures after connecting through Load Balancer

BSM requires sticky sessions for users. Make sure the persistency settings are set to **stickiness by session enabled** or **Destination Address Affinity** (depending on the Load Balancer).

BSM Login page does not appear when connecting through Load Balancer

- ▶ Check the KeepAlive URIs. For more information, see "Load Balancing for the Gateway Server" on page 56.
- ▶ Virtual hosts and Load Balancer should be configured with a fully qualified domain name (and not an IP) for LW-SSO to work.

BSM dialog boxes and applets, such as the Authentication Wizard, do not load properly

Possible Cause:

Old java files on your client PC.

Solution:

Clear the java cache by following this procedure:

- ▶ Navigate to **Start > Control Panel > Java**.
- ▶ In the Temporary Internet Files section, click **Settings**.
- ▶ In the Temporary File Settings dialog box, click **Delete Files**.

BSM has been installed, but the Downloads page is empty

Possible Cause:

The components setup files have not been installed to the Downloads page.

Solution:

Install the components setup files to the Downloads page. For details on installing the component setup files on a Windows platform, see "Installing Component Setup Files" on page 133.

General connectivity problems related to ports

Verify that all ports required by BSM servers are not in use by other applications on the same machine. To do so, open a Command Prompt window, and run netstat (or use any utility that enables you to view port information). Search for the required ports.

You can also check the <HPBSM root directory>\log\EJBContainer \jboss_boot.log for ports in use. If the jboss_boot.log reports "Port <> in use" but you do not see that this port is in use when you run netstat utility, restart the server and then start BSM.

For details on the ports required by BSM, see Port Usage in the *HP Business Service Management Hardening Guide* PDF.

Tip: To troubleshoot port usage problems, use a utility that lists all ports in use and the application that is using them.

BSM connectivity is down, but the Tomcat servlet engine and jboss application server appear to be working

Connectivity problems include the inability to log into BSM, and the inability of Business Process Monitor to connect to the Gateway Server.

Possible Cause:

This can happen if the **TopazInfra.ini** file is empty or corrupt.

To verify that this is the problem:

1 In the browser, type <http://<Gateway Server>:8080/web-console> to connect to the JMX Console.

If prompted, enter the JMX Console authentication credentials (if you do not have these credentials, contact your system administrator).

2 Under **System > JMX MBeans > Topaz**, select **Topaz:service=Connection Pool Information**.

3 Click the **showConfigurationSummary Invoke** button toward the bottom of the page. If the Operation Result page is blank, the **TopazInfra.ini** file is empty or corrupt.

Solution:

To solve this problem, rerun the Setup and Database Configuration utility and either reconnect to your existing management database or define a new management database. If you did not discover a problem with the **TopazInfra.ini** file, contact HP Software Support.

Inability to log into BSM, and jboss application server fails to initialize

Run the database schema verify program to verify that the database server on which the management database is located is up and running. For details, see Appendix D, "Database Schema Verification" in the *HP Business Service Management Database Guide* PDF.

Browser unable to reach BSM and an error about insufficient heap space

A message box opens indicating that BSM is not available and you should try logging in at a later time.

Possible Cause 1:

Check log files in <HPBSM root directory>\log directory for errors.

Microsoft's Security Update 921883 for Windows 2003 Service Pack 1 and for Windows XP Professional x64 Edition may cause applications using more than 700 MB of contiguous memory to fail. BSM JVM uses a heap size larger than 768 MB memory. For more information about Security Update 921883, see <http://www.microsoft.com/technet/security/Bulletin/MS06-040.msp>.

If the BSM server goes down, look for the following error in <HPBSM server root directory>\log\jboss_boot.log when the service or process is restarted:

Error occurred during initialization of VM.
Could not reserve enough space for object heap.

Solution:

Although Microsoft has a hotfix available only for Microsoft Support customers, it is recommend to wait for the next Service Pack release. For more information about this hotfix, see

<http://support.microsoft.com/kb/924054>.

If Security Update 921883 is already installed, do the following:

- ▶ If the Security Update is not critical at your site:
 - ▶ Uninstall it and wait for Microsoft's next Service Pack.
 - ▶ Disable **Windows Automatic Updates** to prevent Security Update 921883 from being installed again.
- ▶ If the Security Update is critical at your site, install the hotfix.

Possible Cause 2:

The page file size is too small.

Solution:

Configure the page file size to be at least 150% of RAM size. Restart the server.

Browser unable to reach BSM or the .jsp source code appears in the browser window

A message box opens indicating that the BSM page does not exist.

Solution:

Ensure that the Jakarta filter path is correct. The path might be incorrect—for example, if you uninstall BSM servers and then reinstall to a different directory. In this case, the Jakarta filter path is not updated, causing redirection problems.

To update the Jakarta filter path:

- 1** Open the IIS Internet Services Manager.
- 2** Right-click the machine name in the tree and select **Properties**.
- 3** With **WWW Service** displayed in the Master Properties list, click **Edit**.

- 4 Select the **ISAPI Filter** tab.
- 5 Select **jakartaFilter** and click **Edit**.
- 6 In the **Filter Properties** box, update the path to point to the drive and directory of the current BSM installation.
- 7 Apply your changes and quit the Internet Services Manager.
- 8 Restart the IIS service.

BSM is sitting behind a proxy and the server name is not recognized by the proxy

The problem occurs for both Microsoft IIS and Apache Web servers.

Possible Cause:

The Web server redirects the browser page to a URL that replaces the server name entered by the user.

Solution:

Add the BSM server name to the <Windows system root directory>\system32\drivers\etc\hosts file on the proxy server machine.

Host names of Gateway or Data Processing Server has changed

You can no longer access BSM on the server names on which they were installed and must change the names of the servers. Refer to the HP Software Self-solve knowledge base, article number [KM522738](#), which can be accessed at <http://h20230.www2.hp.com/selfsolve/document/KM522738>.

Processes do not resume restart automatically after automatic failover

If the High Availability Controller's Automatic Failover mode is enabled and the management database has been down for some time, some processes may be stopped and will not resume automatically when the management database returns to normal operation. These processes will have the status **STARTING** on the BSM Status page (<**HPBSM root directory**>\AppServer\webapps\myStatus.war\myStatus.html, accessible on the Windows operating system from **Start > Programs > HP Business Service Management > Administration > HP Business Service Management Status**).

Solution:

Restart these processes once the management database is available again.

Index

A

- administrator
 - permission level 481
- advanced alert procedures
 - adding custom pager or SMS service provider 477, 579
- advanced procedures
 - modifying location and expiration of temporary image files 131
 - modifying the ping time interval 130
- Alert Details report 708
- alert notification template
 - configure 714
- alert notification templates 712
- alert recipients
 - notification templates 712
- alerts
 - adding custom pager or SMS service provider 477, 579
 - customizations 694
 - downtime 687
 - introduction 683
 - logs 706
 - notification template 711
 - overview 684
 - process flowchart 689
 - recipients 578
 - tips for creating 688
 - tips in creating 687
- applications
 - adding to server deployment 84, 90
- Attach Recipient to a User dialog box 582
- audit log 289
 - audit log page 295
 - file customization 294
 - overview 290
 - use 293
- audit logs
 - Alert Administration 290
 - CI Status Alert Administration 290
 - Data Collector Maintenance 290
 - Database Management 290
 - Deleted Entities 290
 - Downtime/Event Scheduling 290
 - End User Management-Applications 290
 - IT World Configuration 290
 - Locations Manager 290
 - Notification Template Administration 291
 - Operations Management 291
 - Permissions Management 291
 - Recipient Administration 291
 - Scheduled Report Administration 291
 - Service Health 291
 - Service Health Administration 291
 - Service Level Management Configuration 291
 - SLA Status Alert Administration 291
 - System Availability Manager 291
 - User Defined Reports 291
 - User/Group Management 291
 - View Manager 291
- authentication
 - Identity Management Single Sign-On 645
 - IDM-SSO 645
 - Lightweight Directory Access Protocol 651
 - LW-SSO general reference 665
 - LW-SSO, overview 666
- authentication strategy
 - HP Business Service Management login flow 35

Index

- overview 614
- user interface 617
- authentication wizard 619
 - introduction page 619
 - ldap advanced general configuration 630
 - LDAP users synchronization configuration page 631
 - ldap vendor attributes dialog box 630

B

- backup, recommendations 331
- BPM
 - administrator role 517
 - System Health monitors 244
 - viewer role 516
- browser language preference 308
- Business Process Insight context 526

C

- capacity calculator 84, 90
- clear alert notification template 713
- command-line interface
 - Content Packs Manager 381
- Configure HP Business Service Management menu option 27
- Content Pack Manager
 - content types 378
- content packs 363
 - automatically including dependent content 368
 - creating and editing content pack definitions 375
 - creating and managing 375
 - definitions 367
 - deleting referenced content pack 370
 - deleting referenced content pack on which dependency was set 373
 - dependencies 367
 - exporting 373, 376
 - importing 374, 376
 - referencing dependent content 369
 - setting dependency 371

- Content Packs Manager 364
 - command-line interface 381
 - Content Packs page 387
 - Create New Content Pack Definition wizard 392
 - definitions pane 388
 - details pane 390
 - Import Content Pack dialog 401
 - interfaces 366
 - shortcut menus 397
 - troubleshooting and limitations 403
 - user interface 366, 386
- content types 378
- ContentManager CLI 366, 381
- context
 - Business Process Insight 526
 - diagnostics 526
- context-sensitive menus
 - Content Packs Manager 397
- Create Group dialog box 553
- Create New Content Pack Definition wizard
 - content page 394
 - dependencies page 398
 - general page 392
 - summary page 400
- Create User dialog box 554
- custom for alerts 477, 579
- customer superuser permissions role (HP Software-as-a-Service) 502
- customization
 - user management 453

D

- data
 - partitioning and purging 121
 - removing from database 98
 - removing from database using Data Marking tool 102
- Data Flow Management
 - internationalization 307
- data marking
 - information window 115
 - troubleshooting and limitations 123
- Data Marking tool
 - maximum duration setting 110

- data marking utility 112
 - database maintenance
 - main page 111
 - database management 96
 - Data Marking tool 102
 - overview 96
 - removing historical data 98
 - database types
 - MS SQL server 97
 - Oracle server 97
 - databases
 - configuring 96
 - Daylight Saving Time
 - downtime 432
 - fall 434
 - spring 432
 - default container
 - in Location Manager 339
 - default profile database 96
 - delete security officer in JMX 470
 - dependencies
 - content packs 367
 - diagnostics
 - context 526
 - Direct Login dialog box 46
 - Documentation menu option 28
 - downloading components 73
 - available components 72
 - downloads 71, 74
 - overview 72
 - user interface 74
 - downtime
 - alerts 687
 - and event scheduling overview 406
 - Daylight Saving Time 432
 - management user interface 416
 - manager page 417
 - troubleshooting 431
 - wizard 421
- E**
- Edit Recipient dialog box 586
 - email
 - message character set 703
 - Email tab 592
- end-user management context
 - permissions 527
 - EPM
 - determining 109
 - Events Per Minute
 - determining 109
 - exporting
 - content packs 373, 376
- F**
- file backup recommendations 331
 - flash player requirements 61
 - follow-up notification template 715
- G**
- geographical coordinates
 - in Location Manager 339
 - geographical location
 - in Location Manager 338
 - Geographical Map dialog box
 - Location Manager 357
- H**
- hierarchy
 - in Location Manager 339
 - user management 451
 - HP Business Service Management site
 - system requirements for viewing 61
 - HP Software Support Web site 19
 - HP Software Web site 20
- I**
- Identity Management Single Sign-On 645
 - overview 646
 - IDM-SSO
 - overview 646
 - troubleshooting and limitations 649
 - image files, modifying settings for temporary
 - storage 131
 - importing
 - content packs 374, 376

Index

- infrastructure settings 127
 - overview 128
 - screen 141
- internationalization
 - administration issues 303
 - Business Process Monitor issues 305
 - Dashboard issues 304
 - Data Flow Management issues 307
 - database environment issues 302
 - End User Management issues 307
 - installation and deployment issues 300
 - multilingual issues 307
 - Real User Monitor issues 306
 - report issues 305
 - Service Level Management issues 305
 - SiteScope issues 306
- IP Range dialog box
 - Location Manager 356
- IP ranges
 - in Location Manager 339
- J**
- Java
 - requirements 61
 - troubleshooting 61
- JMX console
 - change password 42
 - remove security officer status 470
- K**
- Knowledge Base 19
- KPI Enrichment Service monitors 231
- L**
- language preference 308
- languages
 - working in non-English locales 299
- LDAP 651
 - deleting obsolete users 663
 - group mapping 652
 - map groups and synchronize users 659
 - overview 652
 - troubleshooting and limitations 664
 - user synchronization 654
- LI001 error 48
- LI002 error 48
- LI003 error 48
- LI004 error 48
- LI005 error 49
- LI006 error 50
- LI007 error 51
- License 79
- license update 84, 90
- licensing
 - additional licensing 78
- Lightweight Directory Access Protocol 651
 - deleting obsolete users 663
 - group mapping 652
 - map groups and synchronize users 659
 - overview 652
 - troubleshooting and limitations 664
 - user synchronization 654
- Lightweight Single Sign-On 635
 - overview 636
 - unknown user handling mode 638
 - updating using JMX Console 639, 643
- limitations
 - content packs 403
- link to this page 32, 41
 - dialog box 46
- locales
 - non-English 299
- Location Manager 337
 - default container 339
 - geographical coordinates 339
 - geographical location 338
 - Geographical Map dialog box 357
 - hierarchy 339
 - IP Range dialog box 356
 - IP ranges 339
 - logical location 339
 - mass upload 345
 - Overview 338
 - populating 339, 344
 - RUM locations 339
 - user interface 348
 - XML attribute table 361

- XML elements table 359
- XML file 341
- XML file example 342
- XML tag reference 359
- Location Manager page 349
- log manager 254
- logging in 29, 30
 - automatic login 39
 - automatic login URL mechanism 40
 - limiting access by different machines 41
 - modify the login attribute 663
- logging out 30
- logical location
 - in Location Manager 339
- login
 - advanced 32, 38
 - automatically to a specific page 41
 - precautions 44
 - security notes 44
- login error
 - LI001 48
 - LI002 48
 - LI003 48
 - LI004 48
 - LI005 49
 - LI006 50
 - LI007 51
- login failure
 - troubleshooting 47
- logs 313
 - alerts 706
 - automatic archiving 316
 - changing log levels 318
 - file locations 314
 - file locations in distributed deployment 314
 - JBoss and Tomcat logs 316
 - overview 314
 - severity levels 315
 - size limit 316
- LW-SSO 635
 - general reference 665
 - overview 636, 666
 - security warnings 669
 - system requirements 668

- troubleshooting and limitations 671
- unable to access 643
- updating using JMX Console 639, 643

M

- marking data for removal 102
- mass upload
 - Location Manager 345
- maximum duration setting
 - Data Marking tool 110
- menu customization 610
- message character set
 - modifying 703
- MS SQL server
 - configuring database 116
 - configuring profile database on 103
 - database for Application Management profiles 97
- multilingual user interface support 308

N

- navigation 53
 - menus and options 63
 - navigating HP Business Service Management 54
- New Recipient dialog box 586
- notification template
 - alerts 711
 - clear alerts 713
 - configure for alerts 714
 - follow-up alerts 715
- Notification Template Properties dialog box 716
- Notification Templates page 723

O

- online resources 19
- Operations Management
 - monitors 233
- operations orchestration context
 - permissions 538
- Oracle server
 - configuring profile user schema on 104

Index

- configuring user schema 118
- user schema for Application Management profiles 97
- P**
- Page tab 596
- pager
 - message character set 703
 - provider 477
- pager provider 579
- Partition and Purging Manager 121
 - partitioning data in database, purging data from database 98
- permissions
 - administrator role 481
 - BPM administrator 517
 - BPM viewer 516
 - Business Process Insight context 526
 - customer administrator role (HP Software-as-a-Service) 509
 - customer superuser role (HP Software-as-a-Service) 502
 - diagnostics context 526
 - end-user management context 527
 - operations orchestration context 538
 - platform 539
 - resources 446
 - RTSM context 531
 - RUM administrator 518
 - RUM viewer 518
 - security officer 450
 - service health context 545
 - service level management 546
 - superuser role 480
 - system availability management 547
 - system modifier role 492
 - system viewer role 498
 - user management 445
 - user-defined reports context 551
- personal settings
 - menu customizing 610
 - overview 600
 - refresh rate 608
 - time zone 608
 - user mode 608
- ping time interval, modifying 130
- platform
 - permissions 539
- Platform Administration
 - downloading components 72
 - troubleshooting 729
- Populate the Location Manager 344
- ports
 - incoming HP Business Service Management traffic 323
 - local HP Business Service Management traffic 326
 - manually changing 320
 - outgoing HP Business Service Management traffic 325
 - used by HP Business Service Management 319
- profile database
 - creating 96
 - properties 116
- R**
- Rapid Anomaly Detection Engine
 - monitors 237
- recipient
 - management 577
- Recipient tab
 - Personal Setting 611
 - User Management 560, 586
- recipients
 - alerts and reports 578
 - manage for alerts 456
 - process flowchart 689
- Recipients page 583
- refresh rate 608
- remove security officer JMX 470
- reports
 - recipients 578
- role
 - BPM administrator 517
 - BPM viewer 516
 - RUM administrator 518
 - RUM viewer 518
 - system modifier 492
 - system viewer 498

- roles
 - applied across BSM 480
 - applied to specific contexts 519
- RTSM context
 - permissions 531
- RUM
 - administrator role 518
 - Location Manager 339
 - viewer role 518
- S**
- SAML
 - configuring 623
- Section 508 compliance 58
- security officer 450
 - delete status in JMX 470
 - remove in JMX 470
- sensitive data
 - security officer 450
- server deployment 84
- server deployment interface 90
- service health context
 - permissions 545
- service level management context
 - permissions 546
- services
 - viewing status of 25
- shortcut menus
 - Content Packs Manager 397
- Single Sign-On
 - Identity Management 645
- single sign-on
 - lightweight 635
 - setting up 614
- SMS
 - message character set 703
- SMS provider
 - custom for alerts 477, 579
- SMS tab 594
- Start Menu in Windows 27
- starting and stopping BSM 24
- superuser
 - permissions 480
- system availability management context
 - permissions 547
- System Health
 - access 162
 - adding monitors to 161
 - Backup Server Setup Window 283
 - component status 249, 263
 - components 178
 - concepts 147
 - Dashboard customization 276
 - deploy 162
 - deploy secured environment 170
 - displays 151
 - Gateway machines 251
 - Icons 264
 - information buttons 280
 - introduction 148
 - limitations 287
 - log manager 254
 - monitor status 249
 - monitors table 158
 - Process Manager 284
 - processes 179, 267
 - processing machines 252
 - Quick Report 286
 - server components 267
 - Service Manager 281
 - service reassignment
 - understanding 159
 - synchronization 280
 - system and components 262
 - toolbar buttons 276
 - troubleshooting 287
- System Health Dashboard 257
 - general table 260
 - inventory tab 250
 - left pane 257
 - monitors table 258
 - right pane 258
- System Health monitors 181
 - alerts engine 216
 - application engines/CDM 226
 - application engines/reports DB
 - Aggregator 224
 - application engines/Service Health
 - engine 220
 - application engines/SLM engine 222
 - BPI server 239

Index

- BPM 244
- Bus 217
- Dashboard 208, 211
- data collectors 243
- Data In / Web Data Entry 196
- Data In/Analytics Loader 201
- Data In/Loader 198
- Data In/Operations Management 205
- Data Processing Server 215
- database components 266
- Database Services/Partition Manager 219
- databases 183
- Discovery Probe 247
- Gateway Server 195
- general 185
- KPI Enrichment Service 231
- machine hardware 182
- Modeling/RTSM 190, 226
- Modeling/viewing system 194, 230
- Operations Management 233
- Portal 214
- processes 186
- Rapid Anomaly Detection Engine 237
- RUM Data Collector 248
- SiteScope 246
- System Availability Management 215
- Verticals 214
- System Health Setup Wizard 269
 - accessing 151
 - overview 150
- Recipients Setup Dialog Box 275
- Remote Databases Setup Page 273
- Remote Servers Setup Page 271
- status 270
- system modifier role 492
- system requirements
 - flash player 61
 - Java 61
 - viewing HP Business Service Management 61
- system viewer role 498

T

- template
 - alert notification 714
- temporary image files, modifying settings for 131
- time zone setting 608
- tools
 - Data Marking 110
 - data marking 112
- troubleshooting
 - content packs 403
 - downtime 431
 - IDM-SSO 649
 - login failure 47
 - platform administration 729
- Troubleshooting and Knowledge Base 19

U

- user interface
 - Content Packs Manager 366, 386
 - enhancements 58
 - Location Manager 348
 - multilingual support 308
 - navigating 53
 - user management 553
- user management
 - assign permissions 466
 - configuration scenario 456
 - configuring groups 570
 - configuring users 570
 - customization 453, 555
 - customize users scenario 473, 604
 - customizing user menus 453
 - group mappings page 573
 - hierarchy 451, 468
 - main page 569
 - operations 525
 - permissions 445
 - permissions tab 563
 - roles applied across BSM 480
 - roles applied to specific contexts 519
 - user interface 553
 - workflow 454, 579

- user management roles
 - administrator 481
 - BPM administrator 517
 - BPM viewer 516
 - customer administrator (HP Software-as-a-Service) 509
 - RUM administrator 518
 - RUM viewer 518
 - superuser 480
 - system modifier 492
 - system viewer 498
- user mode
 - personal settings 608
- user permissions
 - resources 446
- user schema properties 118
- user-defined reports context
 - permissions 551

V

- viewing
 - status of services 25

W

- Windows
 - Start Menu 27
- wizard
 - Create New Content Pack Definition 392
 - downtime 421

X

- XML
 - attribute table 361
 - elements table 359
 - example file 342
 - file 341
 - tag reference 359

