HP Business Service Management

For the Windows, Linux operating systems

Software Version: 9.22

BSM Platform Administration Guide

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 Notice

© Copyright 2005-2013 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 (www.apache.org).

This product includes software developed by the JDOM Project (www.jdom.org).

This product includes software developed by the MX4J project (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.

PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format.

This document was last updated: Monday, April 08, 2013

Support

Visit the HP Software Support Online 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

Contents

Platform Administration Overview

This guide provides instructions on how to open, configure, and administer HP Business Service Management (BSM).

The guide is divided into the following parts:

- **Accessing and Navigating BSM**. Describes how to start BSM, how to log into the application, and a general overview of the user interface.

- **Setup and Maintenance.** Describes basic setup options such as infrastructure settings, time zones, languages, logs, and backups.

- **Data Enrichment.** This part has the following sections:

  - **Location Manager.** Describes how to work with multiple geographic locations.

  - **Content Packs.** Describes how to define objects or CIs included in content packs monitored by BSM.

  - **Downtime Management.** Describes how to control system downtime.

- **Users, Permissions, and Recipients.** Describes how to control user access to BSM.

- **Reports and Alerts Administration.** Describes how to schedule reports and set up alerts.

- **Troubleshooting.** Discusses common system issues or limitations.

Part 1

Accessing and Navigating BSM

Chapter 1

BSM Administration

This section discusses how to start BSM, view the status of processes and services, and the options in the Windows Start menu.

Starting, Stopping, and Restarting 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, stop, or restart BSM in Linux:

- `/opt/HP/BSM/scripts/run_hpbsm <start | stop | restart>`

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.

Viewing the Status of Processes and Services

You can view the status of the processes and services run by the BSM service and High Availability Controller on the BSM server status page.

To view the status of the processes and services in Windows:

- Select **Start > Programs > HP Business Service Management > Administration > HP Business Service Management Status**.

To view the status of the processes and services in Linux:

- `opt/HP/BSM/tools/bsmstatus/bsmstatus.sh`

To view the status of the processes and services in from a remote computer:

- In a web browser enter the following URL:
  `http://<server-name>:8080/myStatus/myStatus.html`

  Limitations:

  - This page is available remotely only after the JBoss application server is up.

  - If **JMX-RMI with basic authentication over SSL** was setup using the **SYSTEM** user, this page does not display any data. For details, see Securing JMX-RMI Channel Used for Internal BSM Communications in the BSM Hardening Guide.

Windows Start Menu

In a Windows environment, the installation process adds an HP Business Service Management menu to the Windows Start Menu.

To access the HP Business Service Management menu:

- Select **Start > Programs > HP Business Service Management**.

This menu includes the following options:

Option	Description
Open HP Business Service Management	Opens the BSM application Login page in a web browser.
Administration > Configure HP Business Service Management	Runs the Setup and Database Configuration utility. This 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 BSM Installation Guide.
Administration > Disable HP Business Service Management	Stops BSM on the specific machine, and disables it from running automatically when the machine is started.
Administration > Enable HP Business Service Management	Starts BSM on the specific machine, and sets it to run automatically when the machine is started.
Administration > HP Business Service Management Status	Opens the BSM Status page in a web browser. This page displays the status of the services run by the BSM Service and High Availability Controller. For details, see Post-Deployment in the BSM Installation Guide.
Documentation > HP Business Service Management Help	Opens the BSM Help file in a web browser.

Chapter 2

Logging into BSM

You can 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 more information, see "Permissions" on page 220.

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 25.

For details on browser requirements, as well as minimum requirements to successfully view BSM, see the BSM System Requirements and Support Matrixes.

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

BSM Login Page

This page enables you to log into BSM.

To access	In a browser, enter the following URL: **http://<server_name>.<domain_name>/<HPBSM root directory>** where **<server_name>** and **<domain_name>** represent the Fully Qualified Domain Name (FQDN) of the BSM server. If there are multiple servers, or if BSM is deployed in a distributed architecture, specify the load balancer or Gateway Server URL, as required.
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.
See also	• "Logging into BSM with LW-SSO" on page 25 • "Troubleshooting and Limitations" on page 28 • For details on accessing BSM securely, see the BSM Hardening Guide.

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 this option to bypass the Login page the next time that you open BSM. For further information, see "Enable Automatic Login in the Login Page" on the next page.

After you have logged on, the login name appears at the top right of the page, under the top menu bar.

Logging in for the First Time

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 changing the user password, see "Creating Users" on page 232.

• The login name cannot be changed.

For details on creating users in the BSM system, see "Create Users" on page 227.

To Log Out of BSM

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

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 will open and the user will need to enter a login name and password. This can be useful if another user needs to log in on the same machine using a different user name and password.

Advanced Login Options

Advanced login options enable you to automate login, modify automatic login settings, and create an automatic login URL.

Enable Automatic Login in the Login Page

Automatic Login means that when users open BSM, the Login page does not open and they do not have to enter their user name or password to access BSM.

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

1. On the BSM Login page, select **Remember my login name and password for 14 days**.

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.

Modify Automatic Login Settings

You can 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 modify the following options:

Option	Does the following
Days to remember login	Sets the number of days that users can login automatically without entering a user name and password. The default value is **14**.
Enable automatic login	If this option is set to **false**, users cannot bypass the Login page and will always require a user name and password when opening BSM. The default value is **true**.
Maximum machines per login name	Sets the number of machines that can simultaneously access BSM using the same login name. The default value is **0**; a value of **0** means that the number of logins is unlimited.

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. This is a convenient way to create a bookmark to BSM or to send a direct link to other users.

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

In a browser, enter the following URL:

http://<server_name>.<domain_name>/<HPBSM_root_directory>/TopazSiteServlet? autologin=yes&strategyName=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 **<password>** represent the login name and password of a user defined in BSM.

You can also create a URL to access BSM using the Link to This Page window. For further information, see "Link to This Page Window" on the next page.

How to Track Login Attempts and Logged In Users

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

- Open the following file:
  <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 "JMX Console" on page 102.)

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

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

Link to This Page Window

This window enables you to guide another user to a specific target page in BSM.

Note: By default only administrators have security rights to access this feature.

To access	Select **Admin > Link to this page**.
Relevant tasks	"Advanced Login Options" on page 20
See also	"Generate a Direct Link User Interface" in the Modeling Guide.

User Interface Elements

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. This button is only available after you click **Create Link**. **Note:** If you use the Firefox browser, you must change your security settings for this option to work. Enter `about:config` in the browser's search window, locate the **signed.applets.codebase_principal_support** option, and set it to **true**.
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.
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.

UI Element (A-Z)	Description
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 receivers need to use their own login name and password to access the page specified in the link.
Password	The password to be encrypted in the URL that 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.

Additional Information

Depending on how you use the **Link to this page** option, the receiver accesses the page using one of the following:

- Their 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.

> **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 use this URL, they are sent to the Setup and Maintenance page but will be 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 and there is no 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 Set Up the MyBSM Workspace in the BSM User Guide.

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 the Modeling Guide.

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.

- Receivers have all privileges of the user name they were given in the URL.

Logging into BSM with LW-SSO

Lightweight Single Sign-On (LW-SSO) Authentication Support allows users to log into BSM automatically and securely without needing to enter a user name and password.

When 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 Management Wizard.** For details, see "Authentication Wizard" on page 327.

- **The JMX console.**

When 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**).

How to Secure User Access to BSM Using Client-Side Authentication Certificates

You can secure user access to BSM using client-side authentication certificates. This provides a secure alternative to entering a user name and password to log on.

Configure LW-SSO using the JMX console to accept such certificates. When a certificate is accepted, users are automatically logged into BSM.

> **Note:** Before configuring LW-SSO, the BSM font-end server, such as reverse proxy or web server, needs to be configured to require a client certificate. For details about configuring Apache, see "Configuring Apache to Require a Client Certificate" in the BSM Hardening Guide. The Hardening Guide can be found on the Planning and Deployment Documentation page.

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 (for example: **EMAILADDRESS** in **SubjectDN**). You can view available attributes in the client certificate details, **Subject** or **SubjectAlternativeName** fields.

2. In a browser, enter the URL of the JMX console;
   http://<Gateway or Data Processing Server name>:8080/jmx-console/

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**, you must specify the attribute **ClientCertificateUserIdentifierRetrieveFieldPart**. Otherwise, this value may be left empty.

9. Click **Apply Changes**.

10. In BSM, 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**.

12. Confirm that you can log on to BSM with the client certificate and that the BSM Login page does not appear.

> **Note:**
>
> If the BSM Login page appears after entering a valid client certificate, test the following:
>
> - Try to log on using the User Identifier (often email address) as specified in step 8. If you can log on, make sure that the LDAP user filter was configured to use the same user identifier.
>
> - If the Login page still appears and you are using Apache web server, make sure the following line was added to **httpd-ssl.conf**: **SSLOptions +ExportCertData**.
>
>   For details, see "Configuring Apache to Require a Client Certificate" in the BSM Hardening Guide. The Hardening Guide can be found on the Planning and Deployment Documentation page.

How to Secure User Access to BSM Using an External Authentication Point

LW-SSO 2.4 enables you to use an external authentication point. This allows you to use your own credential validation method, for example LDAP, a proprietary user/password database, or a custom SSO solution.

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. The authentication assertion usually also provides information about how the user was authenticated.

To use an external authentication solution with LW-SSO 2.4:

1. If you are using LDAP, ensure that the same user repository is being used by BSM and the authentication point server.
   If you are 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 Gateway server, use the JMX Console to:

   a. Specify the **AuthenticationPointServer** URL.

   b. Set **validationPoint enabled** to **true**.

   c. Click **Apply Changes**.

   d. Restart the BSM Gateway server.

4. Make sure that 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 342.

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.

Troubleshooting and Limitations

This section describes troubleshooting and limitations for logging into BSM.

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	BSM failed to connect to the JBoss application server running on the Gateway Server. This may be due to: • the JBoss server being down • problems with the BSM service • The port required by the application server being used by another application	**Solution 1:** Close all applications on the Gateway Server machine and restart the machine. **Solution 2:** Ensure that there are no other running applications on the Gateway Server machine that use this port (for example, applications that run from the Startup directory, another instance of JBoss, an MSDE or Microsoft SQL Server, or any other process).
LI002	The JBoss application server running on the Gateway Server is not responding or is not installed correctly.	Restart BSM.
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.	Ensure that none of the JBoss ports are in use by another process. Also, ensure that the RMI ports are bound. For details on ports, see "Port Usage" on page 121.

Error No.	Problem/Possible Cause(s)	Solution(s)
LI005	The BSM login fails or hangs. This may be due to: • An incorrect login name/password combination • Inability to connect to the management database • Current user does not have access rights to any profile • Authentication strategy has not been set/configured correctly	**Solution 1:** Ensure that you or the user enters a correct login name/password combination. **Solution 2:** Ensure that the connection to the management database is healthy: 1. In a browser, enter the following to connect to the JMX Management Console: **http://<Gateway or Data Processing Server name>:8080/jmx-console/index.html** 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. **Solution 3:** Ensure that the user has appropriate permissions to access BSM. For details on user permissions, see "Permissions" on page 220. **Solution 4:** Verify that an authentication strategy has been configured correctly. For details on authentication strategies, see "Authentication Strategies" on page 320.

Error No.	Problem/Possible Cause(s)	Solution(s)

LI006	The BSM login fails. This may be due to:
	
	• Incorrect cookie settings in the web browser
	
	• An unsupported character in the names of the machines running the BSM servers
		Solution 1: Ensure that the client browser is set to accept cookies from BSM servers.
		
		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:
		`http://111.222.33.44/<BSM root directory>`
		instead of
		`http://my_server/<BSM root directory>`

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.	**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. **Solution 2:** Log in using a different login name, if available. **Solution 3:** The administrator can edit the Infrastructure Settings to remove the limitation or increase the maximum number of concurrent logins using the same login name from different machines. For details, see "Advanced Login Options" on page 20.

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. Because 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 **\<BSM 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.

Chapter 3

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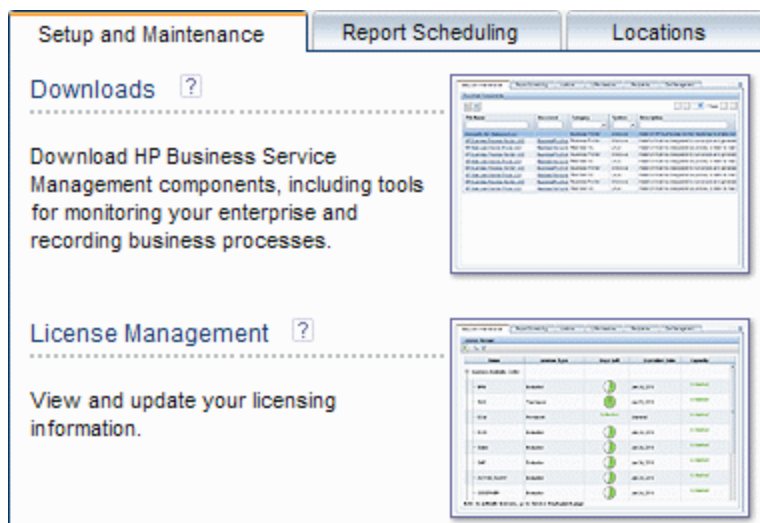
- **Tab controls.** Assist in navigation from any context related to a tab to any other of the tab's contexts. To open the tab main menu, click the tab name.

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.
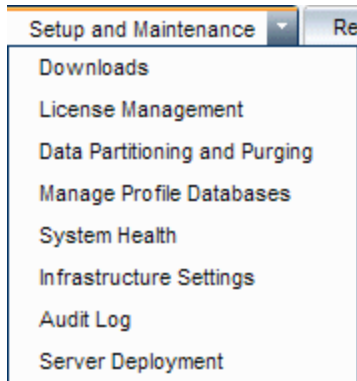
- **Navigation buttons.**

  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 drop-down 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 20 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 20) 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
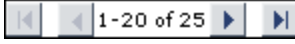
The BSM interface includes many features to enhance the user experience. These include:

- **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 ◁◁ ◁ 1-20 of 25 ▷ ▷▷ to move to a table's first, previous, next, or last page.

  - **Exporting.** Click the appropriate button to export a table to another format, such as Excel ⧉, PDF ⧉, or CSV ⧉.

  For details about table functionality in reports, see Common Report and Page Elements.

  > **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 the next page.

- **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**.

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.

Client Requirements for Viewing BSM

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

Display	**Minimum:** color palette setting of at least 256 colors **Recommended:** color palette setting of 32,000 colors
Resolution	• 1280x1024 or higher (supported) • 1400x1200 or higher (recommended)
Supported Browsers	• Microsoft Internet Explorer (IE) 9.0 • Microsoft Internet Explorer (IE) 8.0 • Microsoft Internet Explorer (IE) 7.0 • Mozilla Firefox ESR 10 or ESR17.0 **Note:** • The browser must be set to accept all cookies. • The browser must be set to enable JavaScript execution. • The browser must support for pop-up windows. HP Business Service Management will not perform properly if you use Web applications that are set to block pop-up windows in your browser. • Internet Explorer users must set browser caching to automatically check for newer versions of stored pages.
Flash Player	Adobe Flash 10.1 or later
Fonts	The following fonts must be installed on client systems: • MS Gothic for Japanese locales • Gulim for Korean locales • SimSun for simplified Chinese locales • Arial for all other locales

Java Plug-in (to view applets)	**Recommended:** Version 6 update 31
	Supported: Version 6 update 26 and higher, or version 7
	Note: You may not be able to view all HP Business Service Management applets with an earlier version of Java and you will need to download the latest version from the Java download site (http://www.java.com/en/download/manual.jsp) and install it. You may also have to disable earlier versions after download.
	To do this in Internet Explorer: Select **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.
	For details about how to verify the Java version in Mozilla Firefox, see the Mozilla Firefox documentation.
Viewing the BSM Help file	The BSM Help file is best viewed in Internet Explorer.
	The Help file 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 Help file automatically opens using the JavaScript implementation. The JavaScript implementation provides the same basic functionality as the Java implementation, but does not allow use of the Favorites tab within the navigation pane.
	If you experience a JavaScript error when opening the Help file, 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:

MyBSM

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

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 Service Health Overview in the BSM User Guide.
CI Status	Opens the CI Status Reports interface. For details, see CI Status Reports User Interface in the BSM User Guide.
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 Service Level Management Application Overview in the BSM User Guide.
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 End User Management Reports Overview in the BSM User Guide.
Transaction Management	Displays transaction topology and infrastructure for data collection and report viewing. For details, see Introducing Transaction Management Reports and Topologies in the BSM User Guide.
System Availability Management	Opens the System Availability Management application, used for complete system and infrastructure monitoring as well as event management. For details, see Using System Availability Management Overview in the BSM User Guide.
User Reports	Opens the Report Manager, used for creating and saving user reports—customized reports containing user-defined data and formatting that can help you focus on specific aspects of your organization's application and infrastructure resource performance. For details on the Report Manager, see Reports Overview in the BSM User Guide.
Application Management for SOA	Opens Application Management for SOA reports.

Admin

Administrators use the **Admin** menu to administer the BSM platform and applications. The Admin menu consists of several sections, organized by function.

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 Introduction to Service Health Administration in the BSM Application Administration Guide.
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 Service Level Management Administration Overview in the BSM Application Administration Guide.
Operations Management	Opens the Operations Management Administration pages. For details, see Setup in the BSM Application Administration Guide.
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 End User Management Administration in the BSM Application Administration Guide.
System Availability Management	Opens the System Availability Management Administration pages, where you configure and administer the SiteScope data collector. For details, see System Availability Management Administration Overview in the BSM Application Administration Guide.
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 the Modeling Guide.
Platform	Opens the Platform Administration pages, which provide complete platform administration and configuration functionality. .

Menu Option	Description
Integrations	Opens the BSM Integrations administration area, where you can administer the following: • BSM Connector integrations to capture and forward data from third-party systems to BSM. • Mappings between CIs and Operations Orchestration runbooks. • Application Lifecycle Management integrations to export related data and monitoring tools configurations. • Deprecated integration methods - Integrations Adapter and EMS Integrations. For details, see Integrating with Other Applications - Overview in the BSM Application Administration Guide.
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 22. **Note:** By default only administrators have security rights to access this feature.
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 313.

Help Menu

You access the following online resources from the BSM Help menu:

Menu Option	Description
Help on this page	Opens the BSM Help file to the topic that describes the current page or context.
BSM Help	Opens the BSM Help home page. The home page provides quick links to the main help topics.
Planning and Deployment Guides	Opens a page with links to planning guides, installation and upgrade guides (including release notes), data collector installation guides, and other resources.
Product News and Updates	Opens the Product News page on the HP Software Support website (requires HP Passport login). The URL for this Web site is http://support.openview.hp.com/product_news.jsp.

Menu Option	Description
Troubleshooting & Knowledge Base	Opens the troubleshooting page on the HP Software Support website (requires HP Passport login). The URL for this Web site is http://support.openview.hp.com/troubleshooting.jsp.
HP Software Support	Opens the HP Software Support website. This site enables you to browse the knowledge base and add your own articles, post to and search user discussion forums, submit support requests, download patches and updated documentation, and more. The URL for this Web site is http://support.openview.hp.com/.
HP Software Web Site	Opens the HP Software website, which contains information and resources about HP Software products and services. The URL for this Web site is http://www.hp.com/go/software.
Movies	Opens the Movies panel with links to instructional movies about how to use BSM.
Site Map	Opens the site map, with links to all top-level contexts in the Applications menu or the Administration Console. Note: The Site Map is the default entry page when you log into 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 313.
What's New?	Opens the What's New document, which describes the new features and enhancements in this version.
BAC Anywhere	Opens BAC Anywhere. For further information, see HP BAC Anywhere Overview.
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 2

Setup and Maintenance

Chapter 4

Downloads

After 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 BSM Installation Guide.

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.

UI Components

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	• 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.

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.
/240 Pages	Divides the table of data into pages. You move from page to page by clicking the relevant button: • To view more reports, click **Next page** or **Last page**. • To view previous reports in the list, click **Previous page** or **First page**.

UI Element (A-Z)	Description
Category	The downloadable component's category. Available categories are: • **Business Process Insight.** Downloadable files that enable you to install and run Business Process Insight components on 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.
Description	An explanation of the specific downloadable file.
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.

Chapter 5

License Management

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) 15 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 specific information on the Operations Manager i (OMi) licensing structure, see Licensing in the BSM User Guide.

To access

To open the License Management Page, select **Admin > Platform > Setup and Maintenance > License Management**.

To review the status of your license, select **Admin > Platform > License Management**.

Tasks

Add a new license

To update your deployment with a new license:

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

2. 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.

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

UI Description

License Management Page

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.
License Type	There are three types of licenses: ● **Evaluation:** A license with a fixed trial period of up to 60 days. This type of license is available only until a Time Based or Permanent license is purchased. Once purchased, the trial period immediately terminates. **Note:** An Evaluation License cannot be renewed. ● **Time Based:** A license which has a time-based expiration date. ● **Permanent:** A license which does not expire.
Days Left	Displays the number of days that the license may continue to be used. When green, expiry time is pending; when red, the license is expired.
Expiration Date	Displays the license's fixed expiration date. This date is displayed only for time-based licenses.
Capacity	If the license is capacity based, the amount of capacity available and the amount of capacity used will be expressed by means of a status bar. **Available when:** This feature is available when the license is capacity based. If the license is not capacity based, the words Not Applicable will appear in the capacity column.
Capacity Details	If the license is capacity based, the amount of capacity available and the amount of capacity used will be expressed by means of a ratio. **Available when:** This feature is available when the license is capacity based. If the license is not capacity based, the words Not Applicable appear in the capacity column.
Server Deployment Link	When you add a license to BSM, you must enable the application in the Server Deployment page. This includes a check to see whether the physical resources of your deployment can handle the added application. For details, see "Server Deployment" on page 52.

Tips/Troubleshooting

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 Server Deployment page, available by clicking the **Server Deployment** link at the bottom of the License Management pane, or by running the BSM Setup and Database Configuration Utility. For details, see "Server Deployment and Setting Database Parameters" in the BSM Installation Guide.

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

Chapter 6

Server Deployment

This section provides information about how to determine and configure the optimal BSM server deployment.

To access

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

Learn More

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.

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.

2. ### Add a new license — optional

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

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

   b. 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.

   c. 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.

4. ### Restart BSM

   After you click **Save** in the Server Deployment page, you need to restart BSM. For details, see

5. ## Results

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

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

UI Description

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. After you save the changes to this page, BSM must be restarted for the changes to take effect.

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

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

UI Element	Description

<Capacity table>	The upper table in the page displays the current information regarding deployment and applications. If you upload a capacity calculator file, this table is automatically updated with the information in the capacity calculator.
	
	You can change capacity level of your deployment for:
	
	● **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.
	
	You can also enable/disable applications and features, and change their capacity levels.
	
	● **End User Management**
	
	● **TransactionVision**
	
	● **Diagnostics**
	
	● **Business Process Insight**
	
	● **OMi:**
	
	    ■ **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**
	
	● **Service Health Analyzer**
	
	● **Baselining**
	
	After you click **Save** and restart BSM:
	
	● 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>	The lower table lists all the servers running BSM including: **Status**. Whether the machine is up and running. **Aligned**. Whether this machine is aligned with the current deployment configuration. It would be aligned only if BSM was restarted on this machine after any changes were made. If BSM was not yet restarted on this machine since any configuration changes were made in this page, the machine is not aligned. **Machine**. The name of the server. **Installed**. Which type of BSM server is installed on the machine, Gateway or Processing or both (Typical installation when Gateway and Data Processing are on the same machine). **Activated**. Which type of BSM server is currently activated on the machine, Gateway or DPS (data processing server). **Detected**. The free memory detected on the machine. **Required**. The required memory for each type of server based on the applications and capacity levels listed in the upper table. If the Required memory is higher than the memory in the Detected column, you must either: - Change capacity levels for your deployment, for example: clear applications from the list of available applications. - Add memory to the physical machines and try to update your deployment again.
To disable machine	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. Before disabling a machine, verify that it is no longer an operational part of the BSM server architecture. To re-enable a machine after disabling it here, you need to run the Setup and Database Configuration Utility on that machine.

Troubleshooting and Limitations

Troubleshooting

- 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.

Chapter 7

Database Administration

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

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 65.

- **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 66.

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

  - 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 BSM Database Guide. It is recommended that you review the relevant portions of the BSM Database Guide 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

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

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

The data collection tables in the profile and SHP 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 SHP database and handles partitioning and later purging of historical data according to the time period listed for the database table. The size of each partition is determined by the EPM (events per minute) value displayed on the Purging Manager page. The default EPM values are preset according to the appropriate level of the specified database table. Optionally, you may want to adjust the EPM value, if necessary:

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

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

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

You can also use the Partition and Purging Manager to set a specific time period—per table—for removing historical data. For details on the user interface for performing this task, see "Purging Manager Page" on page 79.

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 the next page.

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.

  After 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 BSM Database Guide.

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.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

Note: 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 .

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.

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.

1. ## Prerequisites

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

   a. **Server name.** The name of the machine on which a Microsoft SQL server is installed. If you are connecting to a non-default Microsoft SQL server instance in dynamic mode, enter the server name in the following format:

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

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

   c. **Server port.** The Microsoft SQL server's TCP/IP port. The default port, `1433`, is automatically displayed. You must change the port number in one of the following instances:

      ○ The default Microsoft SQL server instance listens to a port other than `1433`.

      ○ You connect to a non-default Microsoft SQL server instance in static mode.

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

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

2. ## Add a Database

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

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

   c. Enter the parameters of your database on the **Profile Database Properties - MS SQL Server** page. For user interface details, see "Profile Database Properties — MS SQL Server Page" on page 76.

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.

1. ## Prerequisites

   Before you begin, make sure that:

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

   b. You are using a secure network connection if you do not want to submit database administrator connection parameters over a non-secure connection. If you do not want to submit database administrator connection parameters 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 BSM Database Guide). 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

If your Profile database is part of Oracle Real Application Cluster (RAC), see Support for Oracle Real Application Cluster in the BSM Database Guide.

How to Work with the Purging Manager

This task describes how to work with the Purging Manager.

This task includes the following topics:

- "Prerequisites" below

- "Change the Database Template" below

- "Change Settings for Multiple Databases" below

- "Change Settings for Individual Databases" on the next page

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 65.

    For details on configuring a user schema on an Oracle server, see "How to Configure a User Schema on an Oracle Server" on page 66.

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 64.

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 Generic Reporting Engine API in the BSM Extensibility Guide. 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.

Database Administration User Interface

This section includes:

- "Database Management Page" below
- "Data Marking Utility Page" below
- "Profile Database Properties — MS SQL Server Page" on page 76
- "Profile User Schema Properties — Oracle Server Page" on page 77
- "Purging Manager Page" on page 79

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	• 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	• "Removing Unwanted Data from the Profile Database" on page 64 • "Troubleshooting Data Marking Utility Errors" on page 83

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 (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 72.
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 the next page.
Locations	List of locations you can mark as obsolete.
Mark data as obsolete	Marks the filtered criteria (Applications, Business Transaction Flows, Transactions, Locations, or SiteScope Targets) as obsolete.
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.

UI Element (A-Z)	Description
SiteScope Targets	List of SiteScope target machines (machines being monitored by SiteScope) that you can mark as obsolete. **Note:** This field is visible only in the SiteScope view (if you chose **SiteScope View** in the **View by** dropdown list).
Start	Activates the Data Marking utility and marks data as obsolete.
Start Time	Select a starting date 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 (if you chose **Applications** in the **View by** dropdown list).
View by	Select the type of view to be visible in the Data Marking utility: • 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 Recalculation for SLAsin the BSM Application Administration Guide.
See also	• "Removing Unwanted Data from the Profile Database" on page 64 • "Data Marking Utility Limitations" on page 83

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.

Profile Database Properties — MS SQL Server Page

This page enables you to configure a new or existing profile database on Microsoft SQL server.

To access	Select **Admin> Platform > Setup and Maintenance > Manage Profile Databases**, select **Microsoft SQL** from the dropdown database list and click **Add**.
Important information	• It is recommended that you configure Microsoft SQL server databases manually, and then connect to them in the Database Management page. For details on manually configuring Microsoft SQL server databases, see "Overview of Microsoft SQL server Deployment" in the BSM Database Guide. • Database creation can take several minutes.
Relevant tasks	"How to Configure a Profile Database on a Microsoft SQL Server" on page 65
See also	"Database Administration" on page 60

User interface elements are described below:

UI Element (A-Z)	Description
Create database and/or tables	Select or clear as required. • To create a new database, or connect to an existing, empty database and populate it with profile tables, select the check box. • To connect to an existing database already populated with profile tables, clear the check box.
Database name	• If you are configuring a new database, type a descriptive name for the database. • If you are connecting to a database that was previously created, type the name of the existing database.
Disconnect	Disconnects the database from BSM. **Note:** This button appears only after you have clicked the **Disconnect Database** ❌ button on the Database Management page.
Make this my default profile database (required for custom data types)	Select or clear as required. **Note:** • This setting is required if you are collecting Service Health, Real User Monitor, HP Diagnostics (if installed), Service Level Management, SOA, or persistent custom data. • Selecting this check box overwrites the existing default profile database.

UI Element (A-Z)	Description
Password	• 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	Enter the port number if: • The Microsoft SQL server's TCP/IP port is configured to work on a port different from the default (1433). • You use a non-default port in static mode. • You use a non-default port in dynamic mode. In this case, enter port **1434**.
Server name	Enter the name of the machine on which the Microsoft SQL server is installed. If you are using a non-default instance in dynamic mode, enter the server name in the following format: `<my_server\my_instance>`
SQL server authentication	Select if the Microsoft SQL server is using SQL server authentication.
User name	• Should remain empty if you are using Windows authentication. • If you are using SQL server authentication, enter the user name of a user with administrative rights on Microsoft SQL server.
Windows authentication	Select if the Microsoft SQL server is using Windows authentication.

Profile User Schema Properties — Oracle Server Page

This page enables you to configure one or more profile user schemas on your Oracle server.

To access	Select **Admin > Platform > Setup and Maintenance > Manage Profile Databases**, select **Oracle** from the dropdown database list and click **Add**.
Important information	• It is recommended that you configure Oracle server user schemas manually, and then connect to them in the Database Management page. For details on manually configuring Oracle server user schemas, see Overview of Oracle Server Deployment in the BSM Database Guide. • 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 66
See also	"Database Administration" on page 60

User interface elements are described below:

UI Element (A-Z)	Description
Create database and/or tables	Select or clear as required. • To create a new user schema, or connect to an existing, empty user schema and populate it with profile tables, select the check box. • To connect to an existing user schema already populated with profile tables, clear the check box. **Note:** Clearing this check box disables the database administrator connection parameter and tablespace fields on the page, and instructs the platform to ignore the information in these fields when connecting to the Oracle server machine.
Database administrator password	Enter the password of a user with administrative permissions on Oracle server. **Note:** This field is enabled only if you selected the **Create database and/or tables** check box.
Database administrator user name	Enter the user name and password of a user with administrative permissions on Oracle server. **Note:** This field is enabled only if you selected the **Create database and/or tables** check box.
Default tablespace	Enter the name of the default tablespace designated for use with profile user schemas. **Default Value:** users
Disconnect	Disconnects the user schema from BSM. **Note:** This button appears only after you have clicked the **Disconnect Database** ✖ button on the Database Management page.
Host name	Enter the name of the machine on which the Oracle server is installed.

UI Element (A-Z)	Description
Make this my default profile database (required for custom data types)	Select or clear as required. **Note:** • This setting is required if you are collecting Service Health, Real User Monitor, HP Diagnostics (if installed), Service Level Management, SOA, or persistent custom data. • Selecting this check box overwrites the existing default profile database.
Port	Enter the required Oracle listener port, or accept the default value.
Retype password	Retype the user schema password.
SID	Enter the required Oracle instance name, or accept the default value.
Temporary tablespace	Enter the name of the temporary tablespace designated for use with profile user schemas. **Default Value:** temp
TNS name	Enter the TNS name of the Oracle Client, as specified in the tnsnames.ora file on the Gateway Server machine, located in the **<ORACLE_HOME>\network\admin** directory.
User schema name	• If you are configuring a new user schema, enter a descriptive name for the user schema. • If you are connecting to a user schema that was previously created, enter the name of the existing user schema.
User schema password	• If you are configuring a new user schema, enter a password that enables access to the user schema. • If you are connecting to a user schema that was previously created, enter the password of the existing user schema. **Note:** You must specify a unique user schema name for each user schema you create for BSM on the Oracle server.

If your Profile database is part of Oracle Real Application Cluster (RAC), see Support for Oracle Real Application Cluster in the BSM Database Guide.

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 BSM Database Guide.
See also	"Partitioning and Purging Historical Data from Databases" on page 62

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 71.
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.
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 71.
Keep Data for	The time range for keeping data in the database tables whose check box is selected. This element appears as follows: ● **Selection fields.** At the top of the page, set the time period for how long you want data kept in the selected database tables. ● **Column heading.** Displays the time range for keeping data in each database table. This value is configured in the **Keep Data for** selection fields at the top of the page. **Note:** The time period configured in the **Keep Data for** fields indicates that the data is stored for at least the specified amount of time; it does not indicate when the data is purged. By default, retention time is Infinite, meaning no purging is set.

UI Element (A-Z)	Description
Name of Table in Database	The name of the table in the database. Database tables are listed by the data collector from which the data was gathered. The following data types are available: ● Alerts ● BPI ● Business Logic Engine ● Business Process Monitor ● Diagnostics ● Real User Monitor ● SOA ● Service Level Management ● SiteScope ● TV ● UDX (custom data) ● WebTrace
Select a profile database	Select a profile database for which you want to modify time range configurations for purging data. **Note:** This field is visible only on the Database Specific tab.
Template and Multiple Databases	Select this tab to: ● Change the partitioning and purging parameters for multiple profile databases. ● Change the database template, for parameters to be adopted by new databases added in the future. **Note:** Once you have made changes, the settings displayed in the **Template & Multiple Databases** tab remain the template settings, even if you did not make changes to the template and have manually changed settings for specific databases. Once those manual changes are applied, the settings displayed revert to the template settings. To see the settings you changed for specific databases, navigate to the **Database-Specific** tab and select the appropriate database.

Loader Persistence Folders Structure

Each gateway server contains a folder named **persist_dir\db_loader** which contains the following sub-directories:

- **.persist_dir\db_loader\main\dlq** – contains samples that the system was not able to insert into the database, for example wrong sample, duplicated samples, or samples with time stamp older then data purging period.

  There is no size limit and no limit of the number of samples in this folder, old files are not automatically purged. If these samples were added to this folder due to an error, for example there was a data flow problem, you can reinsert these samples into the database.

- **.persist_dir\db_loader\main\current** – samples that are currently in the loader memory. Size is limited by memory restrictions of the database loader.

- **.persist_dir\db_loader\flattenfailure** – hierarchy samples (**trans_t**) that temporarily failed to open because of a database connectivity problem. There is no size limit.

- **.persist_dir\db_loader\recovery** – samples that the system was temporary unable to insert. This is usually because of database availability issues. The limit for each sample type is five sub-folders, each can contain up to 509 (8192 samples in each file); approximately 20M of samples for each sample type. After this limit is exceeded, the loader stops working and will not read data from BUS.

Troubleshooting and Limitations

This section describes troubleshooting and limitations for database administration.

This section includes:

- "Troubleshooting Data Marking Utility Errors" below

- "Data Marking Utility Limitations" below

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.

Chapter 8

Infrastructure Settings

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 (Run-time 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 the next page.

Some infrastructure settings are configured outside the Infrastructure Settings Manager. For details, see "How to Modify the Ping Time Interval" on page 86, and "How to Modify the Location and Expiration of Temporary Image Files" on page 87.

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.

5. 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 "How to Modify the Directory in Which Temporary Image Files Are Stored" on the next page.

- **The configuration of a shared location for temporary image files**

  For details, see "How to Access Temp Directory with Multiple Gateway Server Machines" on page 89.

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

  For details, see "How to Modify the Length of Time that BSM Keeps Temporary Image Files" on page 92.

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

  For details, see "How to Specify the Directories from Which Temporary Image Files Are Removed" on page 95.

How to 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 Linux 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 "How to Access Temp Directory with Multiple Gateway Server Machines" on the next page.

How to 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 "How to Modify the Directory in Which Temporary Image Files Are Stored" on the previous page), 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 "How to Modify the Directory in Which Temporary Image Files Are Stored" on page 88). 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 as follows:

   a. Locate the line (note lower case "t" in topaz):

   ```
   Alias /topaz "C:\HPBSM/AppServer/webapps/site.war/"
   ```

   b. Above that line add the following line:

   ```
   Alias /topaz/Imgs/chartTemp/offline "<shared_temp_image_
   directory>"
   ```

   c. Locate the line (note upper case "T" in Topaz):

   ```
   Alias /Topaz "C:\HPBSM/AppServer/webapps/site.war/"
   ```

   d. Above that line add the following line:

   ```
   Alias /Topaz/Imgs/chartTemp/offline "<shared_temp_image_
   directory>"
   ```

3. Replace `<shared_temp_image_directory>` with the path to the physical directory containing the temporary scheduled report images, as defined in the **images.save.directory.offline** parameter (for details, see "How to Modify the Directory in

Which Temporary Image Files Are Stored" on page 88).

When specifying `<shared_temp_image_directory>` you must use double quotes and forward slashes, for example:

```
Alias /Topaz/Imgs/chartTemp/offline
"//myhost.myurl.com/chartTemp/offline"
```

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 "How to Modify the Directory in Which Temporary Image Files Are Stored" on page 88).

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.

How to 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 Linux 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.

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

- **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.

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

How to 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.

UI Description - 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	"Database Administration" on page 60

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

Chapter 9

Baselines

An application's status, which you can use in components such as Service Health, End User Management, Service Level Management, and Service Health Analyzer, is determined by its transactions' actual performance and availability in relation to configured performance and availability thresholds.

When you configure an application for monitoring by Business Process Monitor, you can determine whether its transactions' performance thresholds are static thresholds (specific threshold values that you configure), or are calculated using baselines based on historical transaction data.

Baselines are updated periodically as new metrics data are received.

> **Note:** A minimum amount of accumulated data is necessary before baselines can be calculated. This depends on the number of samples collected and takes approximately one week after baselines are enabled in BSM. You can speed up the process by manually invoking a baseline with limited data. For details, see "How to Manually Invoke a Baseline" on page 100.

Enabling Baselines

You can configure BSM to calculate baselines from actual performance metrics. Creating a baseline enables you to learn the normal performance of your applications. Knowing how an application typically performs enables you to determine whether a performance problem is an isolated incident or a sign of a trend.

To enable baselining in BSM:

1. Select the Baselining option in:

   - The **Setup and Database Configuration Utility** in a regular deployment (for details, see the BSM Installation Guide).

   - The **Upgrade Wizard** if you are performing an upgrade (see the Upgrade Guide relevant to your upgrade path).

2. Create an Analytics database (**Admin > Platform > Manage Analytics Databases**).

> **Note:** You can also enable baselining after BSM has been installed.

Baseline Coefficient

When baselining is enabled, BSM collects metric data from incoming samples over a period of time. After enough data has been collected, BSM creates a baseline for the metric and calculates the mean and standard deviation.

Mean and standard deviation values for a metric are used to create a baseline sleeve and to identify metrics that deviate from the baseline. The mean and standard deviation are a statistical way of

estimating the normal behavior of a metric. By default, the baseline sleeve is calculated using a coefficient of + or - 3 times the standard deviation from a metric's mean value.

This means that a metric is considered abnormal if its value is greater than the mean value plus 3 times the standard deviation, or less than the mean value minus 3 times the standard deviation.

This can be summarized as follows:
((Mean Value)-(3*STD)) <= NORMAL VALUE <= ((Mean Value)+(3*STD))

You can set a different coefficient for each data collector. For example you could set a coefficient of 2 for CIs received from BPM and a coefficient of 5 for CIs received from Diagnostics.

To set the coefficient for a data collector:

1. Select **Admin > Platform > Infrastructure Settings > Applications > Service Health Analyzer > Baseline Coefficient**.

2. Enter the required coefficient. Multiple values should be separated by a semi-colon, for example **BPM,2.0;SiS,2.5;DIAG,5.0;PA,3.5;RUM,2.0;NNM,4.0**.

> **Note:** If you do not set a coefficient for a data collector, BSM uses the default of 3.

Seasonality and Trends

When calculating a metric's baseline, the baseline engine takes into account such things as seasonality and trends.

- **Seasonality** - When a repeated pattern at constant time intervals occurs, a metric has seasonality. For example a metric might have typical values at 8:00 every day when users log on, and different values at 12:00 when users take a break.

- **Trends** - When a metric's values have a consistent linear change over time, a trend is identified.

Seasonality and trends are considered to be part of the normal behavior of a metric, and the baseline sleeve is adjusted accordingly.

Baseline Example

The following example shows the baseline sleeve for the OK, minor, and critical thresholds for a transaction in the Metrics Over Time report :
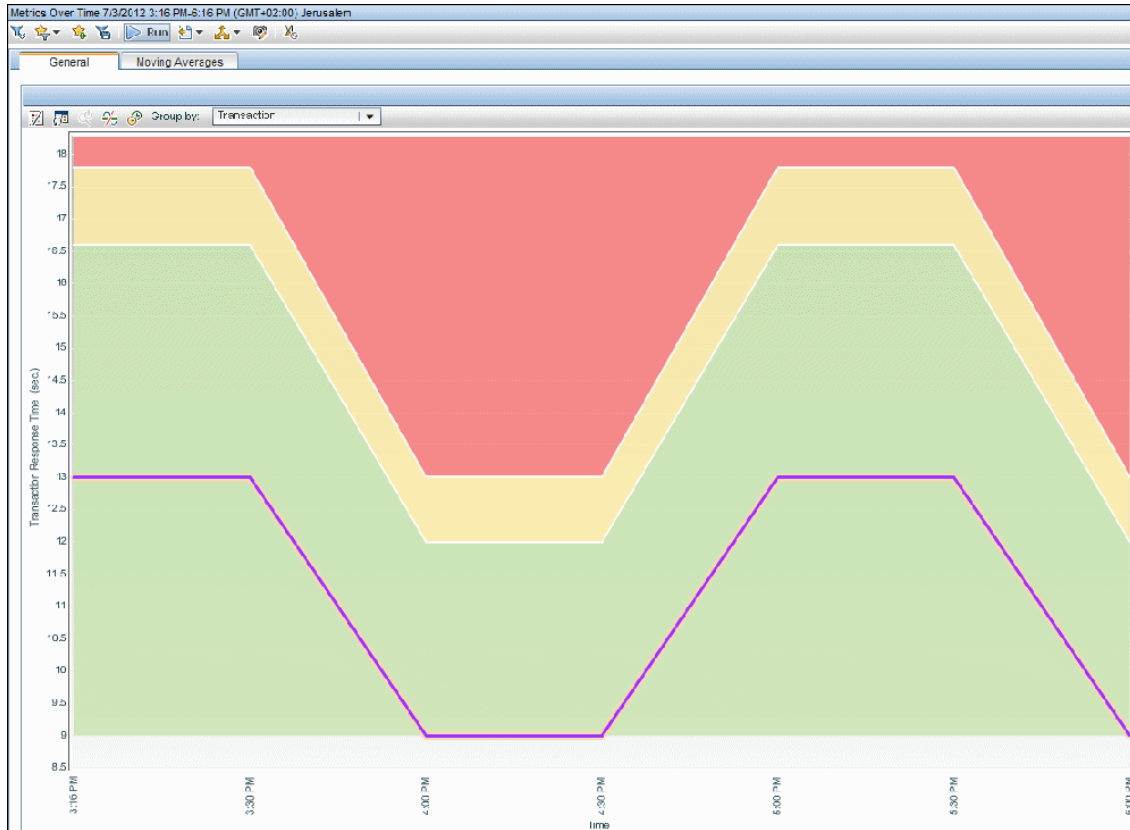
How to Manually Invoke a Baseline

When you initially install and configure BSM it takes a week for the system to gather CI data required to establish a baseline. You can speed up this process by manually creating a baseline using limited data from a single day after installing BSM. This means that 24 hours after installing and configuring BSM, the system can already identify anomalies.

If you manually create a baseline with less than a week's data, the baseline will not include any seasonal information such as different patterns over weekends, however over time BSM will automatically refine and improve the baseline as more data becomes available.

Note: You cannot manually create a baseline on the same day that you install BSM. This is because the baseline process required an off-line process which runs automatically every night.

To manually invoke a baseline:

1. In a web browser, open the baseline JMX page using the following link:
   http://<DPS>:29924/mbean?objectname=Topaz:service=Baseline+Services

2. Invoke the **showTasks** operation to identify the task IDs of your domain for example:

Task ID	Client	Metric Domain	Status	Start of period	End of period	Next run
33	1	RUM	idle	Sat Nov 29 00:00:00 IST 2011	Mon Dec 29 00:00:00 IST 2011	Mon Dec 29 00:01:00 IST 2011
34	1	BPM	idle	Sat Nov 29 00:00:00 IST 2011	Mon Dec 29 00:00:00 IST 2011	Mon Dec 29 00:01:00 IST 2011

3. Record the relevant task IDs and dates, and go back to the baseline JMX page (as listed above).

4. Invoke the **calculateNow** operation on each of the relevant task IDs.

5. To confirm that the process ran successfully, invoke the **showTasks** operation again and confirm that the dates have been updated. The process might take some time.

Troubleshooting and Limitations

This section describes troubleshooting and limitations with baselines.

JVM often crashes in baseline process while running baseline tasks

This problem is caused by the Java Virtual Machine. You can identify the problem with the following errors in the file **hs_err_pid.log**:

- EXCEPTION_ACCESS_VIOLATION

- guarantee(result == EXCEPTION_CONTINUE_EXECUTION) failed: Unexpected result from topLevelExceptionFilter

The log file is located in the working directory at the time of process execution.

To resolve this problem, change the baseline process from 64 bit to 32 bit as follows:

1. In the JMX Console, stop the service **basel_engine** as follows:

    a. In a browser enter **http://<Data Processing Server>:11021/** and enter your user name and password.

    b. Under **Foundations**, click **Foundations:type=NannyManager**.

    c. Under **java.lang.String showServiceInfoAsHTML**, click **Invoke**.

    d. Next to **basel_engine**, click **Stop**.

2. On the Data Processing Server, copy the file **\HPBSM\JRE\bin\hpbsm_basel_engine.exe** to the directory **\HPBSM\JRE64\bin**, overriding the existing file with the copy.

3. Restart the **basel_engine** service.

Chapter 10

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

The credentials to access the JMX console were configured when you installed BSM.

You can monitor the availability of your BSM system on the HP Business Service Management server status HTML page. For details, see "Viewing the Status of Processes and Services" on page 16.

You can configure the JMX console to work with SSL to encrypt JMX data for added security. For details, see "Configuring JBOSS to Work with SSL" in the BSM Hardening Guide.

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.

Chapter 11

Audit Log

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

To access

Select **Admin > Platform > Setup and Maintenance > Audit Log**

Learn More

About the Audit Log

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.

- **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.** Displays actions related to the Service Health application.

- **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.

- **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.

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**.

2. Select a context.

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** or **Next Page** arrows to navigate to the previous or 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.

> **Note:** Do not change the appender name:
> **com.mercury.topaz.tmc.bizobjects.audit.AuditManager.writeAudit**

UI Descriptions

Audit Log Page

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

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.
<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.
Context	Select a context to view.
For user	Displays the user whose actions are displayed in the Audit Log, as specified in the Auditing Filters pane. **Default Value:** All
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.

UI Element (A-Z)	Description
⊗	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.
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 Alerts Log Report in the BSM User Guide.

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.

Chapter 12

HP System Health

System Health is a standalone application that uses the SiteScope monitoring system to enable you to monitor the servers, databases, and data collectors running as part of your BSM system.

You can 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.

  - **Configure Backup Servers**. You can define a backup server in case the server machine is not functioning properly or requires downtime for servicing.

  - **Manage BSM Processes**. You can start or stop various BSM processes.

- 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).

You can access System Health through BSM or in a web browser.

For further information, see the System Health Guide.

Chapter 13

BSM Server Time Synchronization

In order to ensure that the BSM serve clocks are accurate and synchronized, the BSM servers check their system clocks against an NTP server every 20 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.

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://<BSM_Server>/topaz/services/technical/time?alt=text/plain

Example results:

```
1314089070858
```

To view the current time in XML format:

http://<BSM_Server>/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

Chapter 14

BSM Logs

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

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 115.

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" on page 118.

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:

Address	\\myserver\HPBAC\log			▾	🔗 Go
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	
Type: LOG File Size: 0 bytes		0 bytes		🖳 Local intranet	
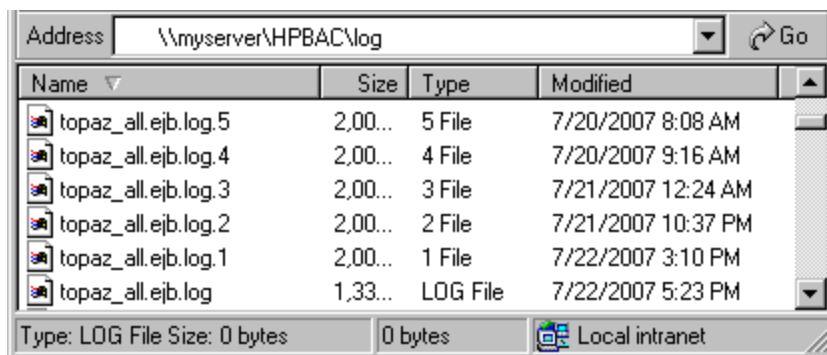
The maximum file size and the number of archived log files are defined in the log properties files located in **<HPBSM root directory>\conf\core\Tools\log4j**. An example is:

```
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`.

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.

How to Enable Debug Trace Logging for an Event

It is possible to enable debug trace logging for an event by setting the custom attribute `__TRACE_`
`_`. It may have any value. This creates flow trace logs at the `INFO` level for this event.

This can be set on the HPOM server or agent sending the event, or can later be added to the event. Whenever this custom attribute is set on an event, trace output for this event appears in the trace logs:

- BSM Data Processing Server: `log/opr-backend/opr-flowtrace-backend.log`

- BSM Gateway Server: `log/opr-gateway/opr-flowtrace-gateway.log`

Default event flow trace logging level is set to `INFO`. Only events with the custom attribute `__` `TRACE__` set are logged to the flow trace log files. To enable flow tracing for all events, set the flow trace log level to `DEBUG`.

Logging Administrator

This tool allows you to temporarily modify the level of details displayed in BSM logs, as well as create custom logs. To open the BSM Logging Administrator Tool, open the following URL:

http://<BSM Gateway Server>/topaz/logAdminBsm.jsp

Chapter 15

Port Usage

This section describes how to configure the ports that are used by BSM.

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 BSM Installation Guide.

    > **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.

Incoming BSM 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
383	Gateway Server, Data Processing Server	Events coming from 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	• **80.** HTTP/S channel to Gateway Server applications • **443.** Port for reverse proxy

Outgoing BSM 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" on page 320.
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.
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	• **80.** HTTP/S channel between the Gateway Server and data collectors for remote administration tasks • **443.** Port for reverse proxy

Local BSM Traffic

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

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.

Port Number	Allocated By	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
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 the JBoss process
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

Port Number	Allocated By	Port Usage
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
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 management channel for the HP services process
29700	Data Processing Server	RMI management channel for online BLE processes
29711,29712, 29713, 29714	Data Processing Server	RMI management channel for online BLE processes
29720	Data Processing Server	RMI management channel for online BLE processes
29800	Data Processing Server	HTTP port for online BLE processes

Port Number	Allocated By	Port Usage
29807	Gateway Server, Data Processing Server	Shutdown of main bus processes
29811, 29812, 29813	Data Processing Server	HTTP port for online BLE processes
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 channel for the Business Impact Process
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

Chapter 16

File Backup Recommendations

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.
\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.

Resource	Comments
\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.

Chapter 17

Working in Non-English Locales

This section describes how to configure BSM to work with languages other than English and discusses some of the issues that arise when using a non-Latin character set.

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 Comand 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 the BSM System Requirements and Support Matrixes.

- 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 BSM Database Guide. For supported and certified Oracle character sets, refer to Oracle Summary Checklist in the BSM Database Guide.

- 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 Sun Microsystems site (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.

Application Management for Siebel Issues

- Non-Latin characters may not appear or may be corrupted in the Topology View. If you encounter this problem, install the Arial Unicode Microsoft font from the Microsoft Web site.

- BSM by default only supports English language Siebel. Do not deliver data from a non-English version of Siebel to BSM. You should use special translation adapters to enable BSM to work with a non-English version of the Siebel application. For details, contact HP Software Support.

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 BPM Admin Console.

  Log files that are saved in the default encoding of the server on which the BPM Admin Console is installed are shown correctly in the View BPM Files window.

- All BPM instances (such as application, scripts, and parameters) 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.

- 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 RUM probe to support non-Unicode encodings, see Configuring the HP Real User Monitor Probe for I18N in the Real User Monitor Administration Guide.

- 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 134.

- 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 Guide.

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 the BSM Application Administration Guide.

- 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 How to View Web Pages That Are Written in a Different Language (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 the Modeling Guide.

- 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 BSM Installation Guide.

Part 3

Data Enrichment

Chapter 18

Location Manager

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).

To access the Location Manager:

Select **Admin > Platform > Locations**

Learn More

Location Manager Overview

You can:

- 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.

Tasks

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 157.

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" below.

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 "JMX Console" on page 102.)

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 164.

Each mass upload XML must begin with the following declarations:

- **<?xml version="1.0" encoding="UTF-8"?>** This states that this is an XML file with UTF-8 character encoding.

- **<!DOCTYPE locations_manager SYSTEM "./locations.dtd">** This is the document type declaration. The **locations.dtd** file is located in the **HPBSM/conf/locations** folder. The path to **locations.dtd** must be specified relative to the location of your XML file, and may need to be updated. If your XML file is saved in the same location as **locations.dtd**, no path is necessary.

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

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

XML File Example

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

World

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

  - location_2

    ○ location_2a

    ○ location_2b

  - location_3

- location_4

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

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

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

```
                    <location location_name="location_2">
                        <locations_list>
                            <location location_name="location_2a" />
                            <location location_name="location_2b" />
                        </locations_list>
                    </location>
                    <location location_name="location_3" />
                </locations_list>
            </location>
            <location location_name="location_4" />
        </locations_list>
    </customer_hierarchy>
</locations_manager>
```

For information on each of the XML elements and attributes, see "XML Tag Reference" on page 164.

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" below

- "Populate the Location Manager using an XML file" below

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 157.

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" below.

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 152. For details on the XML file elements and attributes, see "XML Tag Reference" on page 164.

   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 "JMX Console" on page 102.)

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

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

    customerId. By default, use 1 for **customerID**. If you are an HP SaaS customer, use your HP SaaS customer ID.

    target path. The location where you want to save the XML file.

5. Locate and edit the XML file just saved:

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

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

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

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

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

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

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

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

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

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

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

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.

UI Descriptions

Location Manager Page

This page enables you to manage locations and assign them IP ranges.
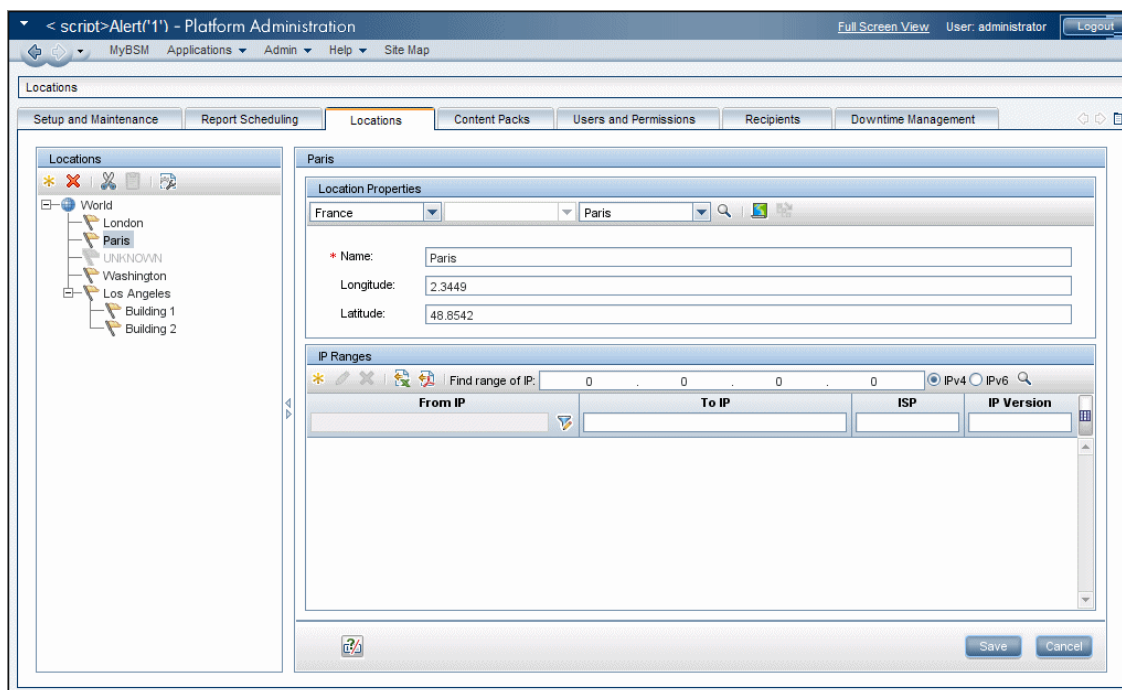
To access	Select **Admin > Platform > Locations**
Relevant tasks	"How to Populate the Location Manager" on page 154
See also	"Location Manager Overview" on page 151

- **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
✳	**Add location**. Click to add a new location below the selected location. Opens the Location Properties area.

UI Element	Description
✖	**Delete location**. Click to delete a location and its children locations. A **Confirmation** window opens, asking if you are sure you want to delete the location, and warning that the location may be in use by other BSM components and that there is no undo for this action. If you delete a location, any IP ranges assigned to it or its children can be moved to its parent location. To do this, select the **Move IP Ranges to the Parent Location** check box in the **Confirmation** window.
✂	**Cut location**. Click to cut a location. The location is copied to the clipboard, and can be pasted below another element in the locations tree. **Note:** When a location is cut, it remains visible, grayed out, in its former place on the tree, until it has been pasted in a different position. To deselect a cut location before it has been pasted to a different position, and return it to its original position, click **Cut location** again.
📋	**Paste location.** Available when a location has been cut and the user has navigated to another part of the tree. **Note:** Locations may be pasted under other locations, creating a hierarchical tree with a maximum of seven levels under the root. Assigning the same name to 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.
🔧	**Set as default container.** Click to set a particular location as the default container. This is the parent location for all automatically discovered locations. For more information, see "Location Manager Overview" on page 151.

- **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 162.
⧉	**Get coordinates from nearest parent.** Click to copy the geographical coordinates of the closest parent location with coordinates, to the selected location.
Name	Enter the name of the location in the **Name** text box. **Notes:** ● 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	Enter the longitude and latitude of the location in the longitude and latitude text boxes. If you select a location from the predefined drop-down lists of countries, states, and cities, or from the Geographical Map dialog box, the longitude and latitude boxes are filled automatically.

- **IP Ranges Area**

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

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

User interface elements are described below:

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

UI Element	Description

Find Range of IP	To find an existing range in which a particular IP address is located:
	
	1. Select the appropriate radio button:
	
	   • **IPv4** (Internet Protocol version 4) for addresses consisting of four numbers, each ranging from 0 to 255, in dot-decimal notation)
	
	   • **IPv6** (Internet Protocol version 6) for addresses consisting of eight hexadecimal numbers, each ranging from 0 to FFFF, in colon-separated notation)
	
	2. Enter the IP address in the **Find Range of IP** box.
	
	3. Click .
	
	The system highlights the range in which the IP address is found.
	
	Note: This searches for the IP range in the currently selected location only.

From IP/To IP, ISP, IP Version	To filter the IP ranges for a particular string of text in their lower and upper IP range limits, ISP names, or IP versions, enter the string in the **From IP**, **To IP**, **ISP**, or **IP Version** boxes. These boxes may be used in combination with each other. An asterisk (*) may be used as a wildcard to represent one or more characters. For example: • To filter for IPv6 addresses, enter "`6`" in the **IP Version** box • To filter for IPv4 address ranges whose upper limits end in 0, enter "`*.*.*.0`" in the **From IP** box.

New/Edit IP Range Dialog Box

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

User interface elements are described below:

UI Element	Description
IP version	Choose **IPv4** or **IPv6** to select: • Internet Protocol version 4 (for IP addresses consisting of four numbers, each ranging from 0 to 255, in dot-decimal notation) • Internet Protocol version 6 (for IP addresses consisting of eight hexadecimal numbers, each ranging from 0 to FFFF, in colon-separated notation)

UI Element	Description
From IP/To IP	Use the **From IP** and **To IP** boxes to set the range of IP addresses for the location. • For IPv4, as you enter an IP address in the **From IP** box, a corresponding address ending with 255 is automatically entered into the **To IP** box. All values in both boxes may be changed to any permissible value (0-255), but the address in the **To IP** box must be the same or higher than the address in the **From IP** box. Note: The IPv4 range must not exceed 50,000,000 IP addresses. • 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 154.
See also	"Location Manager Page" on page 157.

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.
(pan control)	**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.

UI Element	Description
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	
ip_range	Initial element in block defining attributes for a particular IP address range	ip_v6
start_ip	Lower limit of IP address range IP address ranges may be IPv4 or IPv6. Location Manager supports the following notation formats: IPv4 – number of 4 bytes IPv4 – string in x.x.x.x format IPv6 – number of 16 bytes IPv6 – string in x:x:x:x:x:x:x:x format IPv6 – IPv6 regular expression	

Element	Description	Attributes
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: - "undefined" (default) - "country" - "state" - "city"
location_id	location	The real ID of an existing location

Example:

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

Chapter 19

Content Packs

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.

> **Note:** This section discusses BSM-specific content packs only. For information about the HP Universal CMDB Discovery and Integration Content Pack, see **Admin > RTSM Administration > Administration > Package Manager**.

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.

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

BSM provides a number of content packs, for example 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. Such content is usually specified as **Predefined**, and can be modified (**Predefined (Customized)**). This modified content can be reverted to the predefined values.

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 170.

- Manage dependencies between content packs. For details, see "Dependencies in Content Packs" on page 171.

- 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 174.

- Import a content pack (definition and content) and the data it references. For details, see "Importing Content Packs" on page 175.

> **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**.
> After selecting the user for which you want to modify the Content Manager permissions, select the **Permissions** tab in the right pane and in the Context pane, select **Operations Management context > Administrative UIs > Content Packs**.

Content Types

Content types are referred to using the following terminology:

- **Predefined Content**

  Predefined content is usually content provided by HP or HP Partners and is designed to provide the initial configurations for a BSM installation.After installing a predefined content pack, you may change these initial artifacts to suit your environment and management needs. Any modified predefined artifacts are labeled as **Predefined (Customized)**.It is not possible to remove predefined artifacts, but you can revert any customized artifacts to their original, "predefined" values.

- **Custom Content**

  Custom content is content that is created by the customer, for example for managing a custom, in-house application, and is labeled as **Custom**.

- **Customized Content**

  Modified predefined artifacts are labeled as **Predefined (Customized)**.You can revert any customized artifacts to their original, "predefined" values.

Content Pack Types

Content pack types are referred to using the following terminology:

- **Predefined Content Pack**

  Predefined content packs are collections of predefined content typically provided by HP or HP Partners and are designed to provide the initial configurations for a BSM installation.

  After installing a predefined content pack, you may change these initial artifacts to suit your environment and management needs. Any modified predefined artifacts are labeled as **Predefined (Customized)**. It is not possible to remove predefined artifacts, but you can revert any customized artifacts to their original, "predefined" values.

  When importing the content of predefined content packs, this content is labeled as **Predefined**.

  - Predefined content packs must contain unique content. It is not possible to include identical content in more than one predefined content pack. This is checked on export and an appropriate error message displayed.

  - Predefined content packs must not contain referenced content.

  - Predefined content packs cannot be modified or directly deleted (as opposed to artifacts which can be modified). If you want to make changes to a predefined content pack, you must create a new version. When you import a new predefined content pack version, it overwrites the old version.

    > **Note:** To modify a predefined content pack, select **Create a New Version of the Selected Content Pack Definition** and specify a new version number. For more details, see "Create a New Version of a Predefined Content Pack Definition" on page 176.
    >
    > It is only possible to delete a predefined content pack in Content Pack Development mode (enabled in the Infrastructure Setting: Operations Management - Content Manager Settings).

- **Custom Content Pack**

  Custom content packs are collections of content typically created by the BSM user, for example for managing a custom, in-house application.

  When importing the content of custom content packs, this content is labeled as **Custom**.

  Custom content packs can have the same content as other custom or predefined content packs.

Content Pack Definitions

Content Pack Definitions serve two purposes:

- Creating Content Packs including the artifacts referenced by it.

- Describing predefined content of the system, serving as an inventory of predefined content.

A Content Pack Definition is identified by its name and version. It is not possible to have two Content Pack Definitions in the system with same name and version. It is possible to duplicate any definition by specifying either different name or different version. A new or duplicated content pack definition is labeled as a custom definition.

Only one Content Pack Definition with a given name can be predefined. If a Content Pack with predefined content based on a Content Pack Definition with the same name is imported, its definition does replace the existing definition.

Predefined content packs with predefined content from HP are imported during the BSM product installation. You can change the predefined artifacts, which then are marked as **Predefined (Customized)**. You can also revert customized artifacts to their original predefined values, but you cannot delete them.

Exporting and Importing Content Packs

You can export a Content Pack definition and included content. There are two modes:

- **Normal Mode**

  Content of exported content packs is labeled as custom.

- **Content Pack Development Mode**

  When a content pack is exported, you can define its content as predefined or custom, and is independent of whether the content pack definition used as base for the export is predefined or custom.

  Content Pack Development mode is enabled under the Operations Management - Content Manager Infrastructure Settings.

  > **Caution:** It is not recommended to create new versions of predefined Content Packs that you are not responsible for - as this may result in upgrade errors in the future.

If you import a content pack, its content is predefined or custom depending on how the content pack was exported.

Content Packs Manager Interfaces

The Content Packs manager has the following 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 > Setup > Content Packs

  There are two modes for working with content packs:

  - **Normal** — Only custom content packs can be modified and exported.

  - **Content Pack Development** — When exporting a content pack definition, you can specify whether it is predefined or custom. Custom content pack definitions can be modified. Predefined content pack definitions cannot be modified and must be replaced with an updated version if required.

    > **Caution:** It is not recommended to create new versions of predefined Content Packs that you are not responsible for - as this may result in upgrade errors in the future.

  Content Pack Development mode can be enabled in the Infrastructure Setting at the following location:

  Admin > Platform > Setup and Maintenance > Infrastructure Settings > Applications, use the list to set the administration context to **Operations Management**, and set the **Enable Content Pack development** entry under **Operations Management - Content Manager Settings** to true.

  For further details, see "Content Packs Manager User Interface" on page 184.

- **ContentManager Command-line Interface (CLI)**

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

  For details, see "Content Pack Manager Command-Line Interface" on page 193.

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

- **ContentAutoUpload Command-line Interface (CLI)**

  During BSM installation, all prdefined Content Pack Definition files are automatically uploaded from the default content pack location on the Data Processing Server:

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

  Using the ContentAutoUpload, you can:

  - retrigger the default content pack upload

  - specify a different folder from where content packs are uploaded

  For details, see "Content Pack Auto Upload Command-Line Interface" on page 196.

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.
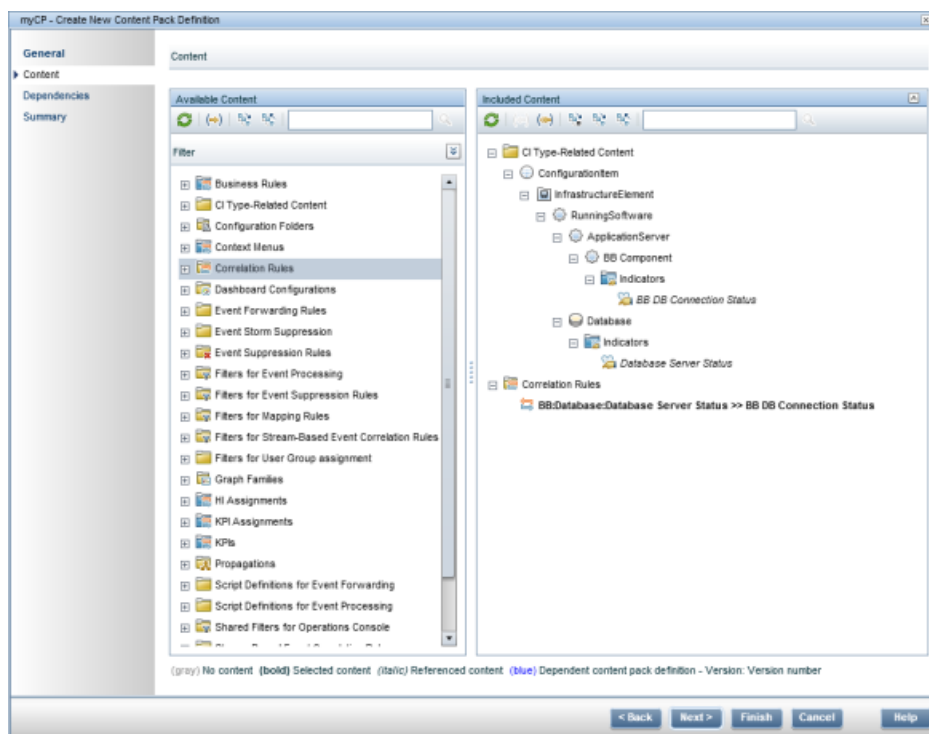
Dependencies in Content Packs

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.

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 the dependency in Content Pack C to reference **CPU Load** in either Content Pack A or B.
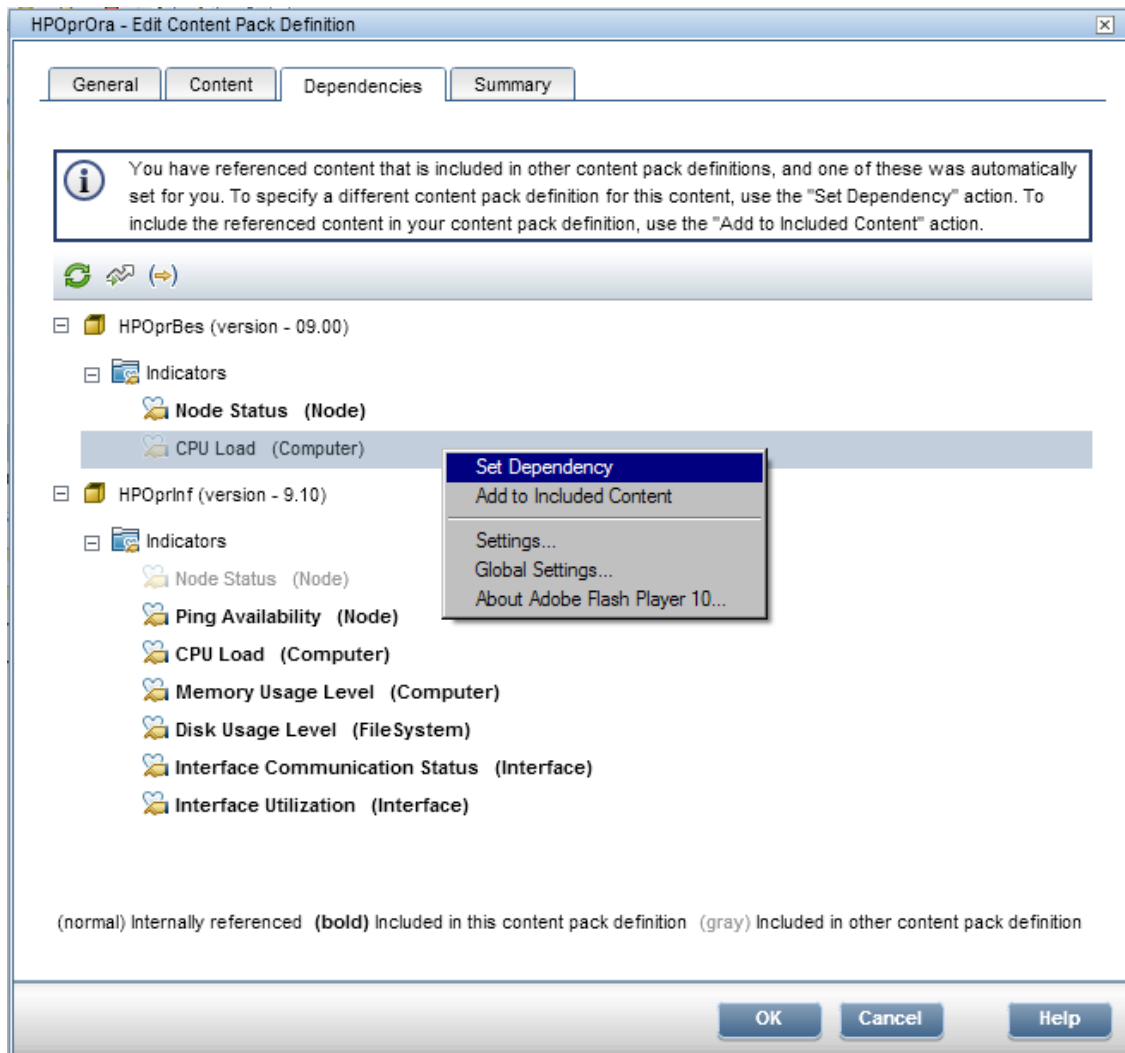
Referencing Dependent Content Included in Another Content Pack

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 The dependency is set automatically. 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.
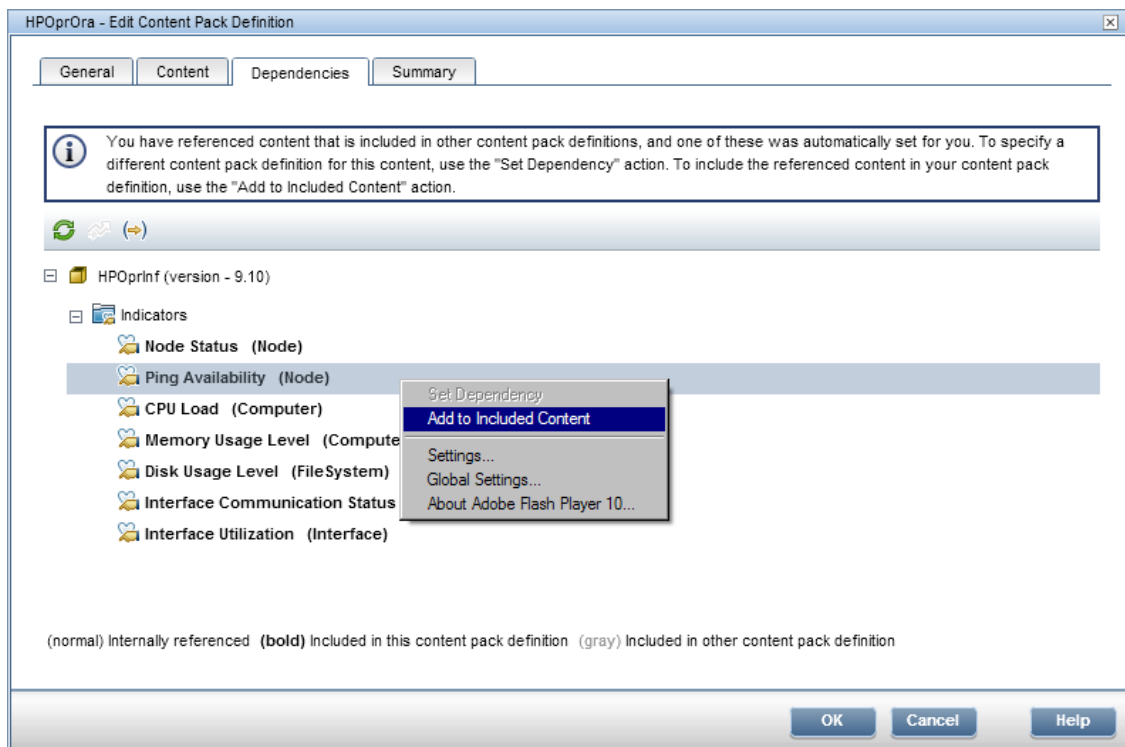
Deleting Referenced Content Pack

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.

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 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 "How to Create and Manage Content Packs" on page 176.

Importing Content Packs

When importing a content pack, you generally overwrite any existing data and add any new data. If you are importing a predefined content pack, only predefined content is overwritten with new data. Customized content is left untouched. Importing a custom content pack always overwrites existing 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 "How to Create and Manage Content Packs" on the next page. For details about the user interface and the options available in the import operation, see "Import Content Pack Dialog Box" on page 192.

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

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 [icon] button. The **Create New Content Pack Definition** wizard opens.

   - To edit an existing content pack definition, select it and click [icon]. 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** and **Version** combination must be unique.

   - The **Name** field 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 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 186.

Create a New Version of a Predefined Content Pack Definition

To create a new version of a predefined content pack definition:

1. Make sure that the **Enable Content Pack development** settings is enabled:

   > **Caution:** It is not recommended to create new versions of predefined Content Packs that you are not responsible for as this may result in upgrade errors in the future.

   a. Open Infrastructure Settings from the Platform Administration:

      Admin > Platform > Setup and Maintenance > Infrastructure Settings

   b. Select **Applications** and use the list to set the administration context to **Operations Management**.

   c. Enable the **Enable Content Pack development** setting in the Content Manager pane.

2. Open the Content Packs Manager: **Admin > Platform > Content Packs** and select the predefined content pack definition for which you want to create a new version.

3. Select the ⬚ button to open the Create New Content Pack Definition Version dialog box.

4. Change the version number of the content pack and click **OK**.

    The new version of this content pack is saved as a custom content pack.

5. Open the new version of the content pack definition, make the changes that you need, and save the changes.

For details on the user interface and all the available options, see "Create New Content Pack Definition Wizard" on page 186.

Export Content Packs

To export a content pack:

Note: It is not possible to export predefined content packs.

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 a 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. The default file type is ZIP.

Import Content Packs

To import a content pack:

Note: In SaaS installations, predefined content packs can only be imported by a SaaS Admin (Super User).

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. Content packs are usually in ZIP format. However, XML format content packs can also be imported. Content Packs to be imported with the Content manager UI must reside on the system that the BSM browser is running on.

    The default location for content packs is:

    <HPBSM root directory>/conf/opr/content/<locale>

    In a distributed deployment, this directory is located on the Data Processing server.

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

3. *Optional:* You can 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.

> **Note:** Existing items with the same ID are generally overwritten.
>
> If you are importing a predefined content pack, only predefined content is overwritten with new data. Customized content is left untouched. Importing a custom content pack always overwrites existing data.
>
> 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 Box" on page 192.

Checklist for Publishing Content Packs

Before you publish a newly developed content pack, you should make the following checks on a system where all available Content Packs (at least all OOTB Content Packs) plus your Content Pack is imported.

These checks help you to have clear ownerships of the content artifacts, which helps in upgrade scenarios and in developing new Content Packs.

Problems Found by Content Manager

Select your Content Pack Definition in the Content Manager and check if there is a **Problems Found** panel reported at the bottom of the Details pane.

This section typically reports inconsistencies between your Content Pack Definition and the available content. You must solve the reported problems before exporting the Content Pack. For example, your Content Pack Definition references content or dependent content that does not exist in the system. You must either remove the referenced content or dependency from your Content Pack Definition or make sure that the referenced content dependency is "installed".
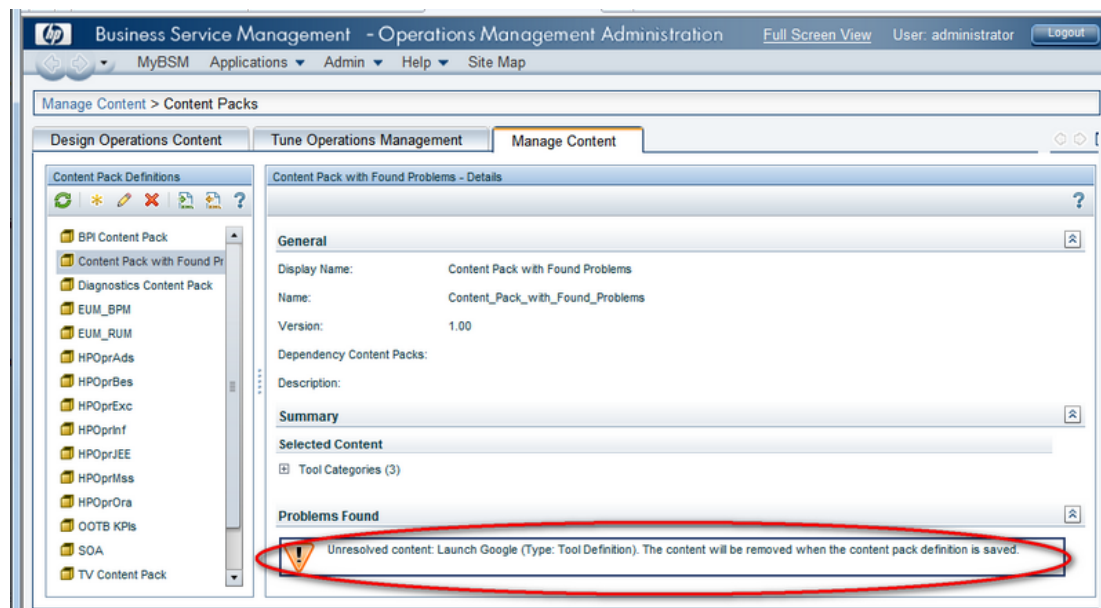
Check for Content in other Content Packs

Open your Content Pack Definition for editing in the Content Manager and select the **Content** tab. Check if there is a section titled **Content in other Content Packs** (bottom of Included Content pane).

In the Content in other Content Packs section, inspect each content artifact and decide if you are really the owner of this content artifact. If you are not the owner, exclude the content artifact from your Content Pack Definition and set a dependency to the owning Content Pack. Otherwise, contact the owner of the other Content Packs and request that they exclude the content artifact from their Content Pack Definition.
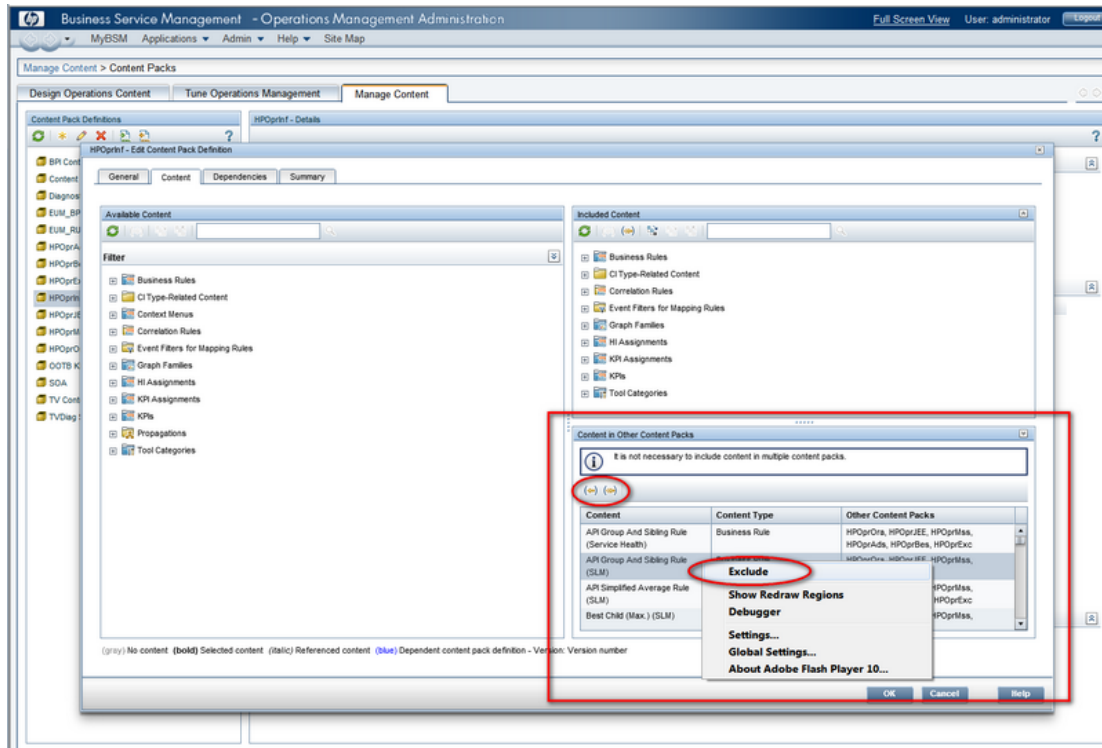
Check for Referenced Content included in This Content Pack

Select your Content Pack Definition in the Content Manager and check if there is a **Referenced Content included in This Content Pack** panel reported in the Details pane.

It is not recommended to have referenced content within your own Content Pack because this is an indication that the ownership of such content is not clear. If you are the owner, include the referenced content into your Content Pack Definition. Otherwise, set a dependency to the Content Pack Definition that owns the referenced content.
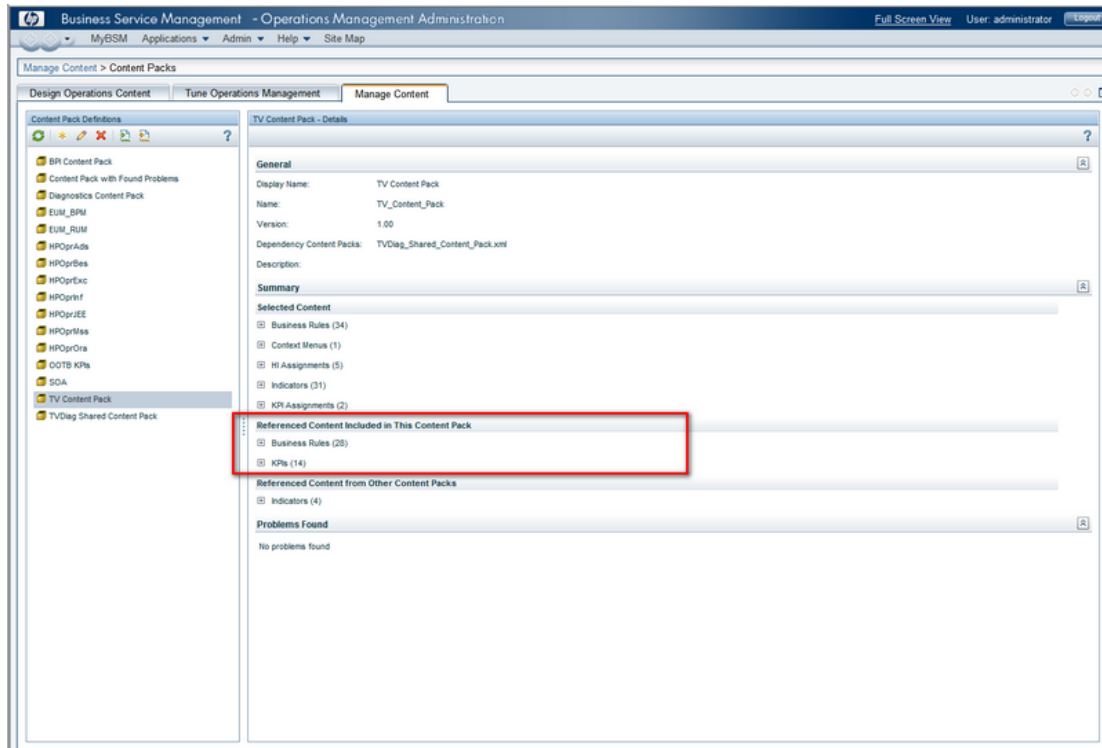
Include the referenced content into your Content Pack Definition

Open your Content Pack Definition for editing in the Content Manager and select the **Content** tab.

Search for referenced content and include it in your Content Pack Definition.

Make sure that you have completed the steps described above.
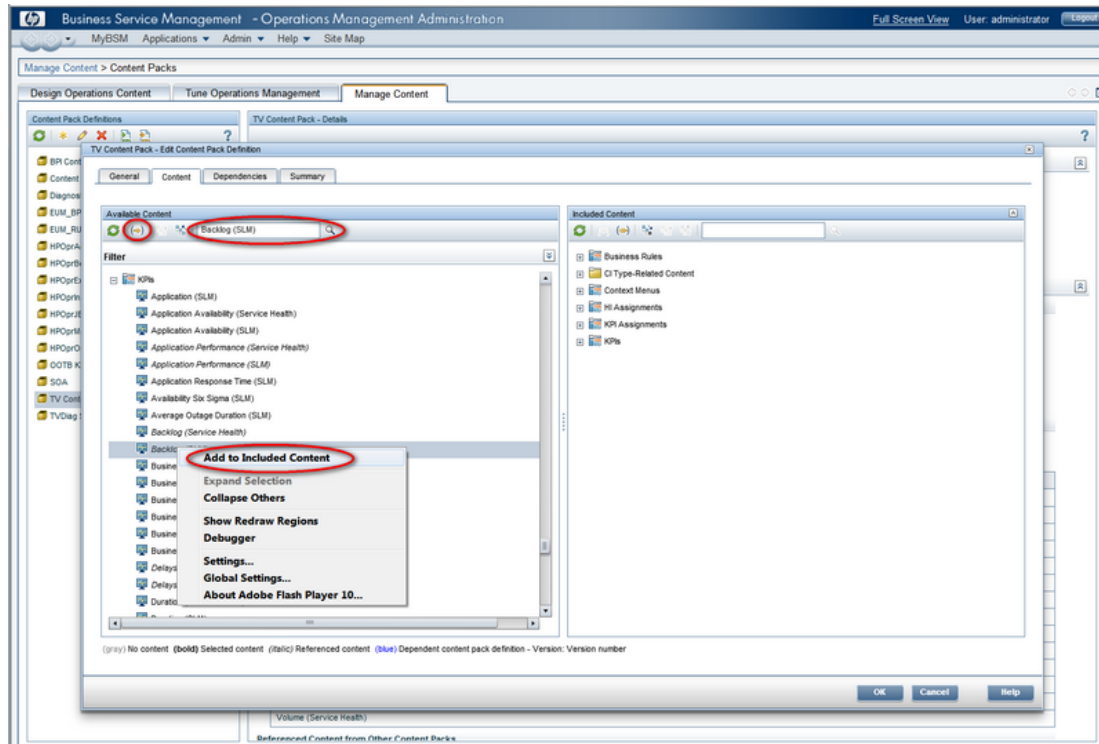
Set a Dependency

Open your Content Pack Definition for editing in the Content Manager and select the
Dependencies tab.

Inspect all content artifacts printed in normal font. Choose the Content Pack that is the owner of the
referenced artifact and set a dependency to it. The goal is to have no content artifacts displayed in
normal font in the Dependencies tab.

Content Packs Manager User Interface

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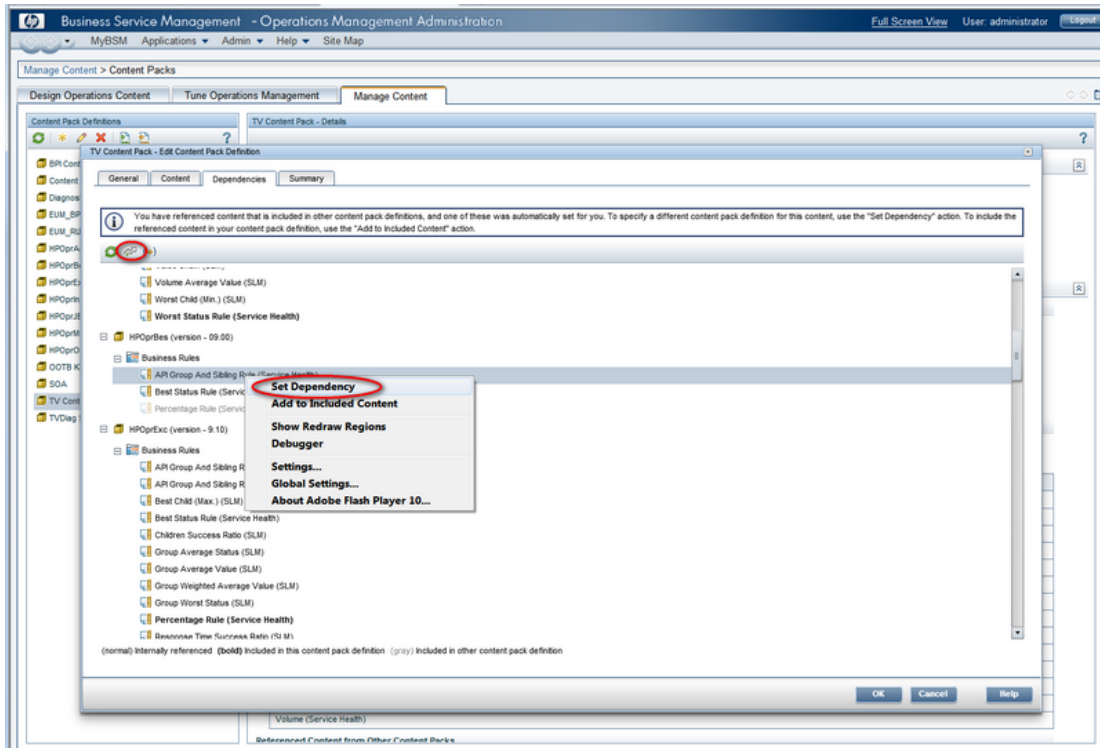
This area enables you to manage content pack definitions. A content pack definition describes the items included in a content pack. A content pack is a snapshot of the configuration data and other items that you have defined to help manage the resources in the IT environment you are monitoring with BSM.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

To access	Use one of the following:
	• **Admin > Platform > Content Packs**
	• **Admin > Operations Management > Setup > 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 176
See also	"Content Packs" on page 166

Definitions Pane

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

UI elements are listed in the following table.

UI Elements	Description
⟳	**Refresh.** Refreshes the contents of the displayed list. Use if new content becomes available while you are working or you have uploaded new contents (for example, from the command-line interface).
✳	**New Item.** Opens the **Create New Content Pack Definition** wizard. For details about the wizard, see "Create New Content Pack Definition Wizard" on page 186.
▤	**Create a New Version of the Selected Content Pack Definition.** Opens the Create New Content Pack Definition Version dialog box from which you can create a new version of the selected content pack definition.
	Alternatively, double-click a section in the **Details** pane to open the appropriate tab in the Create New Content Pack Definition Version dialog box or the Content Pack Definition in the Definitions pane (not valid for content packs that are not predefined).
	For details, see "Create a New Version of a Predefined Content Pack Definition" on page 176.

UI Elements	Description
✎	**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. Alternatively, double-click a section in the **Details** pane to open the appropriate tab in the Edit Content Pack Definition dialog box or the Content Pack Definition in the Definitions pane (not valid for content packs that are not predefined). For details, see "Create New Content Pack Definition Wizard" on the next page.
✖	**Delete Item.** Deletes the selected content pack definition (but not referenced content such as indicators and KPIs) from the list of definitions displayed.
🗔	**Import Content Pack Definitions and Content.** Opens the Import Content Pack dialog box, which enables you to specify or browse to a file that contains the definition details for import. You can first run the import in test mode, where 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 Box" on page 192.
🗔	**Export Content Pack Definitions 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. **Export Content Pack Definitions and Content (Predefined).** 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 as a predefined content pack.

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, a description of the selected content pack definition, and its origin (whether it is predefined or not).

UI Elements	Description
Summary	Displays a summary of the selected content pack definition's contents, divided into the following subsections. Each subsection contains a list of content and for each item in the list, the following information is displayed: ● Total number of artifacts ● Number of predefined artifacts ● Number of Predefined (Customized) artifacts ● Number of custom artifacts Expanding the content group displays the artifacts contained within that group, the CI Type of the artifact, and the origin of the artifact (Predefined, Predefined (Customized), Custom). ● **Selected Content**. Displays a list of the content, grouped by content type, selected for inclusion 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 this content pack. ● **Referenced Content from Other Content Packs**. Displays a list of the dependent content, grouped by content type, referenced from other content packs.
Problems Found	Displays information on any problems, such as unresolved dependencies (content that is included in the selected content pack definition but no longer exists in BSM), found in the selected content pack definition.

Create New Content Pack Definition Wizard

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

To access	Use one of the following: ● **Admin > Platform > Content Packs** ● **Admin > Operations Management > Setup > Content Packs** and then click ✳
Relevant tasks	"How to Create and Manage Content Packs" on page 176
Wizard map	This wizard contains: "General Page" on the next page > "Content Page" on page 188 > "Dependencies Page" on page 191 > "Summary Page" on page 191
See also	"Content Packs" on page 166

General Page

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

See also	"Content Packs" on page 166

User interface elements are described below:

UI Elements	Description
ID	No action required. The content pack ID is assigned automatically when the content pack is first created. **Note:** ID field is only displayed in the General tab of the Edit Content Pack Definition dialog box, not on the General page of the **Create New Content Pack Definition** wizard.
Display Name	Name displayed in Content Pack Definitions list. This name does not have to be unique. It is limited to a maximum length of 255 characters.
Name	Name of the content pack definition, which 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. **Note:** The name and version combination must be unique. When you export the content pack, this is the default file name for the file, with **OMi Content Pack -** as a prefix.
Version	Required, free text field. Use to control versions of your content packs. It is limited to a maximum length of 255 characters.
Description	Brief description (limited to 1024 characters) of the content pack definition you want to add to (or have selected in) the **Content Pack Definitions** pane. Use the Description box to remind other users of the scope and content of the content pack.
Predefined	Predefined content is usually content provided by HP or HP Partners and is designed to provide the initial configurations for a BSM installation.After installing a predefined content pack, you may change these initial artifacts to suit your environment and management needs. Any modified predefined artifacts are labeled as **Predefined (Customized)**. It is not possible to remove predefined artifacts, but you can revert any customized artifacts to their original, "predefined" values. **Note:** Only displayed in the Details pane.

Content Page

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

See also	"Content Packs" on page 166

User interface elements are described below:

UI Elements (A-Z)	Description
⟳	**Refresh:** Refreshes the contents of the displayed list. Use if new content becomes available while you are working or you have uploaded new contents (for example, from the command-line interface).
⟹	**Add to Included Content**: Adds the selected item(s) to the list of included content. If included content has already been included in another content pack, it is listed in the **Content in Other Content Packs** pane, and can safely be excluded from the content pack you are creating. It is not necessary to include content in multiple content packs. **Tip:** Selecting a CI type automatically selects all assigned content of the CI type and also all assigned content for child CI types. Selecting specific content, such as an individual indicator or KPI, automatically selects the reference to the CI type to which the content is related.
⊞	**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.
⌄	**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 (A-Z)	Description
	Search Content: Use the Search field to find the content in the **Available Content** or **Included Content** pane. Enter a search string in the Search box and click . The first content to match the specified string is highlighted. If that content is not initially visible, the tree expands to display it. To find the next occurrence of content matching the specified string, click again. The search string must be at least three characters long. Searching is 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 .
Available Content	Hierarchical list representing the available content in your IT environment. **Tip**: To include content in a content pack definition, drag it from the **Available Content** pane to the **Included Content** pane or select it and click the **Add to Included Content** button. BSM warns you if content already exists in other content packs when you perform an include operation. Color coding: • Folder with no content: gray • Selected content: bold • Referenced content: italic • Dependent content pack definition with version number: blue
Filter: Show only CI types with assigned content	Filters the CI Types tree to display only CI types that have content assigned to them.

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

Shortcut Menus

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

You display a shortcut menu by right-clicking an element in the 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.
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.

See also	
	• "Content Packs" on page 166
	• "Dependencies in Content Packs" on page 171

User interface elements are described below:

UI Elements	Description
⟳	**Refresh.** Refreshes the contents of the displayed list of dependencies. Use if new content becomes available while you are working or you have uploaded new contents (for example, from the command-line interface).
⤴	**Set Dependency.** If referenced content is also included in other content pack definitions, a message indicating this is displayed, and one of these was automatically set for you.
	To specify a different content pack definition for this content, use the **Set Dependency** action. To include the referenced content in your content pack definition, use the **Add to Included Content** action.
	The dependent content in the referenced content pack is displayed in bold, indicating that dependency has been set on it.
⇨	**Add to Included Content.** Adds the selected dependent content to the list of content included in this content pack.
<Color coding>	Color coding:
	• Internally referenced content: normal
	• Content included in the currently selected content pack definition: bold
	• Content included in another content pack definition: gray
<Version dropdown box>	If there is more than one version of a content pack that could be specified for referenced content, the version dropdown box becomes active and displays the selected content pack version.You can select an alternative version and set the dependency to it.

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.

See also	"Content Packs" on page 166

User interface elements are described in the table below:

The Summary Page displays a summary of the selected content pack definition's contents, divided into the following subsections. Each subsection contains a list of content and for each item in the list, the following information is displayed:

- Total number of artifacts

- Number of predefined artifacts

- Number of Predefined (Customized) artifacts

- Number of custom artifacts

Expanding the content group displays the artifacts contained within that group, the CI Type of the artifact (where applicable), and the origin of the artifact (Predefined, Predefined (Customized), Custom).

For example, indicators, mapping rules, and 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.
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 Box

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:
	● **Admin > Platform > Content Packs**
	● **Admin > Operations Management > Setup > Content Packs**
	and then click 🔲.
Relevant tasks	"How to Create and Manage Content Packs" on page 176

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.
Test	Runs a simulated import operation using the selected content pack definition, but does not commit any changes to BSM.
Import	Starts the specified content data import and closes the Import Content Pack dialog box.

Content Pack Manager Command-Line Interface

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

> **Note:** The appropriate identity assurance software, such as ActivIdentity, must be installed to be able to authenticate using a smart card when executing the ContentManager CLI tool.
>
> When connecting to BSM servers using Remote Desktop Connections, the client system must also have the appropriate identity assurance software, such as ActivIdentity, installed to be able to authenticate using a smart card attached to the client system when executing the ContentManager CLI tool remotely.
>
> In addition, in the Remote Desktop Connections dialog box, select More **Show Options > Local Resources > More** to open the Local devices and resources dialog box. Ensure that the **Smart Cards** checkbox is selected.

The **ContentManager** command-line interface is located on the Gateway Servers and the Data Processing Servers in:

<BSM_Root_Directory>/bin

> **Note:** The user executing the **ContentManager** CLI must have read access to the file:
>
> `<BSM_Root_Directory>/conf/TopazInfra.ini`

Usage

```
ContentManager <Operation> [Connection] <UserCredentials> [Option]
```

Operation (one of the following):

Import Operations:

-import <in_file> [-test]

Export Operations:

-snapshot -output <out_file>

-export <name> -output <out_file>

[-contentPackVersion <version>] [-asPredefined]

Miscellaneous Operations:

-list

-delete <name> [-contentPackVersion <version>]

-version

Connections (one of the following):

-url <URL>

-server <gatewayserver> [-port <port>] [-ssl]

User Credentials:

-username <login name> [-password <password>]

[-customer <customer Id>]

Options:

-verbose

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

Option	Description
-asPredefined	Marks the exported Content Pack as predefined.
-cpv,-contentPackVersion <version>	Version number of the Content Pack Definition
-cu-customer <customer Id>	Id of customer in SaaS environment. If this parameter is not set the default value is 1.
-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.

Option	Description
-e,-export <content_pack_ name>	Exports the named content pack definition and its content to the file specified using the `-output` option.
-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. Importing a custom content pack overwrites the existing objects. Importing a predefined content pack overwrites all none-customized objects.
-j, -jks <arg>	Specifies the java key store to be used for authentication.
-l,-list	Lists the content pack definitions.
-o,-output <output_file>	Specifies the name of the file to which you want the command to write during the export operation.
-p,-port <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.
-password <password>	Requests the password of the user specified in the -username option, whose account is being used for authentication purposes.
-sc, -smartcard	Use certificate stored on smart card or security token for authentication.
-server <gateway_server>	Sets the target BSM gateway server using either a hostname or an IP address. The specified server must be a BSM gateway server. Default is "{0}". **Note:** 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. **Caution:** This option should only be used when upgrading to a newer version of the Content Pack.
-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.

Option	Description
-u, -url <URL>	Specifies the URL of the BSM gateway server to access. The default value is: `http://<Gateway Server DNS name>:<port>/opr-admin-server` Do not specify this option in conjunction with the -server option.
-username <login_name>	The name of the user, whose account is being used for authentication purposes.
-v,-verbose	Prints verbose output.
-version	Prints the version information of the command and exits.
-wc, -winCrypto	Use the windows certificate store for authentication. This option is only available on Windows systems.

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 Pack Auto Upload Command-Line Interface

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

The **ContentAutoUpload** command-line interface is located on the Data Processing Server in:

<BSM_Root_Directory>/bin

> **Note:** The user executing the **ContentAutoUpload** CLI must have read access to the file:
>
> `<BSM_Root_Directory>/conf/TopazInfra.ini`

Usage

```
ContentAutoUpload <Operation> [Option]
```

Operation (one of the following)::

Import Operations:

-autoUpload [-uploadFolder <directory>]

[-forceReload]

Miscellaneous Operations:

-version

Options:

-verbose

The following table gives more information about the arguments recognized by the **ContentAutoUpload** command:

Option	Description
-a,- autoUpload	Automatically uploads the Content Pack Definition files from the default content pack directory on the Data Processing Server: *<BSM Root Dir>*/conf/opr/content/*<locale>*/ **Windows:** **C:\HPBSM\conf\opr\content*<locale>*** **Linux:** **/opt/HP/BSM/conf/opr/content/<locale>/** If you want to upload content pack definitions from an alternative directory on the Data Processing Server, specify the directory location using the `uploadFolder` *<directory>* option. **Note:** If you have more than one Data Processing Server, you must keep the content pack folders synchronized because it is not possible to specify from which Data Processing Server content packs may be imported. All predefined 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. For information about import errors, see the following log file: *<BSM Root Dir>*/log/EJBContainer/opr-webapp.log **Windows:** **C:\HPBSM\log\EJBContainer\opr-webapp.log** **Linux:** **/opt/HP/BSM/log/EJBContainer/opr-webapp.log**
-forceReload	Enforces the reload of all content packs located in the default directory (*<BSM Root Dir>*/conf/opr/content/*<locale>*/) or the directory specified using the `uploadFolder <directory>` option. Non-customized content is overwritten.
-h,-help	Displays a summary of the command options and exits.
-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. **Caution:** This option should only be used when upgrading to a newer version of the Content Pack.
- uploadFolder <directory>	If you want to upload content packs from an alternative directory, specify the directory location using the **-uploadFolder <directory>** option. For example: `ContentAutoUpload -a -uploadFolder c:\temp`

Option	Description
-v,-verbose	Prints verbose output.
-version	Prints the version information of the command and exits.

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

Exit Status	Description
0	SUCCESS (At least one content pack was imported and no errors occurred.)
1	FAILURE (No content packs were imported - complete failure.)
2	FAILURE_PARTIAL (Some content packs were imported successfully, others had errors.)
3	NO_OPERATION (No new content was found for upload.)
4	NO_PERMISSION (User does not have appropriate permissions to execute this tool.)
5	SYNTAX_ERROR (Wrong command-line arguments were specified.)

Troubleshooting and Limitations

This section provides troubleshooting help related to content management, including 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.

Chapter 20

Downtime Management

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. This page 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 application

- CI collection

- Infrastructure service

- Business service

Downtime Actions

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

- **Alerts and Events**. Events are suppressed and no CI Status alerts, EUM alerts, or notifications are sent for any of the CIs associated with the downtime.

- **KPIs**. KPIs attached to the CI and impacted CIs are not updated and display the downtime for the CI in Service Health. For details on how downtime configurations affect Service Health, see KPI Status Colors and Definitions in the BSM User Guide.

- **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 the BSM User Guide.

- **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 Retroactive SLA Data Corrections in the BSM Application Administration Guide.

- **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 the BSM User Guide.

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 depend 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 Behavior in the BSM Application Administration Guide.

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 in the BSM Extensibility Guide.

How to Create and Manage Downtimes for CIs

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

1. Prerequisites

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

- When determining which CIs may need downtimes, take into consideration CIs that impact the CIs that you selected. In some cases, these CIs are also affected by downtime.

  To understand the downtime impact model, see the **BSMDowntime_topology TQL** in the RTSM Modeling Studio.

  > **Note:** By default, **BSMDowntime_topology TQL** is hidden. To view this TQL, in the Modeling Studio go to **Admin > RTSM > RTSM Administration > Administration > Package Manager > Tools > User Preferences > General > Show hidden queries** and set the value to **True**. The maximum depth that the impact can affect is 15 steps.

  You can only select CIs from the following CI types:

  - node
  - running_software
  - 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 > Event Automation > Downtime Behavior.**

For details on this topic, see Downtime Behavior in the BSM User Guide.

3. ## Run the Create Downtime wizard

   Go to **Admin** > **Platform** > **Downtime Management** and click the **Create New Downtime**

   button

   For user interface details, see "New Downtime Wizard" on page 207.

4. ## Results

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

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

   Tip: To limit the downtimes in the exported file to a specified selection, you can filter the
   visible downtimes in the Downtime Management page 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.

Downtime Management User Interface

Downtime Management Page

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

To access:	Select **Admin > Platform > Downtime Management**
Important information	• To add, edit, or delete downtimes, you must have Full permission on the Downtime resource. In addition, you should have View permission on the Views to which CIs in the downtime belong. For details on permissions, see "Permissions" on page 220.
	• Information displayed on this page is view only. To edit any of the values, double-click on a downtime or select a downtime and click the **Edit** button.
	• For downtimes that have already occurred, only the following fields are editable:
	▪ Properties page - all fields
	▪ Scheduling page - **End by** date in **Range of recurrence**
	▪ Notification page - **Selected Recipients**
	• You can filter the list of downtimes displayed using the field at the top of each column. For example, you can view only items with a specific "Action" using the drop-down list at the top of the Action column. By default, downtimes with status of "*Completed*" are hidden, to view them, click the **Edit the Filter** button at the top of the Status column.
Relevant tasks	"How to Create and Manage Downtimes for CIs" on page 203
See also	"Downtime Management" on page 201

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 207.
✎	**Edit downtime.** Opens the Edit Downtime wizard, which enables to you edit the configuration of an existing downtime. This wizard contains the same screens as the New Downtime wizard. For details, see "New Downtime Wizard" on page 207.
⧉	**Duplicate downtime.** Clones the settings of an existing downtime to a new downtime.

UI Element (A–Z)	Description
	Delete downtime(s). Deletes selected downtime(s). Downtimes that are active now or were active at any time in the past cannot be deleted. This is designed to prevent the loss of historical data.
	Terminate Active Downtime. Cancels all future occurrences of the selected downtime and marks the downtime status as *Completed*.
	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 210.
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.
Scheduling	Displays the: ● Date, time, time zone, and duration For recurring downtimes, also displays: ● What day of the week or month the downtime is scheduled to recur ● Range of recurrence
Status	Displays whether the downtime is currently: ● **Active.** The CIs are currently in downtime and the action selected for the downtime is now taking place. ● **Inactive.** The downtime is configured but it is currently not the time for the downtime to take place. ● **Completed**. The time for the downtime has passed and the actions configured for the downtime have occurred.
Optional Columns	
Approved by	Indicates if there was an approval for the downtime and who approved it.

UI Element (A–Z)	Description
Category	The category assigned to the downtime. Options include: ● Application installation ● Application maintenance ● Hardware installation ● Hardware maintenance ● Network maintenance ● Operating system reconfiguration ● Other ● Security issue You can also create your own customized categories using Infrastructure Settings. To add a custom downtime category: 1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**. 2. Select **Foundations** > **Downtime**. 3. 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 will appear as an option in the list of available downtime categories.
Planned	Indicates whether the downtime is planned or not.

New Downtime Wizard

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

To access	**Admin > Platform > Downtime >** click the **Create new downtime** button, or select existing downtime and click the **Edit downtime** button.
Relevant tasks	"How to Create and Manage Downtimes for CIs" on page 203
Wizard map	This **New Downtime Wizard** contains: "Properties Page " on the next page > "Select CIs Page " on the next page > "Scheduling Page " on page 209 > "Action Page" on page 210 > "Notification Page " on page 212 > "Preview Page " on page 213
See also	"Downtime Management" on page 201

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.
See also	"Downtime Management" on page 201

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 the BSM User Guide. Cannot exceed 2000 characters.
Approved by	You can enter the person or department who approved this downtime. Cannot exceed 50 characters. **Note:** In Oracle, if you are using East Asian Languages (Chinese, Japanese, or Korean), the maximum number of characters for **Downtime Name**, **Downtime Description**, or **Approved by** may be less than specified above.
Planned	Select if you want this downtime marked as planned. You can create downtimes that are unplanned. This is for information purposes only.
Downtime Category	Select a category from the drop-down menu. This category describes the reason for the downtime. You can also create your own customized categories using Infrastructure Settings. To add a custom downtime category, select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**: • Select **Foundations**. • Select **Downtime**. • In the **Downtime - General settings** table, edit the **Downtime category** value to the name you want to use as a customized category for the downtime. The name you enter appears as an option in the list of available downtime categories after you restart BSM.

Select CIs Page

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

Important information	For downtimes that have already occurred, you cannot edit the selected CIs in this page.
See also	"Downtime Management" on page 201

User interface elements are described below:

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

Scheduling Page

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

Important information	• You cannot schedule a downtime in the past.
	• For downtimes that have already occurred, only the following field is editable in the Scheduling page:
	End by date in **Range of recurrence**
	To cancel a recurring downtime that has already occured at least once, edit the downtime and modify this field.
See also	"Downtime Management" on page 201

User interface elements are described below:

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

Action Page

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

Important information	For downtimes that have already occurred, no fields in the Action page are editable.
See also	"Downtime Management" on page 201

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	• 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. **Note:** During the downtime period, the affected CI may change its status, and the status change may trigger the relevant CI Status alert.
Enforce downtime on KPI calculations; suppress alerts and close events	• 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. • Reporting and monitoring continue. SLAs are updated.
Enforce downtime on Reports and KPI calculations; suppress alerts and close events	• 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
Stop active monitoring (BPM & SiteScope); enforce downtime on Reports & KPI calculations; suppress alerts and close events (affects all related SLAs)	• 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. **Note:** If you configure a downtime period for an Application CI (whose data is updated by BPM monitoring), Downtime Manager automatically sends an event to the BPM Agent when the downtime period starts. The agent stops sending samples to BSM. The samples that are suppressed are the BPM samples that correspond to the Transaction CIs, which are child CIs of the Application CIs on which the downtime is configured. There is one sample per transaction.

Notification Page

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

Important information	For downtimes that have already occurred, you can edit the **Selected Recipients** in the Notification page.
See also	"Downtime Management" on page 201

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 298.
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.

See also	"Downtime Management" on page 201

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.

Editing Downtimes

- If while editing a downtime in the Downtime wizard its status changes from **Idle** to **Active**, the downtime cannot be saved.

- If you want to cancel a recurring downtime that has already occured at least once, edit the downtime's **End by** date in the Scheduling page.

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 216.

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

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

Users, Permissions, and Recipients

Chapter 21

User Management

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. You can grant permissions directly to an individual user or to a user group. User groups 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. For example:

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 "Create Users" on page 227.

- **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**).

  You can apply superuser permissions to other users in the system. These users with superuser permissions can be modified in User Management.

- **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" on page 297.

- **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 groups, or granted individually when its parameters are configured. For details on permissions, see "Permissions" on the next page.

- **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 225.

- **Customize User Settings.** Select the page users see they open BSM, and choose the menu items available on pages throughout the system. For details, see "Customize User Settings" on page 229.

Permissions

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 the next page.

- The roles and operations area on the right side of the page. For details on roles, see "Roles" on page 223. For details on operations, see "Operations" on page 223.

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

The following is an example of Granting Permissions:
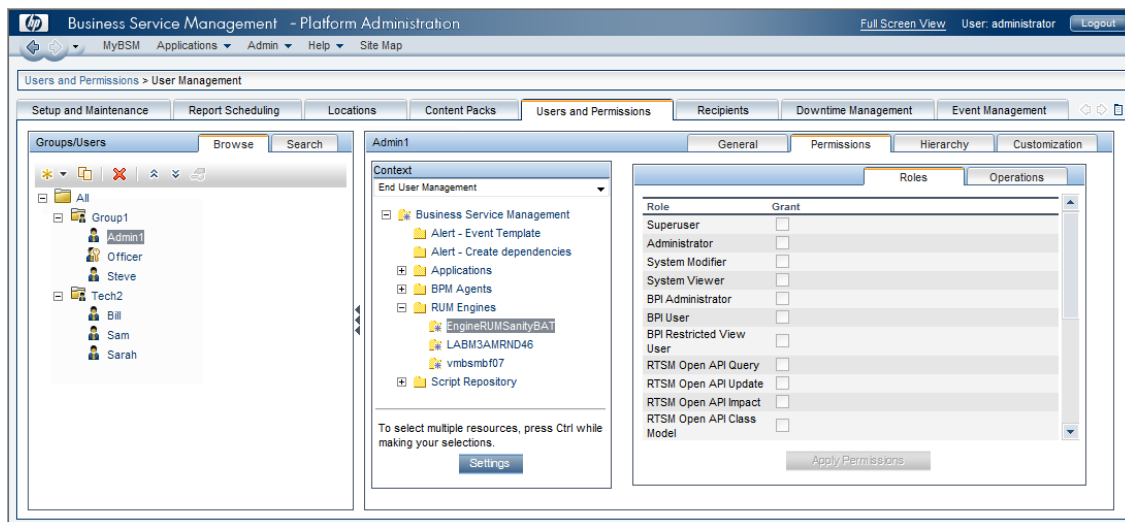
For details on assigning permissions, see "Assign Permissions to Groups or Users" on page 228.

> **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 223.
>
> - 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 are 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.

Resources and Resource Instances

There are the following types of resources in Permissions Management:

📁	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.
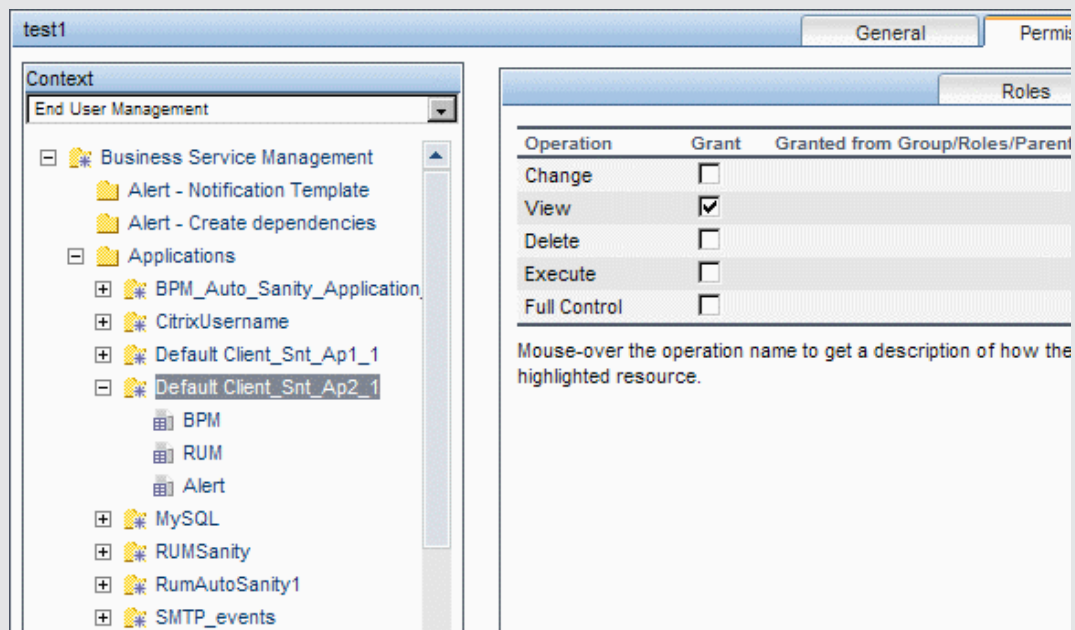
Guidelines for Working with Resources

- 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 the next page.

- To manage the permissions on a sub-resource, 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 sub-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" below.

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 243.

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 272.

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 RUM, the security officer can configure settings for masking sensitive data. For details, see Sensitive Data Area in the BSM Application Administration Guide.

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 their 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 288.

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 240.

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**.
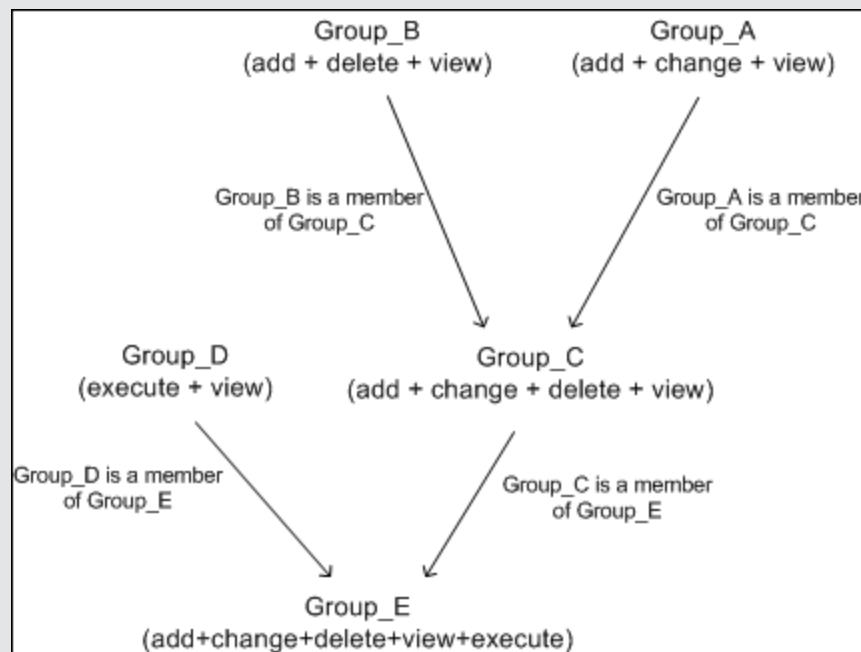
A circle of nested groups is not permitted. For example, **Group_A** is a member of **Group_ B**, and **Group_B** is a member of **Group_C**. **Group_C** cannot be a member of **Group_A**.

Note: All permissions in the previous example refer to the same resource.

For details on setting up nested groups, see "Configure User and Group Hierarchy" on page 228.

Configure Users and Permissions

Below is a suggested workflow for the User Management application. For a use-case scenario related to this task, see "How to Configure Users and Permissions — Use-Case Scenario" on page 231.

Prerequisites

Before you configure User Management, you should map out the required users and groups and their relevant permission levels. 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 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 the BSM Application Administration Guide.

- If multiple users require similar system permissions, create a list of groups, 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 221.

Create Groups

You create groups in the **Groups/Users** pane. You can create groups as sub-groups nested under other groups. Sub-groups have the same access restrictions as the parent group.

1. Select **Admin > Platform > Users and Permissions > User Management**.

2. In the Groups/User pane select a location for the group, for example you may want to create the group as a sub-group under another group.

3. Click the **New Group/User** ⚹ ▾ button, and then select **Create Group**.

4. In the Create Group dialog box, enter the group name and if required a group description.

> **Note:**
>
> The group name must be unique, cannot exceed 40 characters, and cannot contain any special characters: **" \ / [ ] : | < > + = ; , ? * % &**
>
> The group description is optional and cannot exceed 99 characters.

Create Users

You create users and then place them into the appropriate groups.

1. In the Groups/User pane select the group that the user should belong to, click the **New Group/User** ⚹ ▾ button, and then select **Create User**.

2. In the Create User dialog box, on the User Account tab, enter the following information:

   ■ **User name.** Cannot exceed 40 characters and cannot contain special characters: **" \ / [ ] : | < > + = ; , ? * % &**

   ■ **Login name.** The name that the user will use to log into the system. The Login name must be unique, cannot exceed 40 characters, and cannot contain special characters.

   ■ **User Mode.** Available options are:

     ○ **Unspecified.** Leaves the user without a particular mode. Select this option if your system does not work with user modes or if the system does work with user modes but you want this user to see KPIs for both modes in Service Health views.

     ○ **Operations User.** Enables the user to view the operations version of KPIs.

     ○ **Business User.** Enables the user to view the business version of KPIs.

   ■ **Time zone.** The time zone of the user's location.

   > **Note:** When you modify the time zone, the linked recipient offset from GMT is also updated after you confirm the change. Half time zones (also known as offset time zones) are not supported.

   ■ **Password** and **Confirm password.** The password cannot exceed 20 characters.

3. **(Optional)** On the Recipient tab, enter required information. For information about the fields on this tab, see "New or Edit Recipient Dialog Box" on page 303.

Once you have created a user, you can modify user information in the Groups/User page. For user interface details, see "Groups/Users Pane" on page 288.

Assign Permissions to Groups or Users

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 more information about permissions, see "Permissions" on page 220.

1. In the Groups/User pane select the groups or users that you need to assign permissions to, and select the **Permissions** tab on the right side of the page.

2. Select a context for the groups or users. For details on the available contexts, see "Resource Contexts" on page 293.

3. Select the required roles for the groups or users. For details on the available roles, see "User Management Roles Applied Across BSM" on page 243.

4. **(Optional)** On the **Operations** tab, select the operations that the groups or users can perform. For details on the available operations, see "User Management Operations" on page 272.

> **Note:** After you have changed user permissions, the user needs to log out of BSM and log in again for the changes to take effect.

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.

> **Note:**
>
> 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 350.

1. Ensure that you have configured at least one group and one user in the **Groups/Users** pane.

2. 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.

3. In the Hierarchy tab, click the **Edit Child Groups and Users** button.

4. Use the ▷ or ◁ buttons to add or remove groups or users from the list of nested items.

Customize User Settings

You can customize user settings to:

- Select the default context that is displayed for specific users or groups when they log into BSM.

- Specify the first page that is displayed for specific users or groups in each of the different parts of BSM.

- Select contexts, applications, tabs, and options that will be available for users or groups.

You can customize settings for individual users or for all users in a group, including all members of sub-groups that are part of a parent group. If you restrict access to a feature or report for a group, all members of that group will not have access to the feature and you will not be able to override the setting for individual users.

If you add users or sub-groups to a group that has group settings applied, the users or members of the sub-groups will automatically get the access restrictions that were applied to the parent group.

> **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.

For a use-case scenario related to this task, see "How to Customize User Menus — Use-Case Scenario" on page 237.

1. Select a group or user in the **Groups/Users** pane, and select the **Customization** tab on the right side of the page.

2. Select a context from the **Contexts** pane that you want to be the default entry context that this user or all users in a group will see when they log into BSM, and click **Set as Default Entry Context**.

> **Note:** The **Default Entry Page** icon appears next to the specified context.

3. In the **Contexts** pane, clear the check boxes of the contexts and applications that you want hidden from the user or all members of the group.

4. In the **Pages and Tabs** pane, select the pages and tabs that you want to be visible on the selected context for the user or group.

5. If required, select a default page or tab for each context that will appear by default when the user opens that context.

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 298.

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 "Configure Users and Permissions" on page 227.

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, and 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:
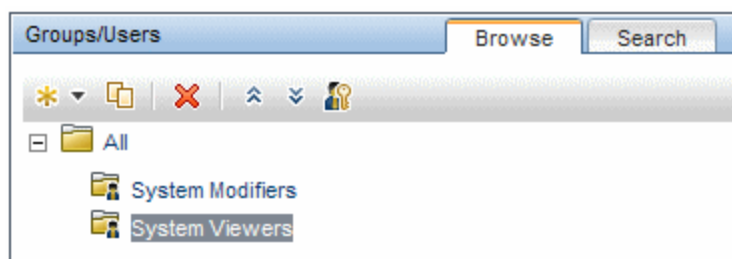
3. ## Assigning Permissions to Groups

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:
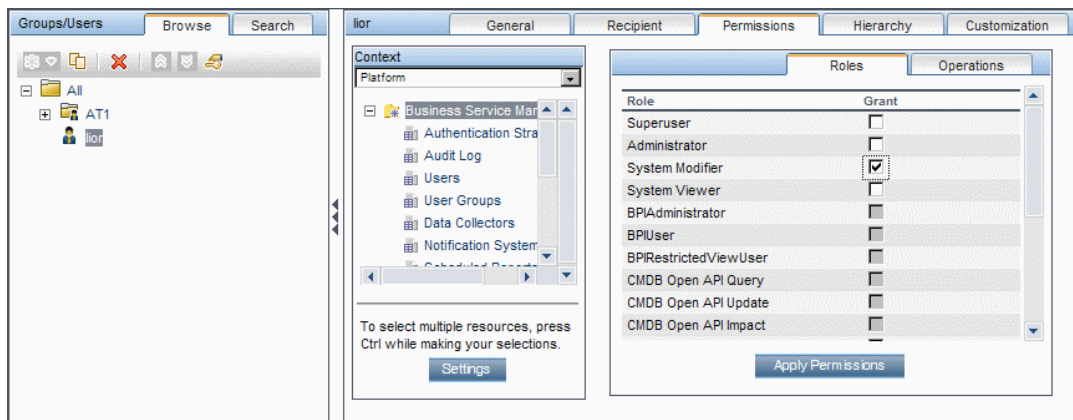
4. ## Creating Users

Jane must now create users to nest within the groups, based on the required 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:
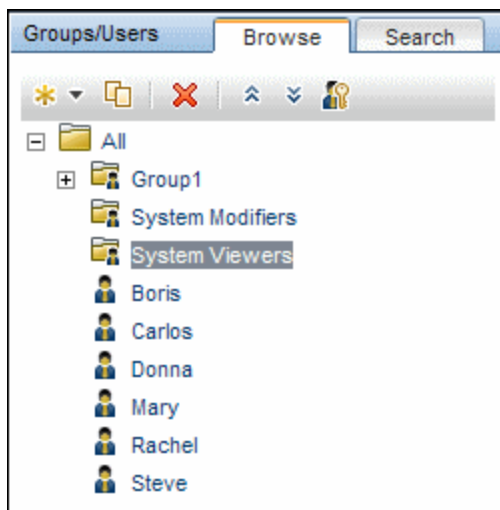
5. ## Configuring User and Group Hierarchy

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:
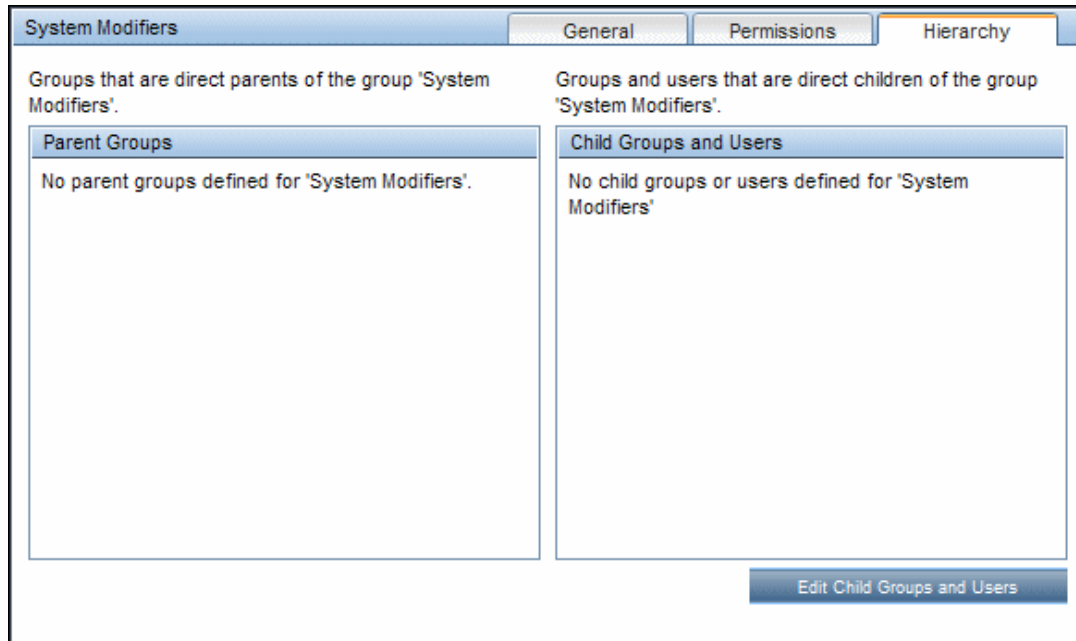
Jane clicks the **Edit Child Groups and Users** button to open the Edit Child Groups and Users dialog box:
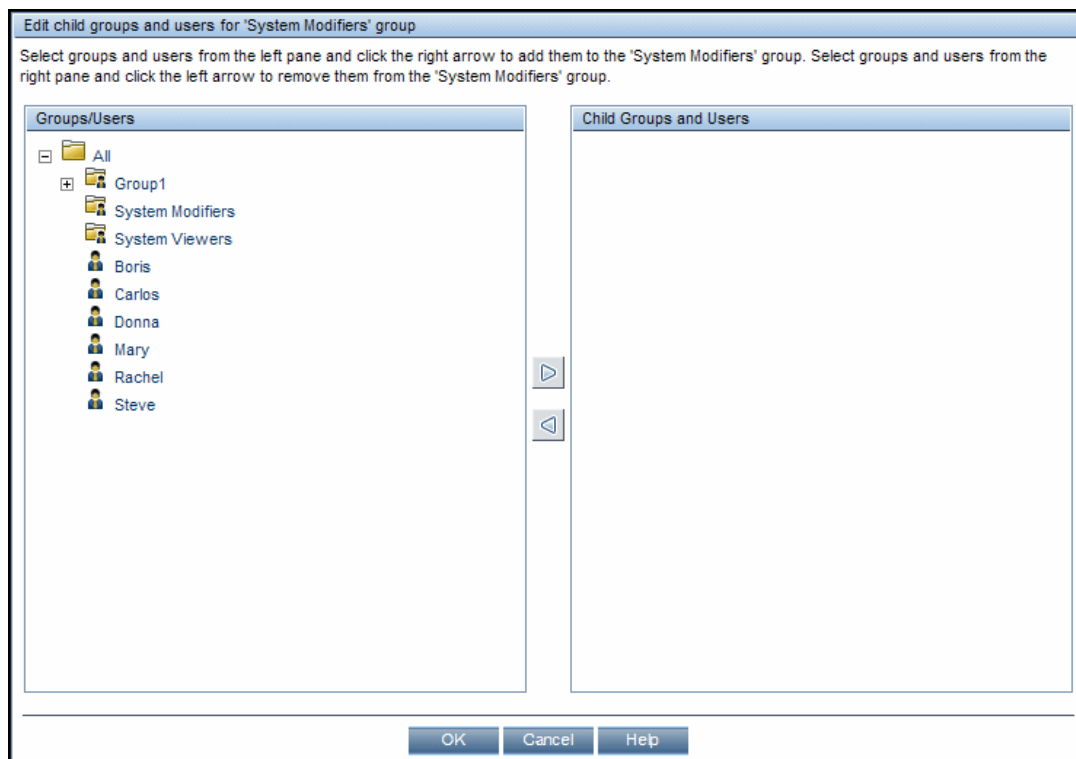
She then selects the relevant users from the **Groups/Users** pane and clicks the right arrow to move them to the **Child Groups and Users** pane. The Hierarchy tab indicates that these users are nested within the System Modifiers group, as follows:
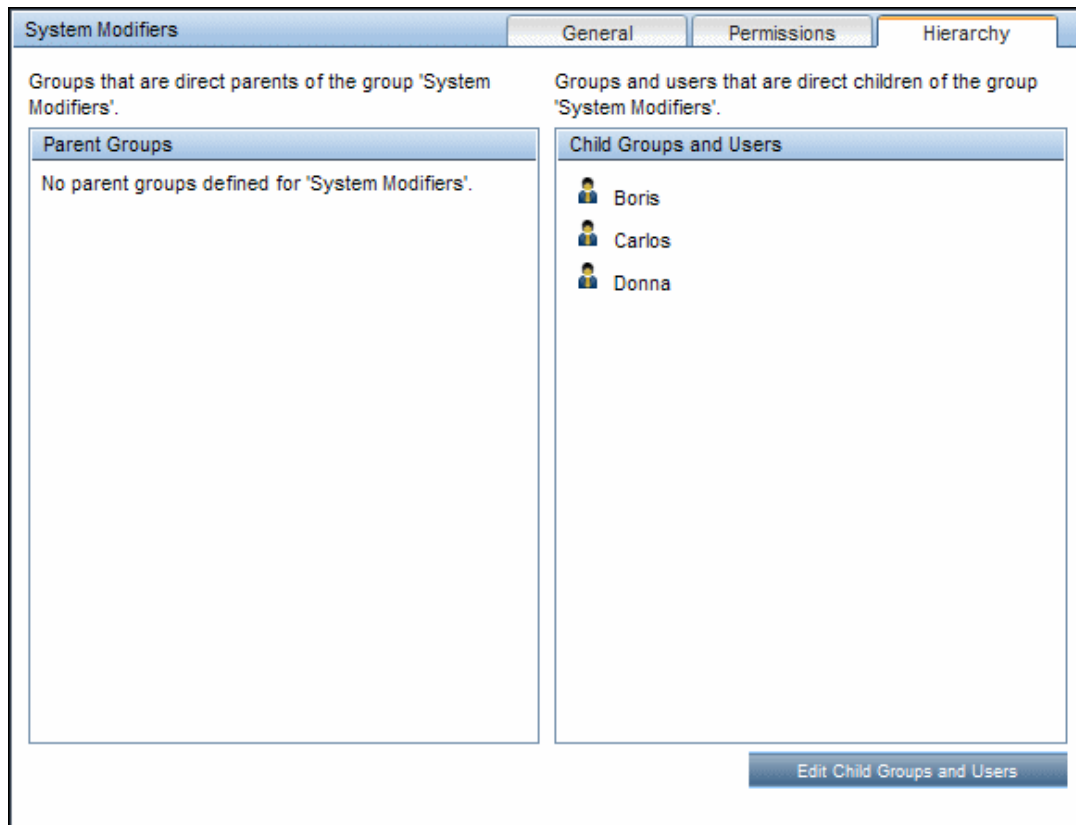
After following the same procedure to nest the relevant users in the System Viewers group, the **Groups/Users** pane is displayed as follows:
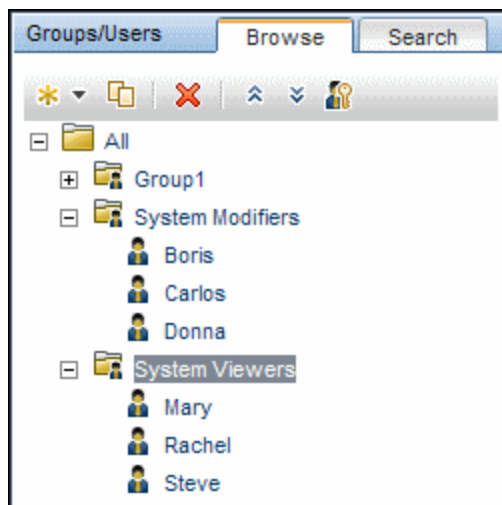
Since Steve has the added permission level of SiteScope Administrator, Jane selects the username of the user in the **Groups/Users** pane whom she wants to give the added permission level of SiteScope Administrator, and in the **Permissions** tab, selects the **System**

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:
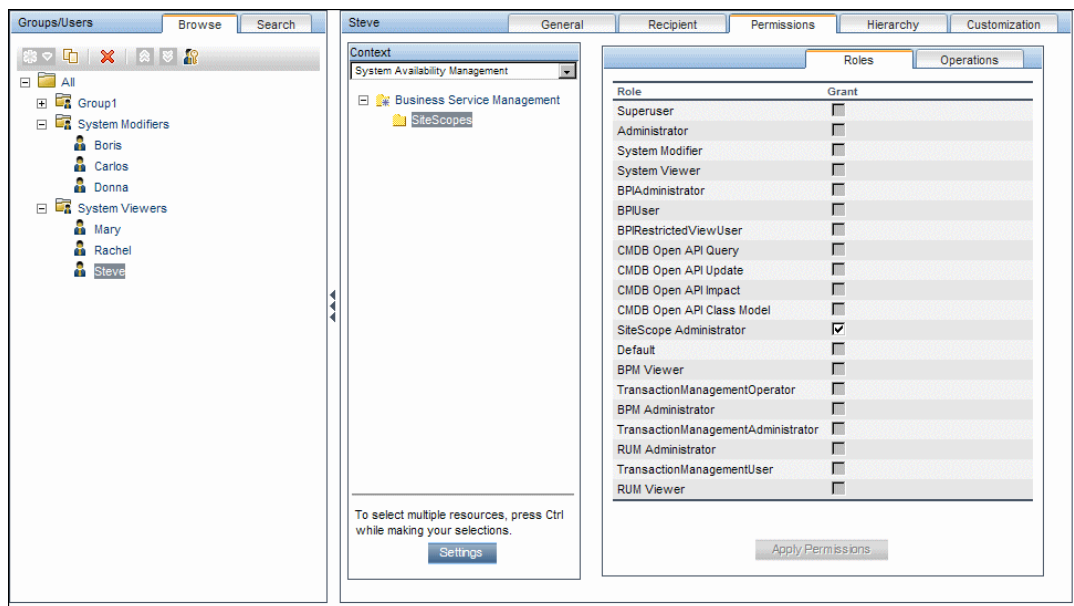
6. ## Customizing User Settings

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 login page that the user sees according to the customized configurations is as follows:
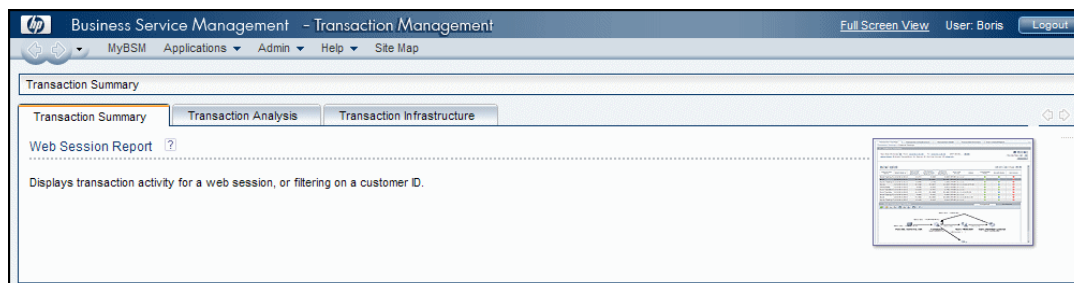
How to Customize User Menus — Use-Case Scenario

This use-case scenario describes how to customize user menus for individual users.

> **Note:** For a task related to this scenario, see "Customize User Settings" on page 229.

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:

   Set as Default Entry Context

   Contexts

   - ☑ Applications - MyBSM
   - ☑ Applications - Service Health
   - ☑ Applications - Service Level Management
   - ☑ Applications - End User Management
   - ☑ Applications - Transaction Management
   - ☑ Applications - System Availability Management
   - ☑ Applications - Business Service Management for Siebel
   - ☑ Applications - Application Management for SOA
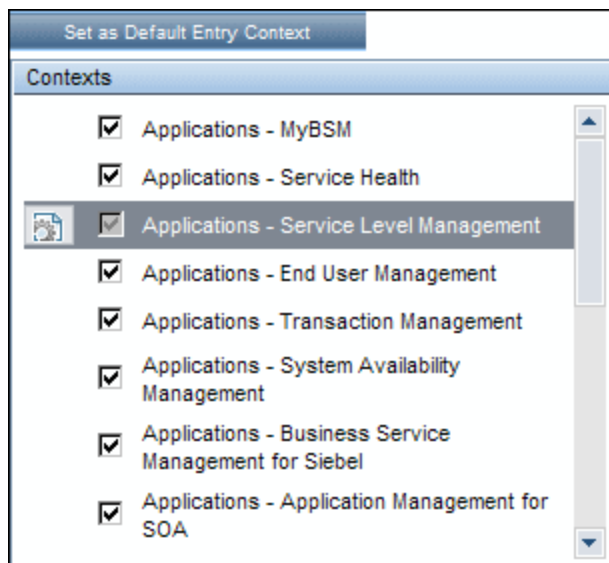
3. ## Selecting Context Pages and Tabs

   Since John is not authorized to view Outage Reports, that option is cleared in the Pages and Tabs pane, leaving the remaining pages and tabs checked to be visible when John logs into 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:
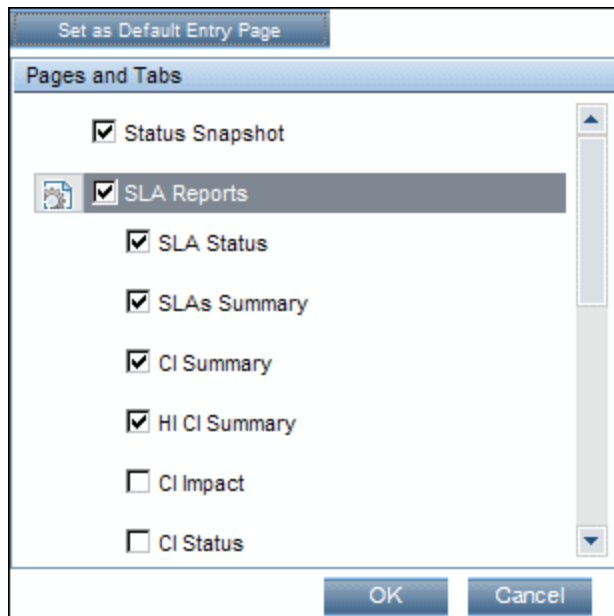
4. **Results**

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:
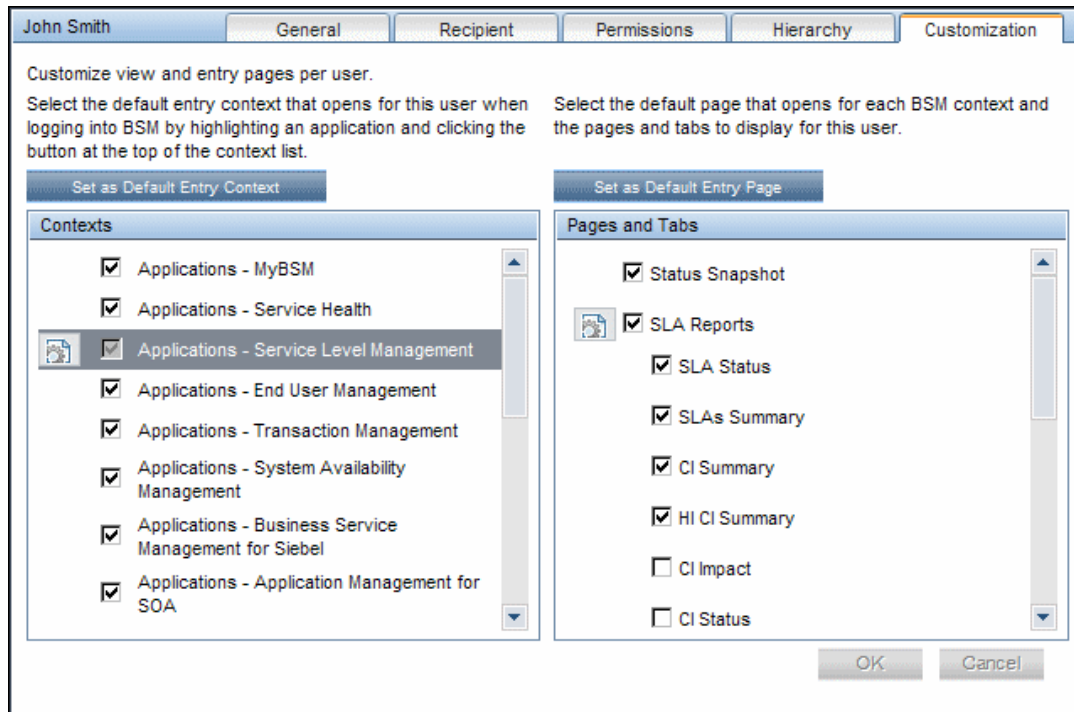
Screen that John sees when logging into BSM:
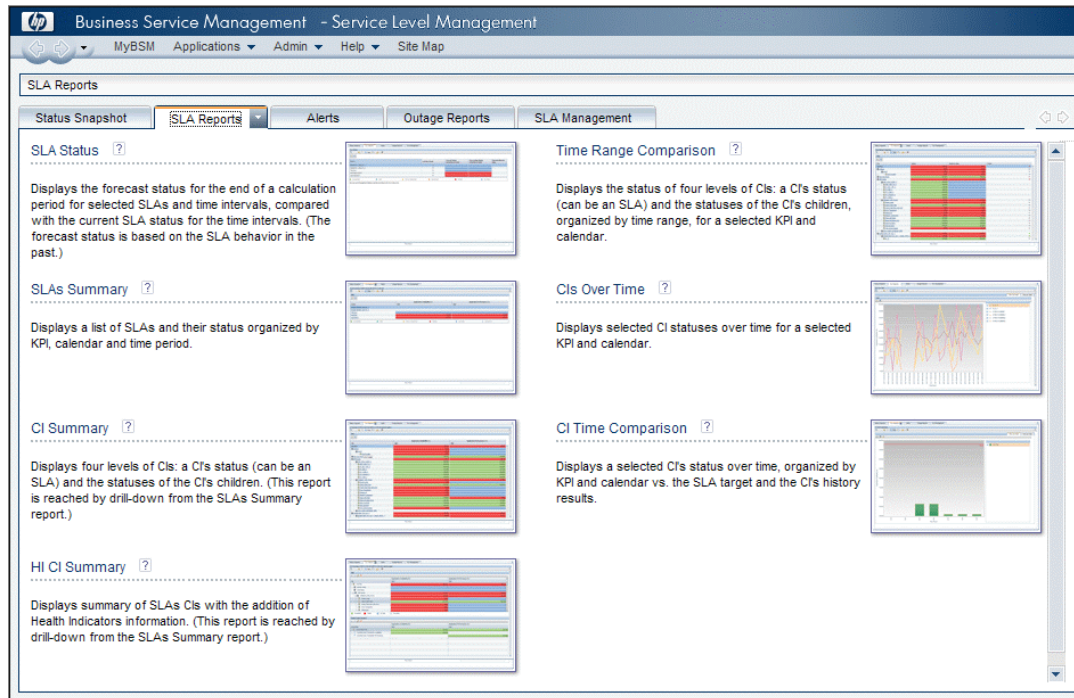
How to Remove Security Officer Status Using the JMX Console

This task describes how use the JMX console to remove security officer status from a user. 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 223.

To remove a security officer:

1. In a browser, enter the URL of the JMX console:
   http://<Gateway or Data Processing Server name>:8080/jmx-console/

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: **setSettingValuePerCustomerId**

   > **Note to HP BSM SaaS customers:** You need to enter the relevant customer ID at the top of the page. For assistance, please contact HP Support.

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 Export and Import User Information Using the JMX Console

This task describes how use the JMX Console to copy user, role, and permission information from a source system to a target system. For example, if you need to configure a new BSM database, you may need to copy user information from an existing database.

Set Contexts to Export

You can limit which contexts will be included in the export. You can view a list of available contexts in the JMX Console:

1. In a browser, enter the following URL:
   http://<SOURCE_Server>:8080/jmx-console/HtmlAdaptor?action=inspectMBean& name=Topaz%3Aservice%3DAuthorization+Service

2. Enter your JMX Console user name and password.

3. On the JMX MBean View page, click the **Invoke** button below **java.util.Set listAuthorizationContexts()**. JMX Console displays all contexts in TAS.

If you need to limit the contexts included in the export:

1. On the source server, open the following file **HPBSM\conf\tas\exportedContexts.properties**

2. Modify the **contexts-to-export** property.
   Contexts in the **contexts-to-export** property must be separated by commas only, without spaces.

3. Save your changes.

Export

Use JMX Console to create a .zip file that contains .xml files with user, role, and permission information.

1. In a browser, enter the following URL:
   http://<SOURCE_Server>:8080/jmx-console/HtmlAdaptor?action=inspectMBean& name=Topaz%3Aservice%3DAuthorization+Service+Data+Import+Export

2. On the JMX MBean View page, click the **Invoke** button below **void loadExportedContexts()** and then click the Browser's Back button to return to the JMX MBean View page.

3. Below **void exportAllTasEntities()**, in the **ParamValue** field, enter a location and file name for the export file on the source server. The file name must have a .zip extension for example: **C:\HPBSM\export.zip**

4. Click the **Invoke** button below **void exportAllTasEntities()**.

Transfer

You need to copy the export .zip file from the source server to the target server.

1. On the source server, browse to the export file as defined above.

2. Copy the file to the target server.

Import

Import the users, roles and permissions from the .zip file to the target BSM system.

> **Caution:** Before you import user and group information, make sure that the target server does not have any created resources, such as reports, profiles, and monitors, that have user information that is not compatible with the information that you are importing.

1. In a browser, enter the following URL:
   **http://<TARGET_Server>:8080/jmx-console/HtmlAdaptor?action=inspectMBean&
   name=Topaz%3Aservice%3DAuthorization+Service+Data+Import+Export**

2. Enter your JMX Console user name and password.

3. Below **void importAllTasEntities()**, in the **ParamValue** field, enter the location and file name of the export file and click the **Invoke** button.

User Management Roles Applied Across BSM

This section lists roles that can be applied across all contexts within BSM and the resources that each role applies to.

For details about roles that can be applied only to specific contexts, see "User Management Roles Applied to Specific Contexts" on page 268.

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 "User Management Roles Applied to Specific Contexts" on page 268.

Administrator

The **Administrator** role can be applied only to the **Business Service Management** resource.

Administrators have a collection of permissions that enable them to add profiles to the system and manage the resources related to those profiles. After a profile had been added, the administrator has full control privileges on all resources within that profile instance.

Business Process Insight

Resource	Allowed Operations
Business Process Insight Application	View
Business Process Insight Administration	Full Control

Diagnostics

Resource	Allowed Operations
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
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
Scheduled Reports	Add Change View Delete Full Control
Recipients	Add Change View Delete Full Control

Resource	Allowed Operations
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

SiteScopeOn 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

Resource	Allowed Operations
User Data	View Full Control
Applications	Add

User Defined Reports

Resource	Allowed Operations
Custom Reports	Add Change View Full Control
Trend Reports	Add Change View Full Control
Custom Links	Change View Full Control
Excel Reports	Change View Full Control
Default Footer/Header	Change Full Control
Favorite Filter	Change 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 resources in 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.

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
Pre-defined Pages	View
User Pages	Full Control
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
Databases	Change View
System Recipient Template	Change View

RTSM

Resource	Allowed Operations
Views	Change View

Resource	Allowed Operations
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

SiteScopeOn 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

Resource	Allowed Operations
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 with the exception of the RUM Engines resource. There

are some resources on which the view operation is not applicable, a system viewer has no access to those resources.

Business Process Insight

Resource	Allowed Operations
Business Process Insight Application	View

Diagnostics

Resource	Allowed Operations
Diagnostics	View

End User Management

Resource	Allowed Operations
Alert - Notification Template	View
Applications	View
BPM Agents	View
RUM Engines	View Edit
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

Resource	Allowed Operations
Data Collectors	View
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

SiteScopeOn 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).

Business Process Insight

Resource	Allowed Operations
Business Process Insight Application	View
Business Process Insight Application	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
Script Repository	Add Change View Delete Full Control

MyBSM

Resource	Allowed Operations
Predefined Pages	Full Control
User Pages	Full Control
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
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
Scheduled Reports	Add Change View Delete Full Control
Recipients	Add Change View Delete Full Control

Resource	Allowed Operations
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
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

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.

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
Predefined Pages	View
User Components	Full Control
User Pages	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

Resource	Allowed Operations
Central Repository Service	Add Change View Delete Execute Full Control
Notification System	View Execute Full Control
Package Work Manipulation	Change Full Control
Scheduled Reports	Add Change View Delete Full Control
Recipients	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

Resource	Allowed Operations
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

Resource	Allowed Operations
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
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 cannot modify transaction threshold settings and transaction descriptions.

Any regular user who was added as a user on a specific application in the previous version is upgraded to the BPM Viewer role for that application.

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 applications, including permissions.

Any administrator who was added as a user on a specific BPM application in the previous version is upgraded to the BPM application administrator role for that application. This is in addition to being assigned the administrator role as described above (for details, see "Administrator" on page 243).

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.

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.

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 243.

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 **SiteScope**s 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

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 Diagnostics when accessing Diagnostics from BSM.
	Execute	Enables changing the settings in the 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. Applies to End User Management (administration and reports) only.
		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.
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
	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.
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 the scripts in those folders, as well as downloading scripts from the script repository. **Note:** This does not enable uploading scripts to the script repository.
		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.
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 the BSM User Guide.

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 the BSM User Guide.

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.
Administrative UIs	View	Grants access to the Administration features in the Operations Management Administration, for example: • Correlation Rules manager • Content Packs manager • Performance Graphs manager • View Mappings manager • Event Processing Customization • Custom Actions Users who do not have read access to Operations Management Administration are not able to see the Operations Management Administration features or see an error message when they try to start an Administration manager.

Resources	Operation	Description
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.

Resources	Operation	Description
Authentication Strategy	Change	Enables the Configure button on the Authentication Management page, which enables changing configurations on the Authentication Management Wizard.
	View	Enables viewing the Authentication Management Wizard.
	Full Control	Enables performing all available operations on the Authentication Management 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.

Resources	Operation	Description
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.
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.
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.

Resources	Operation	Description
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.
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.
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.

Resources	Operation	Description
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.
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.
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.
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.

Resources	Operation	Description
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.
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.
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

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	When you first access the User Management page or the cursor is located on the **All** node, the page includes: • the **Groups/Users** pane. For details, see "Groups/Users Pane" below. • the **Workflow** pane. The Workflow pane displays introductory information about the User Management application, and a suggested workflow for configuring groups and users.
Relevant tasks	"Configure Users and Permissions" on page 227
See also	• "User Management" on page 219 • "Groups/Users Pane" below

Groups/Users Pane

This pane displays the list of users and groups of users configured to access BSM.

To access	Select **Admin > Platform > User Management**. The Groups/Users pane appears on the left side of the page, and is visible on all tabs of the User Management application.
	
	The Groups/Users pane contains the following tabs:
	
	• **Browse.** Displays a list of configured users and groups, and enables you to create or delete users and groups.
	
	• **Search.** Displays a table view of users and groups, and enables you to search for a user or group by any of the following criteria:
	
	   • Group name
	
	   • Login name
	
	   • User name
	
	   • User last login
	
	You can sort the columns by clicking on the column headers above the boxes.
	
	You can include wildcards (*) in your search.

Important information	• When selecting more than one user or group and modifying parameters, the changes take effect only for the first selected user. The exception is the Delete option, which deletes multiple users at once. • When creating a group, the access permissions are automatically inherited by the group's users. • When creating users with the cursor on a group, the users are automatically nested within that group.
Relevant tasks	"Configure Users and Permissions" on page 227
See also	"User Management Main Page" on the previous page

User interface elements are described below:

UI Element	Description
✳ ▾	Creates a user or group. Depending on whether you choose to create a user or group, the **Create User** or **Create Group** window opens. When you create a new group or user, the **Groups/Users** pane refreshes and the newly created group or user is selected. **Note:** In Firefox, after refresh, the **All** node is selected.
⧉	Clones the settings of an existing user or group to a new user or group
✖	Deletes the selected user or group. **Note:** When you delete a user, the linked recipient is also deleted.
⌃⌃ ⌄⌄	Collapses or expands the groups selected in the hierarchy tree. **Note:** Only previously loaded nodes are expanded.
👥▾	Click and select **Group Mappings** to map local groups to groups configured on the LDAP server, or **Delete Obsolete Users** to delete 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. For details, see "Group Mappings Dialog Box" on the next page. **Note:** This button is displayed only if the Mapping option has been enabled in the Authentication Management Wizard. For details, see "Authentication Wizard" on page 327.

UI Element	Description
	Click to assign or view the Security Officer. The security officer is a user who can configure certain sensitive reporting information in the system, such as which RUM transaction parameters to include or exclude from certain reports (such as Session Details or Session Analyzer). 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 223.
	A configured user
	A configured group
	Security officer
	Root node

Group Mappings Dialog Box

This dialog box enables you to map groups configured in BSM to groups configured on the LDAP server.

To access	Select **Admin > Platform > Users and Permissions > User Management**. In the Groups/Users pane, click the **LDAP Configuration** button and select **Group Mappings**. The Group Mappings dialog box consists of the following panes: • **Corporate Directory Pane.** For details, see "Corporate Directory Pane" on the next page. • **BSM Local Repository For Remote Group Pane: <group name>.** For details, see "BSM Local Repository for Remote Group: <group name> Pane" on the next page. • **Local Groups to Remote Group Mappings.** Displays a table of the LDAP groups and the BSM groups that they are assigned to. The LDAP groups are displayed in the **Remote Group Name** column, and the BSM Groups are listed in the **Local Group Name** column.
Important information	**Note:** This dialog box is accessible only if LDAP mode has been enabled in the Authentication Wizard. For details, see "Authentication Wizard" on page 327. If you are switching from one LDAP server to another, ensure that you remove all existing group mappings from the original LDAP server before mapping to the new one.

Corporate Directory Pane

This pane enables you to assign BSM groups to LDAP groups, and to list the users in the LDAP groups.

Description	Select **Admin > Platform > Users and Permissions**; in the Groups/Users pane, click the **LDAP Configuration** [icon] button and select **Group Mappings**.
Important information	• 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**. You can also select either of these options by right clicking on the group. • 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: ▪ 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** [icon] button and select **Group Mappings**.
Important information	• To remove groups, select the group you want to remove and click **Remove Groups**. • You can remove mulitple groups at once by holding the `Ctrl` button while selecting groups.

Permissions Tab (User Management)

This tab enables you to apply permissions to groups and users for specific resources and instances of those resources that are defined in the system.

To access	Select **Admin > Platform > Users and Permissions > User Management > Permissions** tab.
	The **Permissions** tab is divided into the following areas:
	● **Groups/Users** pane on the left side of the page. For details, see "Groups/Users Pane" on page 288.
	● Resource tree pane in the center of the page. For details, see "Resource Tree Pane" below.
	● **Roles** tab on the right side of the page. For details, see "Roles Tab" on page 294.
	● **Operations** tab on the right side of the page. For details, see "Operations Tab" on page 295.
Important information	● You can grant permissions to only one user or group at a time.
	● Assigning **Add** permissions on the Operations tab **does not** automatically grant **View** permissions on the given resource.
	● If you have many users for whom you have to grant permissions, it is recommended that you organize your users into logical groups using the Hierarchy tab.
Relevant tasks	"Configure Users and Permissions" on page 227
See also	"Permissions" on page 220

Resource Tree Pane

This tab displays the instances and resources available within each BSM context for which you set permissions.

To access	Select **Admin > Platform > Users and Permissions > User Management > Permissions** tab.
	The types of resources displayed in the Resource Tree pane are:
	● Resource with instances 📁
	● Instances of a resource 📁
	Note: When a user defines or creates an instance of a resource, for example creates a Business Process profile, that user has **Full Control** permission on that resource instance and all of its child resources.
	● Resource without instances 🏢

Important information	● The **Business Service Management** resource refers to all contexts in 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 "Understanding Permissions Resources" on page 221.
Relevant tasks	"Configure Users and Permissions" on page 227
See also	"Understanding Permissions Resources" on page 221

User interface elements are described below:

UI Element (A-Z)	Description
🖳	An instance of a resource.
🏢	A resource without instances.
📁	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" below.
Settings	Applies specific permissions settings for configurations in your User Management session. Select from the following options:
	● **Apply permissions automatically when selecting another resource.** Selecting this option removes the necessity for clicking the **Apply Permissions** button after each operation. If this option is not selected, you must click **Apply Permissions** before going on to the next operation.
	● **Do not display warning message when revoking VIEW from resource.** When the view operation is removed from a resource for a user, that user has no access to the resource or to any of its child resources or instances. Therefore, by default, a warning message appears when removing view permissions. Selecting this option will disable that warning message.
	Note: When you select the settings for applying permissions, the options selected apply only to the current BSM session.

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 Diagnostics.
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	"Configure Users and Permissions" on page 227
See also	• "Understanding Permissions Resources" on page 221
	• "User Management Roles Applied Across BSM" on page 243

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 243.

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	"Configure Users and Permissions" on page 227
See also	• "Understanding Permissions Resources" on page 221
	• "User Management Operations" on page 272

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.

UI Element (A-Z)	Description
Granted from Group/Roles/Parent	Displays those permissions that have been granted from either a group, a role, or a parent resource. **Note:** • You cannot remove any of these permissions individually, but you can grant additional permissions. • If you want to remove permissions that are granted from a group, role or parent resource, you must make the change at the group, role or parent resource level.
Inherit	Select the check box in the **Inherit** column for the operation to be inherited to all the child resources within the selected resource. **Note:** • The **Inherit** check box is enabled only for selected resources. • By default, the **Inherit** check box is selected when you assign an operation to specific resource instances. You can remove the **Inherit** option to prevent the operation from being inherited to all the child resources within the selected resource.
Operation	The operations that can be assigned to a group or user for the selected resource or instances. For details on the available operations, see "User Management Operations" on page 272.

Chapter 22

Recipient Management

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 "Setting Up an Alert Delivery System" on page 369.

- **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" on page 367.

For details on where to configure and manage recipients, see "Recipients Page" on page 301.

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 301.

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

   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.

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.

   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.

Property Name	Property Value	Description
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.

Recipient Management User Interface

This section includes:

- "Attach Recipient to a User Dialog Box" below

- "Recipients Page" below

- "New or Edit Recipient Dialog Box" on page 303

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** [icon] button in the Recipient page.
See also	"Group and User Hierarchy" on page 225

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	• 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 291.
	• 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 298
See also	"Recipient Management" on page 297

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 the next page.
✏	**Edit selected recipient.** Opens the Edit Recipient dialog box. For details, see "New or Edit Recipient Dialog Box" on the next page.
✖	**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 the previous page.
👤	**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.

UI Element (A-Z)	Description
Linked User	The name of the user linked to the recipient. **Important:** Cannot exceed 49 characters. **Syntax Exceptions:** The following characters are not supported: ` ~ ! @ # $ % ^ & * - + = [ ] { } \ | / ? . , " ' : ; < >
Pager	The pager numbers of the recipient. **Syntax Exceptions:** • The following characters are not supported: @ & " ' ... • The following special characters are allowed: ( ) - _ + = [ ] { } | : ; < > . ,
Recipient Name	The name of the recipient. **Important:** Cannot exceed 49 characters. **Syntax Exceptions:** The following characters are not supported: ` ~ ! @ # $ % ^ & * - + = [ ] { } \ | / ? . , " ' : ; < >
SMS	The SMS numbers of the recipient. **Syntax Exceptions:** • The following characters are not supported: @ & " ' ... • The following special characters are allowed: ( ) - _ + = [ ] { } | : ; < > . ,

New or Edit Recipient Dialog Box

This tab enables you to define recipients their email, pager and SMS, and the template to use to send alert notices to those recipients.

To access	You can also access this page from: • Select **Admin > Platform > Recipients > Recipient Management**, and click ✳️. • Select **Admin > Platform > Users and Permissions > User Management**, select a user, and click the **Recipient** tab. • Select **Admin > Personal Settings > Recipient**. • Click the **New Recipient** button in the **Templates and Recipients** page in the Create New Alert wizard for CI Status alerts. For details, see Templates and Recipients Page in the BSM User Guide. • 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 the BSM User Guide. • Click the **Create Recipient** button in the Attach Recipient dialog box for event-based alerts. For details, see Attach Recipients Dialog Box in the BSM User Guide. • Click the **New Recipient** button in the **Report Manager Main** page. For details, see Report Manager Main Page in the BSM User Guide.
Important information	• How you access the Recipients page and what you see in the page depends on your user's permissions. For details, see "Permissions Tab (User Management)" on page 291. • 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 298
See also	"Recipient Management" on page 297

User interface elements are described below:

UI Element (A-Z)	Description
👤	**Attach user to selected recipient.** Select a recipient in the list of and click the button to open the Attach Recipient to a User dialog box where you can select the appropriate user. For details, see "Attach Recipient to a User Dialog Box" on page 301. **Note:** This button is displayed only when you access the dialog box from **Admin > Platform > Users and Permissions > User Management**.

UI Element (A-Z)	Description
	Detach user from selected recipient. Detaches the current recipient from the corresponding user (listed in the page). A confirmation message is issued. **Note:** This button is displayed only when you access the dialog box from **Admin > Platform > Users and Permissions > User Management**.
	Delete the recipient attached to the selected user. Detaches the recipient from the user and deletes the recipient. **Note:** This button is displayed only when you access the dialog box from **Admin > Platform > Users and Permissions > User Management**.
	Update selected recipients email address from LDAP. This icon appears only if LDAP is connected to the BSM application. Click to synchronize the user data, meaning that the email information stored in the User Repository for the specific user updates the email recipient information corresponding to the user linked to the recipient.
EUM Alert notification template	Select the template you want to use for the EUM alert notification, or any custom template already created. **Note:** When you change the selection in the **EUM Alertnotification 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 Alertnotification 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 Alertnotification template** field in the top part of the page, the changes are propagated to the Email, Pager, and SMS tabs in the same page and the **Mixed Value** button is cleared. For details on EUM alert notification templates and creating custom templates, see "How to Configure EUM Alerts Notification Templates" on page 391. **Note:** This field is relevant only for event-based alerts. For details on alert notification templates and creating custom templates, see "Notification Templates Page" on page 397. **Note:** • The default template is **LONG**. • For details on the parameters displayed in each template, see "Default Notification Templates" on page 311. • 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	This field is displayed only when you access this page from: • **Admin > Platform > Users and Permissions > User Management**, select a user in the tree and click the **Recipient** tab. • **Admin > Personal Settings > Recipient**.
Recipient name	The name of the recipient. **Important:** Cannot exceed 49 characters. **Syntax Exception:** The following characters are not supported: ` ~ ! @ # $ % ^ & * - + [ ] { } \ | / ? " ' < >
Schedule for receiving alerts	Enabled if you selected the **Per notification method** scheduling option for the recipient in the **Schedule for Receiving Alerts** in the General tab. Select: • **Mixed value.** When you change the selection in the **EUM Alertnotification 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 Alertnotification 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 Alertnotification template** field in the top part of the page, the changes are propagated to the Email, Pager, and SMS tabs in the same page and the **Mixed Value** button is cleared. • **All Day.** If you want the recipient to receive email messages all day. • **From... to.** If you want the recipient to receive email messages during the specified time period. The time range is calculated based on the GMT offset selected for the recipient. Scheduled reports are sent based on the schedule configured in the Scheduled Reports page and not on the schedule configured for the recipient. For details, see How to Schedule a Report in the BSM User Guide.

UI Element (A-Z)	Description
Time zone	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.
	Note:
	• 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.
	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 the BSM User Guide.
	• 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.
	• Half time zones (also known as offset time zones) are not supported.

Communication Method Area

Important information	This area includes the following tabs:
	• "Email Tab" below
	• "SMS Tab" on page 309
	• "Pager Tab" on page 310

Email Tab

Enables you to specify multiple email addresses for the recipient, the type of notification template, which overrides the notification template selected in the global level in the page, the schedule for sending email notifications, and the security certificate if necessary.

To access	Select **Admin > Platform > Users and Permissions > User Management**, select a user in the tree and click the **Recipient** tab. In the Communication Method pane for the user, click the **Email** tab.
Important information	Only those recipients who have been configured to receive email can be selected to receive scheduled reports and are listed in Available Recipients when configuring scheduled reports.
	Note: The text displayed in email messages can only be in 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.

User interface elements are described below:

UI Element (A-Z)	Description
Email Addresses	Enter one or more email addresses. Separate multiple entries with a semi-colon (;).
Enable secure mail	Select this option if you want the recipient to receive encrypted mail. You must then copy, into the text box below the option, the contents of the certificate that the recipient uses to secure incoming email messages.
	Note:
	● The encrypted mail option is supported only for alerts. Encrypted mail is not supported for scheduled reports or subscription 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.
EUM Alert notification template	Select the template you want to use. For details, see "EUM Alerts Notification Templates" on page 389.
	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.
Schedule for receiving Email notifications	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 303.

SMS Tab

This tab enables you to specify the SMS (short message service) service provider, the SMS numbers, the type of notification template, which overrides the notification template selected in the global level in the page, and the schedule for sending alert notifications to the SMS.

To access	Select **Admin > Platform > Users and Permissions > User Management**, select a user in the tree and click the **Recipient** tab. In the Communication Method pane for the user, click the **SMS** tab.
Important information	SMS is a text messaging service provided by most GSM-based cellular phone providers. SMS messages are useful to notify staff who are mobile, or who do not have email or pager access. Note that the maximum message length of SMS text messages is generally 160 characters. **Note:** You can use a pager or an SMS service provider that does not appear on the default list. For details, see "How to Add a Custom Pager or SMS Service Provider" on page 299.

User interface elements are described below:

UI Element (A-Z)	Description
EUM Alert notification template	Select the template you want to use. For details, see "EUM Alerts Notification Templates" on page 389. **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.

UI Element (A-Z)	Description
Provider	Select an SMS service provider from the list: • **Genie-UK** • **Itineris** • **SFR-France** • **GoSMS-Israel** • **MtnSMS-Global** **Note:** If your provider does not appear on the default provider list, and the provider uses an email gateway, you can manually add your provider to BSM. For details, see "How to Add a Custom Pager or SMS Service Provider" on page 299.
Schedule for receiving SMS notifications	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 303.
SMS numbers	Type one or more SMS access numbers in the box. Separate multiple entries with a semi-colon (;).

Pager Tab

This tab enables you to specify the pager service provider, the pager numbers, the type of notification template, which overrides the notification template selected at the global level in the page, and the schedule for sending alert notification to the pager.

To access	Select **Admin > Platform > Users and Permissions > User Management**, select a user in the tree and click the **Recipient** tab. In the Communication Method pane for the user, click the **Pager** tab.
Important information	You can use a pager that does not appear on the default list. For details, see "How to Add a Custom Pager or SMS Service Provider" on page 299. **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 include, for example, Alert Name, Alert description, and KPI name.

User interface elements are described below:

UI Element (A-Z)	Description
EUM Alert notification template	Select the template you want to use. For details, see "EUM Alerts Notification Templates" on page 389. **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.
Pager Numbers	Enter one or more pager access numbers. Separate multiple entries with a semi-colon (;). **Note:** If your pager is numeric only, when creating an alert scheme in the Alert Wizard, you can only type a numeric user message.
Schedule for receiving pager notifications	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 303.
Type	Select a pager service provider. The following providers are supported: ● **MetroCall** ● **Arch** ● **AirTouch** ● **PageMci** ● **SkyTel** ● **PageNet** ● **PageMart** ● **AmeriPage** ● **Nextel** ● **PageOne**

Default Notification Templates

Important information	Each template enables you to display, in the notification, selected information that corresponds to specific parameters. For details on the parameters displayed in each template, see "Notification Template Properties Dialog Box" on page 393.

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 392.
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.

Chapter 23

Personal Settings

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" below.

- **Menu Customization.** For details, see "Menu Customization" below.

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 317.

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 318.

How to Customize 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 BSM Menus and Pages — Use-Case Scenario" on the next page.

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 318.

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 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 BSM Menus and Pages — Workflow" on the previous page.

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:
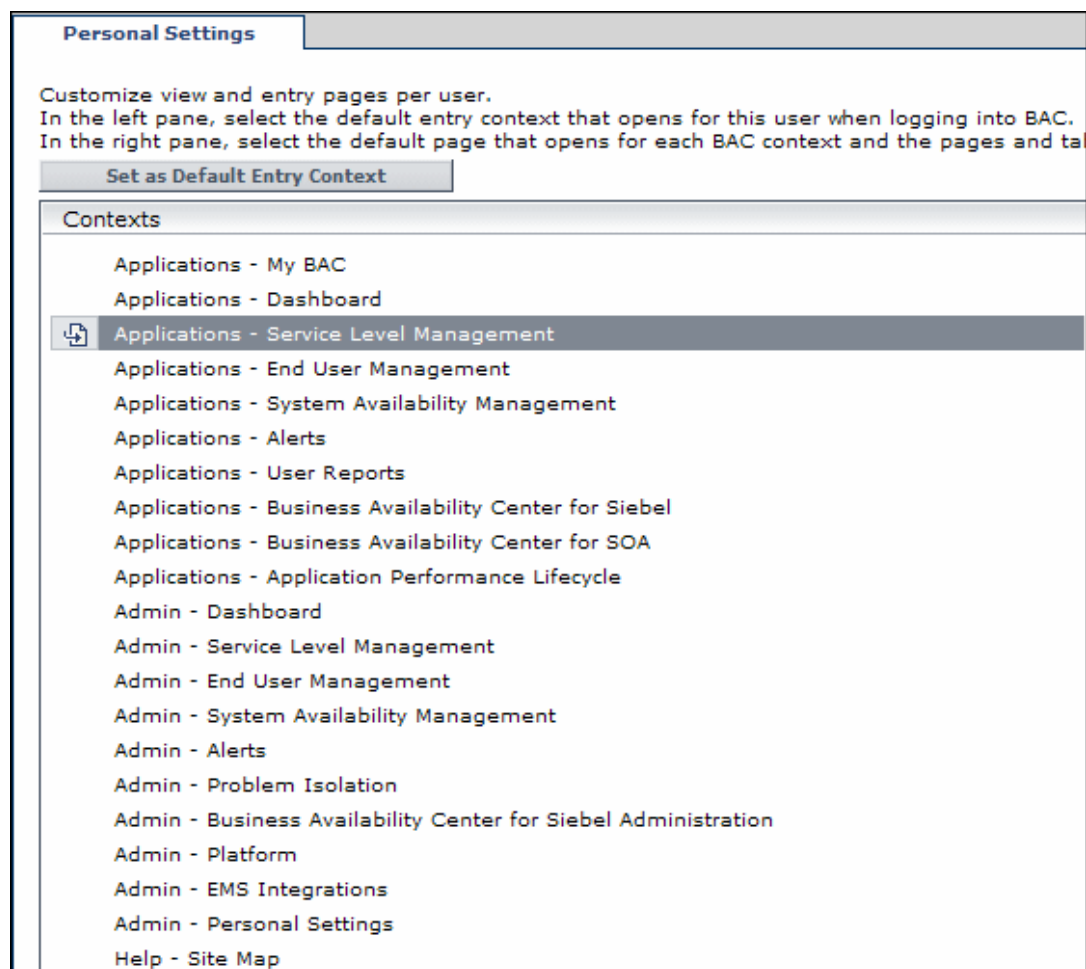
2. **Selecting Context Pages and Tabs**

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:
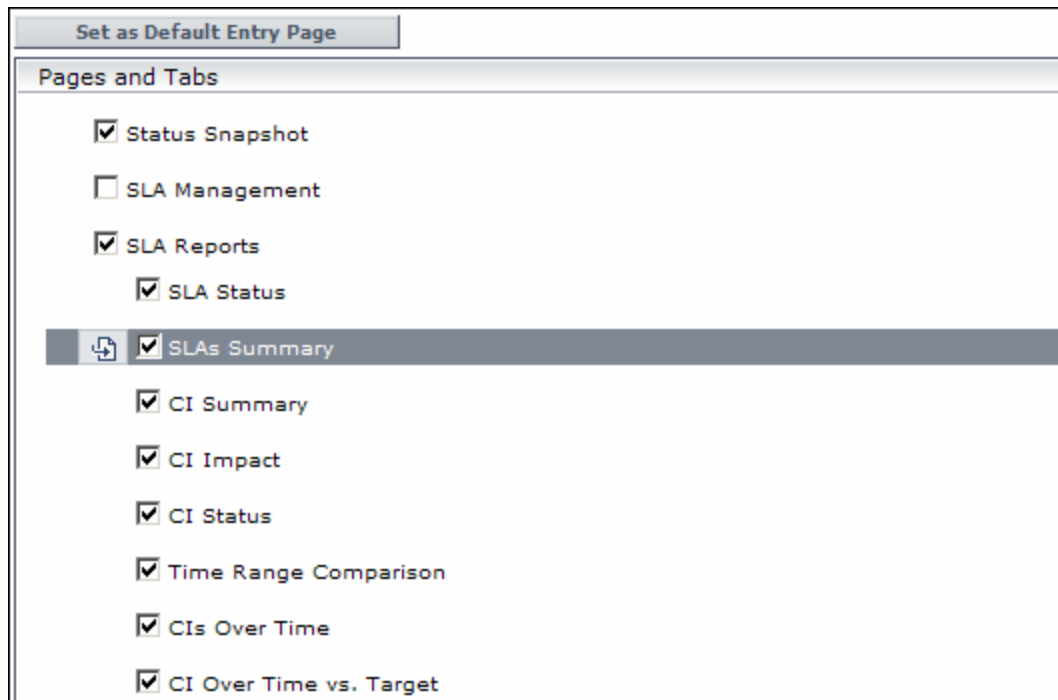
3. **Results**

   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:
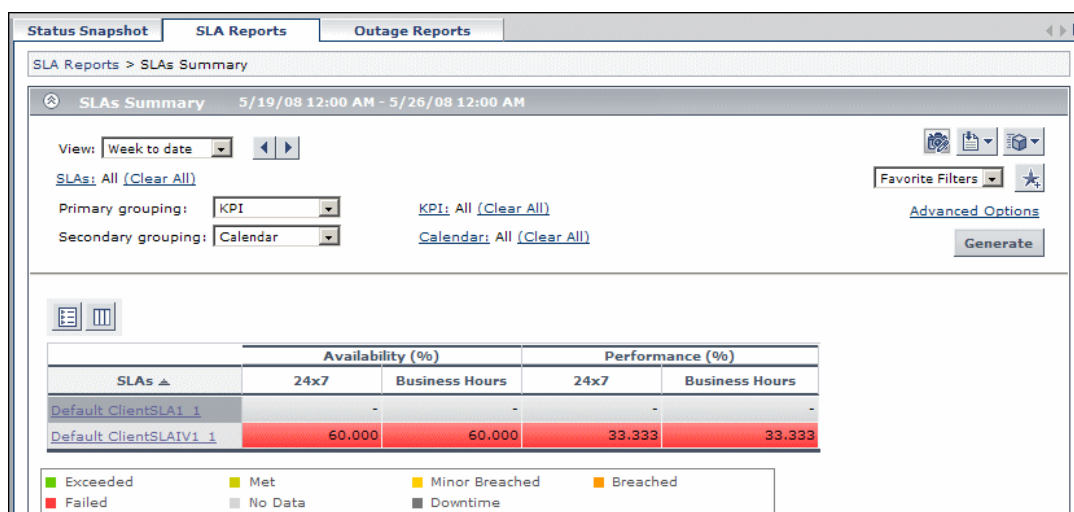
Personal Settings User Interface

This section includes:

- "User Account Page" below

- "Menu Customization Page" on the next page

- "Recipient Tab " on page 319

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	"Personal Settings" on page 313

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.
Select auto-refresh rate	Select the rate at which you want BSM to automatically refresh the browser and load the most up-to-date data from the database.
Time zone	Select the appropriate time zone, according to the user's location.

UI Element (A-Z)	Description

User mode	Select the user mode for the user, from the following options:
	
	● **Unspecified.** Leaves the user without a particular mode. Select this option if:
	
	    ■ 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.
	
	Note: For details on user modes, see KPIs for User Modes in the BSM Application Administration Guide.

User name	The user name for the user. **Notes:** ● The maximum number of characters you can enter is 50. ● All special characters are allowed except the following: " \ / [ ] : | < > + = ; , ? * % &

Menu Customization Page

This page enables you to customize the view and entry pages per user. You can specify:

● The default context that is displayed when logging into 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 BSM Menus and Pages — Workflow" on page 314
See also	"Personal Settings" on page 313

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: • 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	• 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.
Set as Default Entry Context	Click to set the selected context in the Contexts pane as the entry context that is displayed when the specified user logs into BSM. Note: The **Default Entry Context** icon appears next to the specified context.
Set as Default Entry Page	Click to assign the specified page or tab as the default page that opens for the context selected in the Contexts pane. **Note:** The **Default Entry Page** icon appears next to the specified page or tab.

Recipient Tab

This tab enables you to define recipients, their email, pager, and SMS information, and the template to use to send alert notices to those recipients.

For user interface details, see "New or Edit Recipient Dialog Box" on page 303.

Chapter 24

Authentication Strategies

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.

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 348.

Authentication strategies are configured in the Authentication Management Wizard. For details on the Authentication Management Wizard, see "Authentication Wizard" on page 327.

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 "Lightweight Single Sign-On Strategy" on page 338.

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 334.

All requests to client applications are channeled through the SSO authentication. The supported applications need to know only the name of the authenticated user.

For details on the IDM-SSO authentication strategy, see "Identity Management Single Sign-On Authentication" on page 343.

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 354.

You enable and disable LDAP using the Authentication Management Wizard. For details, see "Authentication Wizard" on page 327.

Smart Card Authentication

BSM supports user authentication using smart cards. If smart card authentication is configured, you cannot log in without a valid smart card.

To access the Smart Card Authentication Configuration Wizard:

Select **Admin > Platform > Users and Permissions > Authentication Management > Smart Card Authentication Configuration >** button

Learn More

Smart Card Authentication

Smart cards are physical devices used to identify users in secure systems. These cards can be used to store certificates both verifying the user's identity and allowing access to secure environments.

BSM can be configured to use these certificates in place of the standard model of each user manually entering a user name and password. You define a method of extracting the user name from the certificate stored on each card.

When using smart cards with BSM, users can only log in using the smart card. The option of logging in by manually typing in your username and password is locked for all users unless smart card configuration is disabled.

Tasks

Enable or Disable Smart Card Authentication

Smart cards are both enabled and disabled on the BSM Gateway and Data Processing servers by using the Smart Card Authentication Configuration Wizard. This wizard is only a part of the overall workflow for configuring smart card authentication in your BSM environment. For more details, see the Smart Card Authentication Configuration Guide.

> **Note:** Your machine must have the openssl command installed. This is included as part of the Apache installation included on Windows BSM environments. In Linux environments, it is sometimes included. To check if this is installed on your machine run
>
> **usr/bin/openssl**
>
> If you do not have this command, install it and make sure you can execute it from any path before configuring smart card authentication.

Emergency Disable of Smart Card Authentication

> **Note:** This procedure should only be used if you cannot access BSM normally.

If you cannot log in to BSM using any smart card and want to disable smart card authentication, run the following batch file from any BSM Gateway or Data Processing Server:

- **Windows:** <BSM Installation Directory>\bin\RevertHardening.bat

- **Linux:** <BSM Installation Directory>/bin/RevertHardening.sh

When the batch file is complete, restart all BSM Gateway Servers to activate the change.

Manually Configure Reverse Proxy for Smart Cards

This procedure differs depending on whether your reverse proxy is using the IIS or Apache web server. This procedure describes the general settings that are required, but you may need to refer to the web server documentation for the details. It must be performed before you restart your BSM Gateway servers to enable smart card authentication.

For the IIS web server:

1. Prerequisite: IIS is already configured to require client certificate

2. Configure the reverse proxy to forward the encoded client certificate in the header **CLIENT_ CERT_HEADER**.

For the Apache web server:

1. Prerequisite: Apache is already configured to require a client certificate.

2. In httpd.conf, enable the **mod_headers.so**

3. In httpd-ssl.conf, add the following line before </VirtualHost>:

   requestHeader set CLIENT_CERT_HEADER "%{SSL_CLIENT_CERT}s"

UI Descriptions

Smart Card Authentication Configuration Wizard

This wizard guides you through the process of enabling and disabling smart card authentication configuration with BSM.

To access the Smart Card Authentication Configuration Wizard:

Select **Admin > Platform > Users and Permissions > Authentication Management > Smart Card Authentication Configuration >** button

Notes and Limitations

- User names are case sensitive

- When smart card authentication is enabled, the JXM console can only be accessed directly from the BSM servers.

- When creating an admin user as directed in the smart card authentication wizard, make sure you enter a secure password even though no password is required for authentication with smart cards. If smart card authentication is disabled, the user will still exist on the system and if an insecure password is defined it could pose a security risk.

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:

- "Authentication Management Page" below

- "Authentication Wizard" on the next page

Authentication Management 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	Access to the Authentication Management page is dependent on the following permission levels: - **View.** Enables viewing the Authentication Management Page. - **Change.** Enables you to access the Authentication Management Wizard and change configurations. The **Configure** button is enabled. You configure permissions on the Users and Permissions interface. For details, see "Permissions" on page 220.
See also	- "Authentication Strategies" on page 320 - "Infrastructure Settings" on page 84

User interface elements are described below:

UI Element (A-Z)	Description
Configure	Click to open the Authentication Wizard and configure an authentication strategy. For details on the Authentication Wizard, see "Authentication Wizard" on the next page. 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. There is a separate **Configure** button for **Smart Card Authentication Configuration**.

UI Element (A-Z)	Description
Lightweight Directory Access Protocol Configuration	The section displays: • **Name.** The name of the **Lightweight Directory Access Protocol** parameter. • **Value.** The value of the **Lightweight Directory Access Protocol** parameter as configured in the wizard.
Single Sign-On Configuration	The section displays: • **Name.** The name of the **Single Sign-On** parameter. • **Value.** The current value of the **Single Sign-On** parameter as configured in the wizard.
Smart Card Authentication Configuration	The section displays: • **Name.** The name of the **Smart Card Authentication Configuration** parameter. • **Value.** The current value of the **Smart Card Authentication Configuration** parameter as configured in the wizard.

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: 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: **Authentication Wizard** > "Single Sign-On Page" on the next page > ("SAML2 Configuration Dialog Box" on page 330) > "LDAP General Configuration Page" on page 332 > ("LDAP Vendor Attributes Dialog Box" on page 334) > "LDAP Users Synchronization Configuration Page" on page 335 > "Summary Page" on page 336

Single Sign-On Page

This wizard page enables you to configure a Single Sign-On strategy. The elements displayed on the Single Sign-On page are determined by the Single Sign-On mode you choose.

Important information	• If a value in one of the wizard fields is blank or invalid, an error icon ![error icon] is displayed on the field's cell. You can view a description of the error in one of the following ways: ■ Hover over the error icon to display a tooltip with the error message. ■ Access the log file **<HPBSM>/log/EJBContainer/login.log.**

User interface elements are described below:

UI Element (A-Z)	Description
Disabled	Select to disable the Single Sign-On (SSO) authentication strategy.
IdentityManagement	Select to configure the Identity Management Single Sign-On (IDM-SSO) authentication strategy. For details on the elements displayed this page, see below. For details on this topic, see "Identity Management Single Sign-On Authentication" on page 343. **Note:** If you have selected this option, LDAP can be configured only for group mapping and not for authentication.
Lightweight	Select to configure the Lightweight Single Sign-On (LW-SSO) authentication strategy. For details on the elements displayed on this page, see below. For details on this topic, see "Lightweight Single Sign-On Strategy" on page 338.

Identity Management Single Sign-On (IDM-SSO) Configuration

User interface elements are described below:

UI Element (A-Z)	Description
![error icon]	Indicates that the value in the specified field is empty or invalid. Hover over this icon to view a tooltip describing the error.

UI Element (A-Z)	Description
Header Name	Enter the header name for the token name passed by the Identity Management Single Sign-On. **Example:** `sso_user` **Note:** 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.
Enable SAML2 authentication schema	Select to enable authentication using the Security Assertion Markup Language 2.0 protocol.
HP Business Service Management Domain	Enter the relevant BSM domain, to be used for token creation. This field may be needed for multi-domain support and normalized URLs when the domain cannot be parsed automatically, for example when using aliases. **Example:** `devlab.ad`
Parse automatically	Click to parse the BSM domain automatically.
SAML2 Settings	Click to set parameters in the SAML2 Configuration Dialog Box.
Token Creation Key (initString)	Enter an initString value, used for encryption and decryption of the LW-SSO token. If changing this value, remember to set initString to the same value in all HP products participating in LW-SSO integration. **Example:** `Xy6stqZ`

UI Element	Description
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** button ❌.

SAML2 Configuration Dialog Box

This dialog box page enables you to modify the SAML authentication parameters for your Lightweight Single Sign-On configuration.

To access	In the Authentication Management Wizard, navigate to the Single Sign-On page, select **Lightweight**, and select the **Enable SAML2 authentication schema** check box. Click **SAML2 Settings** to open the SAML2 Configuration dialog box. The SAML2 Configuration dialog box consists of the following sections: • **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	• BSM comes with SAML enabled by default. If you want to disable SAML authentication, clear the **Enable SAML2 authentication schema** check box.

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	The filename of the keystore in BSM. ● 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	Select for the Lightweight Single Sign-On framework to search for the keystore in the classpath. **Note:** When this option is selected, you enter only the name of the actual keystore file in the **Keystore filename** field.
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
Look for keystore in classpath	Select for the Lightweight Single Sign-on framework to search for the keystore in the classpath. **Note:** When this option is selected, you enter only the name of the actual keystore file in the **Keystore filename** field.
Keystore filename	The filename of the keystore in BSM. ● When **Look for keystore in classpath** is not selected, this value must be the full path of the keystore's location, for example: `C:\mystore\java.keystore.` ● When **Look for keystore in classpath** is selected, this value must be just the file name of the keystore, for example: `java.keystore.`
Keystore password	The password of the public key used for decryption during the SAML authentication request.

LDAP General Configuration Page

This wizard page enables you to use an external LDAP server to store authentication information (user names and passwords) and to enable user synchronization between LDAP users and BSM users.

To access	Select **Admin > Platform > Users and Permissions > Authentication Management**, and click **Configure**. Navigate to the **LDAP General Configuration** page. The available LDAP modes are: • **Enabled** • **Disabled** **Note:** LDAP cannot be used for authentication when you choose **IdentityManagement** on the Single Sign-On Configuration page of the wizard.
Important information	• When configuring LDAP parameters, consult your LDAP Administrator for assistance.

LDAP General Configuration Section

User interface elements are described below:

UI Element (A-Z)	Description
✖	Indicates that the value in the specified field is empty or invalid. You can view a description of the error in one of the following ways: • Hover over the error icon to display a tooltip with the error message. • Access the log file **<HPBSM root directory>\log\EJBContainer\login.log**.
Advanced	Opens the LDAP Vendor Attributes dialog box enabling you to modify configurations for the selected LDAP vendor. For details, see "LDAP Vendor Attributes Dialog Box" on page 334.
Distinguished Name (DN) Resolution	Select to enable entering LDAP search user credentials. **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.
Distinguished Name of Search-Entitled User	Defines the Distinguished Name (DN) of a user with search privileges on the LDAP directory server. **Note:** Leave this entry blank for an anonymous user.

UI Element (A-Z)	Description
LDAP server URL	Enter the URL of the LDAP (or, for Active Directory users, Global Catalog [AD GC]) server. To represent different trees in the same forest, enter multiple DNs, separated by semicolons. To allow failover, enter multiple LDAP (AD GC) server URLs, separated by semicolons. The required format is: **ldap://machine_name:port/scope??sub** ● 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. ● BSM ignores the attribute between the two question marks, if one exists. ● When the port number and scope value are empty, default values are used. ■ **Default port number for regular communication:** 389 ■ **Default port number for SSL communication:** 636 ■ **Default scope value:** sub **Examples:** Single DN, single LDAP server: `ldap://my.ldap.server:389/ou=People,o=myOrg.com??sub` Multiple DNs: `ldap://my.ldap.server:389/ou=People, o=myOrg.com??sub; ldap://my.ldap.server:389/ou=Staff,o=my2ndOrg.net??sub` Multiple LDAP servers: `ldap://my.ldap.server:389/ou=People, o=myOrg.com??sub; ldap://my.2ndldap.server:389/ou=People,o=myOrg.com??sub` **Note:** If you receive a red X after entering the URL with the following popup text: ERROR - sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target This means that you need to establish trust to the LDAP server. For details, see "How to Secure Communication Between the LDAP Server and BSM Server Over SSL" on page 358

UI Element (A-Z)	Description
LDAP vendor type	Enter the LDAP vendor you are using. Select from: ● Common LDAP ● Microsoft Active Directory ● Other **Note:** If you click **Advanced** and modify the LDAP Vendor Attribute settings, the value of this field automatically changes to **Other**.
Password of Search Entitled User	Defines the password of the user entitled to search the LDAP server entities for groups. **Note:** Leave this entry blank for an anonymous user.

Test DN Resolution Section

Enables you to verify that both the configured LDAP parameters and the credentials of a specified user are valid.

User interface elements are described below:

UI Element (A-Z)	Description
Password	The password of the user whose credentials are entered in the **UUID** field. **Note:** This field is optional. If left empty, anonymous user is used.
Test	Tests the LDAP configuration and user credentials validity. A message is displayed indicating whether or not the validation was successful.
UUID	The actual login name (Unique User ID) of the LDAP user you want to verify.

LDAP Vendor Attributes Dialog Box

This 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	● 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**.

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	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. **Note:** The filter should be as narrow as possible and include only users who require access to BSM.
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 Management**, and click **Configure**. Navigate to the **LDAP Users Synchronization Configuration** page.
Important information	• This page is enabled only if the LDAP General Configuration page has been configured correctly.

User interface elements are described below:

UI Element (A-Z)	Description
	Indicates that the value entered in the specified field is invalid.

UI Element (A-Z)	Description
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 354.
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.

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.

UI Element (A-Z)	Description
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.

Chapter 25

Lightweight Single Sign-On Strategy

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 321.

You can configure LW-SSO in BSM using the Authentication Wizard. For details on the Authentication Wizard, see "Authentication Wizard" on page 327.

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 25.

For details on limitations of working with LW-SSO, see "LW-SSO Authentication – General Reference" on page 361.

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 327), 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
```

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.

Troubleshooting and Limitations

This section describes troubleshooting and limitations for Lightweight Single Sign-On.

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 the previous page.

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 354.

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.

Chapter 26

Identity Management Single Sign-On Authentication

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 327.

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.

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/*
- /mcrs/*
- /MercuryAM/*
- /odb/*
- /opal/*
- /opr-admin-server/*
- /opr-console/*
- /opr-gateway/*
- /opr-web/*
- /ovpm /*
- /topaz/*
- /topazSettings/*
- /tv/*
- /tvb/*
- /ucmdb-ui/*
- /uim/*
- /utility_portlets/*
- /webinfra/*

> **Examples of URL with form authentication**
>
> - The following URL verifies that the IDM header is correct:
>
>   `https://<gateway server>/topaz/verifyIDM.jsp?headerName=sm_user`
>
>   **Expected Result:** The system displays the user name of the current user (provided that SM authentication was performed prior to this action).

> ▪ The following URL shows values of all cookies in the session:
>
> ```
> https://<gateway server>/topaz/DumpSession.jsp
> ```
>
> **Expected Result:** The system displays a table of all cookies in the user session and their corresponding values.

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.

> **Example of URL with basic authentication**
>
> - The following URL is used by data collectors to establish a connection to BSM:
>
> ```
> https://<gateway server>/topaz/topaz_api/api_getsystemkey.asp
> ```
>
> **Expected Result:** The system displays the basic authentication window followed by a value, for example -7.

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:

- /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/services/technical/time

- /topaz/static

- /topaz/stylesheets

- /tvb/rest

- /ucmdb-api

If you are using a Load Balancer, you should also **unprotect** the following resources:

- /topaz/topaz_api/loadBalancerVerify_core.jsp

- /topaz/topaz_api/loadBalancerVerify_centers.jsp

Example of URL with unprotected authentication

- The following URL is used by the TV Component:

```
https://<gateway server>/topaz/services/technical/time
```

Expected Result: the system displays the time in XML format without a request for authentication.

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 use **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).

Chapter 27

LDAP Authentication and Mapping

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 327.

For details on securing communication between an LDAP server and your BSM server over SSL, see "How to Secure Communication Between the LDAP Server and BSM Server Over SSL" on page 358.

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 Management 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 353.

> **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 manually assign users 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 357.

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:
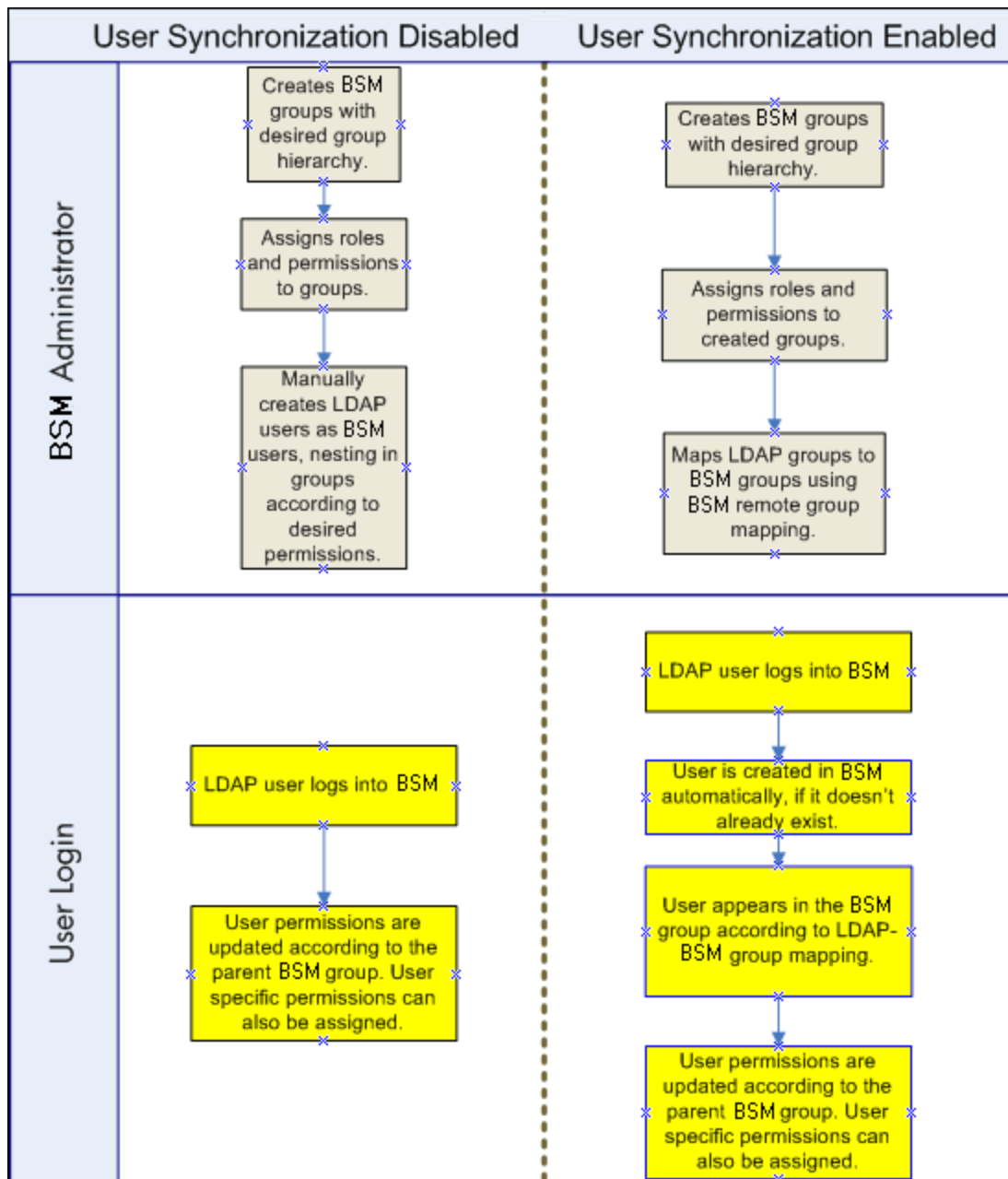
For an LDAP user to log into BSM, he must match the criteria defined in the **Users filter** field on the LDAP Advanced General Configuration dialog box in the Authentication Wizard. For details on the LDAP General Configuration page, see "LDAP Vendor Attributes Dialog Box" on page 334.

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 359.

For details on synchronizing LDAP users with BSM users, see "How to Map Groups and Synchronize Users" on page 354.

For details on synchronizing groups after upgrading from a previous version of BSM, see "Synchronizing Users After Upgrading from a Previous Version of BSM" below.

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 356.

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 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.

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:

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 327.

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 288.

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.

Mapping local groups to remote groups:
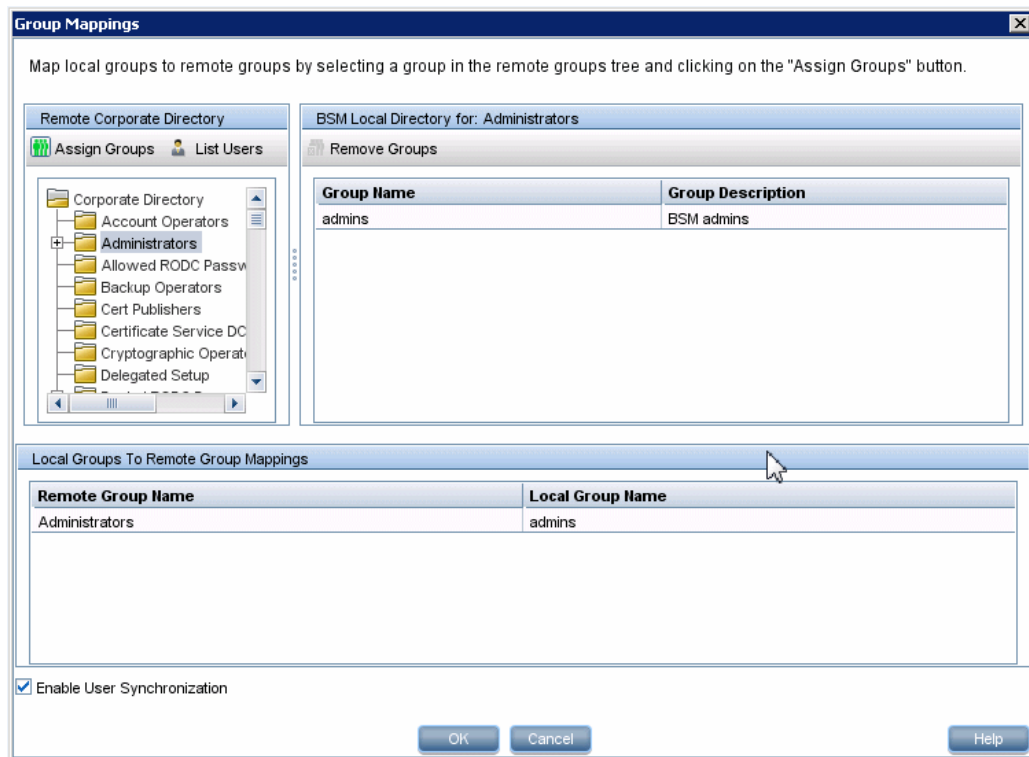
4. **Enable User Synchronization**

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.

- 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 **User Management > LDAP > Group Mappings** user interface.

For details on synchronizing users through the Authentication Wizard, see "LDAP Users Synchronization Configuration Page" on page 335.

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 earlier than 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 354.

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 Management**.

2. Click the **Configure** button to activate the Authentication Management 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 Secure Communication Between the LDAP Server and BSM Server Over SSL

1. If the LDAP server requires a secure connection perform the following steps:

   a. Obtain root CA certificate from the Certificate Authority that issued LDAP server certificate.

   b. Import it into the truststore of JVM on each BSM gateway (for both JRE and JRE64).

   c. Restart the BSM gateway servers.

   Example

   ```
   cd C:\HPBSM\JRE64\bin
   keytool -import -trustcacerts -alias myCA -file c:\RootCA.cer -
   keystore ..\lib\security\cacerts
   cd C:\HPBSM\JRE\bin
   keytool -import -trustcacerts -alias myCA -file c:\RootCA.cer -
   keystore ..\lib\security\cacerts:
   ```

2. Verify that communication between the LDAP server and the BSM server is valid over SSL, using the Authentication Management Wizard, as follows:

   a. Navigate to the Authentication Management Wizard by selecting **Admin > Platform > Users and Permissions > Authentication Management**, click **Configure** and navigate to the LDAP General page.

   b. Enter the URL of your LDAP server, according to the following syntax: ldaps://machine_name:port/<scope>??sub.

      Ensure that the protocol is ldaps://, and the port number is configured according to the SSL port, as configured on the LDAP server (default is 636).

   c. Test your configuration on the LDAP General Configuration page by entering the UUID and password of a known LDAP user in the relevant fields. Click Test to authenticate the user. For details, see "LDAP General Configuration Page" on page 332.

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 Management 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.

Troubleshooting and Limitations

This section describes troubleshooting and limitations for Lightweight Directory Access Protocol (LDAP) Authentication.

- When setting LDAP server URL: if you see a red cross containing the following error:

  ERROR - sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target

  You have not yet configured a secure connection to the LDAP server.

- 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**.

Chapter 28

LW-SSO Authentication – General Reference

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.

- **LW-SSO Token Expiration**
  The LW-SSO Token's expiration value determines the application's session validity. Therefore, its expiration value should be at least the same value as that of the application session expiration value.

- **Recommended Configuration of the LW-SSO Token Expiration**
  Each application using LW-SSO should configure token expiration. The recommended value is 60 minutes. For an application that does not require a high level of security, it is possible to configure a value of 300 minutes.

- **GMT Time**
  All applications participating in an LW-SSO integration must use the same GMT time with a maximum difference of 15 minutes.

- **Multi-domain Functionality**
  Multi-domain functionality requires that all applications participating in LW-SSO integration configure the trustedHosts settings (or the **protectedDomains** settings), if they are required to integrate with applications in different DNS domains. In addition, they must also add the correct domain in the **lwsso** element of the configuration.

- **Get SecurityToken for URL Functionality**
  To receive information sent as a **SecurityToken for URL** from other applications, the host application should configure the correct domain in the **lwsso** element of the configuration.

HP Business Service Management (9.22)

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.

- **Level of authentication security.** The application that uses the weakest authentication framework and issues a LW-SSO token that is trusted by other integrated applications determines the level of authentication security for all the applications.

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

- **Symmetric encryption implications.** LW-SSO uses symmetric cryptography for issuing and validating LW-SSO tokens. Therefore, any application using LW-SSO can issue a token to be trusted by all other applications sharing the same **initString** parameter. This potential risk is relevant when an application sharing an initString either resides on, or is accessible from, an untrusted location.

- **User mapping (Synchronization).** The LW-SSO framework does not ensure user mapping between the integrated applications. Therefore, the integrated application must monitor user mapping. We recommend that you share the same user registry (as LDAP/AD) among all integrated applications.

  Failure to map users may cause security breaches and negative application behavior. For example, the same user name may be assigned to different real users in the various applications.

  In addition, in cases where a user logs onto an application (AppA) and then accesses a second application (AppB) that uses container or application authentication, the failure to map the user will force the user to manually log on to AppB and enter a user name. If the user enters a different user name than was used to log on to AppA, the following behavior can arise: If the user subsequently accesses a third application (AppC) from AppA or AppB, then they will access it using the user names that were used to log on to AppA or AppB respectively.

- **Identity Manager.** Used for authentication purposes, all unprotected resources in the Identity Manager must be configured with the **nonsecureURLs** setting in the LW-SSO configuration file.

Troubleshooting and Limitations

Known Issues

This section describes known issues for LW-SSO authentication.

- **Security context.** The LW-SSO security context supports only one attribute value per attribute name.

  Therefore, when the SAML2 token sends more than one value for the same attribute name, only one value is accepted by the LW-SSO framework.

  Similarly, if the IdM token is configured to send more than one value for the same attribute name, only one value is accepted by the LW-SSO framework.

- **Multi-domain logout functionality when using Internet Explorer 7.** Multi-domain logout functionality may fail when the browser used is Internet Explorer 7 and the application is invoking more than three consecutive HTTP 302 redirect verbs in the logout procedure.

  In this case, Internet Explorer 7 may mishandle the HTTP 302 redirect response and display an **Internet Explorer cannot display the webpage** error page instead.

  As a workaround, it is recommended to reduce, if possible, the number of application redirect commands in the logout sequence.

Limitations

Note the following limitations when working with LW-SSO authentication:

- **Client access to the application**.

  If a domain is defined in the LW-SSO configuration:

  - The application clients must access the application with a Fully Qualified Domain Name (FQDN) in the login URL, for example, http://myserver.companydomain.com/WebApp.

  - LW-SSO cannot support URLs with an IP address, for example, http://192.168.12.13/WebApp.

  - LW-SSO cannot support URLs without a domain, for example, http://myserver/WebApp.

  If a domain is not defined in the LW-SSO configuration: The client can access the application without a FQDN in the login URL. In this case, 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.

- 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 5

Reports and Alerts Administration

Chapter 29

Report Schedule Manager

This page enables you to edit, delete, resume, or pause scheduled reports.

To access	Select **Admin > Platform > Report Scheduling**
Important information	You cannot create a new schedule from the Report Schedule Manager. For details on creating schedules, see How to Schedule a Report in the BSM User Guide.

Caution: Scheduled reports place pressure on the system and can cause performance issues for users who are logged on. When possible, you should schedule reports for off hours when fewer users access the system. If your system does not have off hours, you should stagger reports at different times of the day to minimize the number of reports running simultaneously.

User interface elements are described below:

UI Element (A–Z)	Description
	Opens the Edit Schedule for the <Report Name> dialog box enabling you to edit the selected schedule. For details, see Creating a New Schedule Dialog Box in the BSM User Guide. **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 Creating a New Schedule Dialog Box in the BSM User Guide.
	Deletes the selected schedule.
	Resumes the selected schedule, this button is only available if the selected report has been paused.
	Pauses the selected schedule.
	Refreshes the Report Schedule Manager page.
	Resets the width of the columns to the default setting.
	Enables you to select columns to be visible in the table.
Generation Time	The time (in the indicated time zone) that the schedule is to be generated.

UI Element (A–Z)	Description
Recipients	The individuals configured in the Report Manager to receive the report or report item at scheduled intervals. For details on configuring Schedules, see Creating a New Schedule Dialog Box in the BSM User Guide.
Recurrence	The recurrence pattern for the selected schedule.
Report Name	The name of the report for which the schedule is configured.
Report Type	The type of report for which the schedule is configured.
Status	The status of the schedule. Possible values are: ● Active ● Paused

Chapter 30

Setting Up an Alert Delivery System

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 373.

Alert Recipients

Alerts can be configured to send notification to specified recipients. For task details on configuring recipients, see "Recipient Management" on page 297.

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 391.

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 372.

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 in the BSM User Guide.

- HP Service Manager automatically opens incidents when a CI Status alert is triggered in BSM. For details, see HP Service Manager in the BSM section of the Integrations tab in the HP Software Integrations site.

- **SLAs.** SLA status alerts are triggered by changes to an SLA's key performance indicator status. For details, see SLA Alerts Administration in the BSM User Guide.

- **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 End User Management Alerts Administration in the BSM User Guide.

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 Operations Manager in the BSM Platform section in the HP Software Integrations site.

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 the BSM User Guide.

- **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 the BSM User Guide.

- **EUMAlerts 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 the BSM User Guide.

  - **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 the BSM User Guide.

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" on page 201.

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 the BSM User Guide.

For task details, see "How to Set Up an Alert Delivery System" on page 373.

For user interface details, see "Downtime Management Page" on page 205.

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.

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.

Setting Up an Alert Delivery System - Flowchart
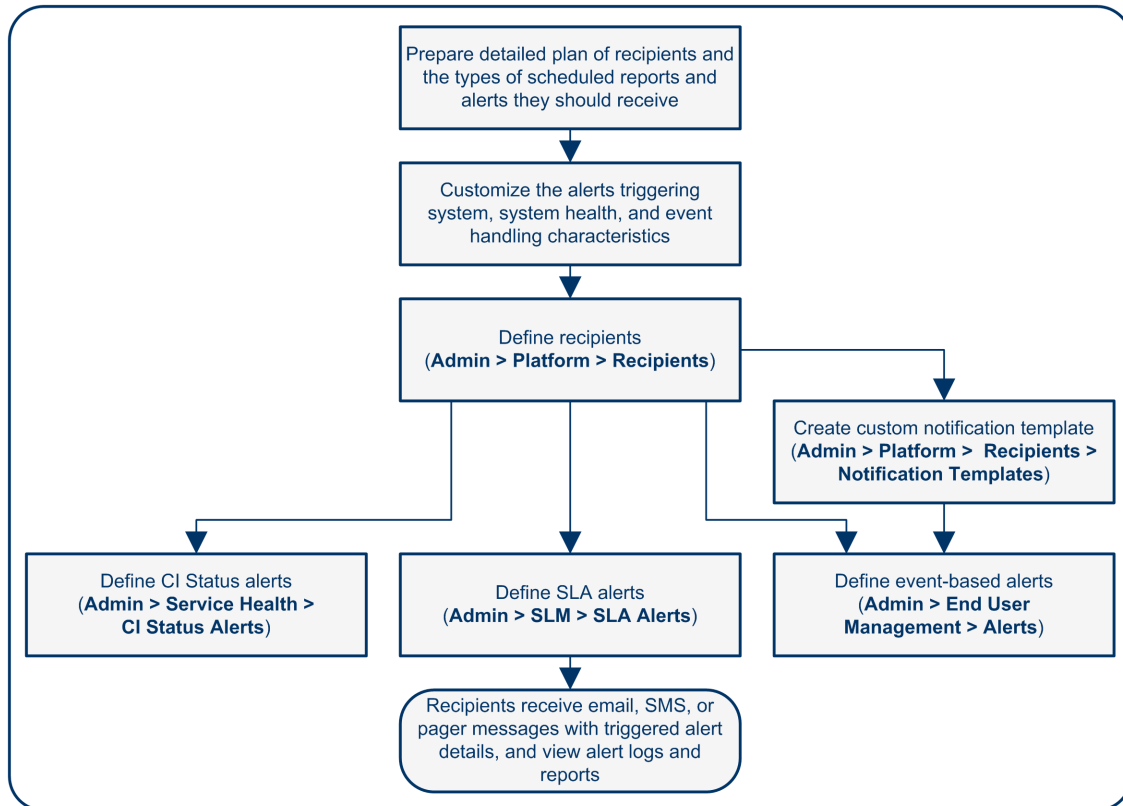
Plan the alert recipient requirements

Before you start, we recommend that you:

- 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 the previous page.

- 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 375.

Specify the appropriate user permissions

Specify the appropriate user permissions for the following. To set these permissions:

1. Select **Admin > Platform > Users and Permissions > User Management**.

2. Create or edit a user, and open the **Permissions** tab.

3. Select the required option from the Context drop-down list as described below.

- **The EUM alerts.**

  You can specify that a user can have a **View** or **Full Control** permission per application.

  - In the **End User Management** context, select **Business Service Management > Applications >** <Application> **> Alert**

  You must also specify the permission for the CEM event template.

  - 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.

  - In the **RTSM** context, select **Business Service Management > Views >** <view_name>.

- **The SLA alerts.**

  You can specify that a user can have an **Add, Change**, **View, Delete,** or **Full Control** permission per SLA.

  - 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.

  - 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.

  - 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 223.

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 371.

For user interface details, see "Downtime Management Page" on page 205.

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 the next page.

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 Management" on page 297.

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 391.

Set up to open an event in Operations Manager and Operations Management when an alert is triggered in BSM

You can set up to open events in Operations Manager and Operations Management when an alert is triggered in BSM. For details, see Operations Manager in the BSM section of the Integrations tab in the HP Software Integrations site.

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, see How to Create a CI Status Alert Scheme and Attach it to a CI in the BSM User Guide.

- **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 the BSM User Guide.

- **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 the BSM User Guide.

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.

To customize alerts:

1. Select **Admin > Platform** > **Setup and Maintenance** > **Infrastructure Settings**.
2. Select **Foundation > Alerting** and modify the required settings as described below.

Modify the way events are handled

You can modify the following parameters in the **Event handling** area:

Parameter	Does the Following
Acceptable event delay (minutes)	The system discards alerts after the number of minutes defined here.
Alert persistency during Downtime	If this option is set to **true**, the system does not reset the alert persistent state when an application goes into Downtime. This means that the system retains data and uses it when generating alerts after the Downtime ends. Applies to EUM alerts only.
Calculation persistency	If this option is set to **true**, if the system goes down, the system retains data and uses it when creating alerts when the system comes back up.

Modify the Alerting System Health parameters

You can modify the following parameters in the **System Health monitors** area:

Parameter	Does the Following
Error threshold for the notification queue monitor	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**.
Error threshold for the alert queue monitor	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 notification queue monitor	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**.
Warning threshold for the alert queue monitor	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

You can modify the following parameters in the **Triggered alerts** area:

Parameter	Does the Following
Command line execution timeout (seconds)	The default timeout for an action (by default 30 seconds) after which a command line alert action is not executed.
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 first character (**a**) is replaced by the second (**b**). ● Multiple pairs are separated by a comma (,). For example: `|a|b|,|c|d|,|e|f|`.
Default EXE path	The default path to the default executable for EUM alerts.
Default SNMP Port, Default SNMP Target Address	The default SNMP Trap host address. You can enter 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 the BSM Application Administration Guide or Create SNMP Trap/Edit SNMP Trap Dialog Box in the BSM Application Administration Guide. 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.
Default URL	The default URL address for EUM alerts.

Parameter	Does the Following
Enable alert dependencies across CIs	If this option is set to **true**, alert dependencies are allowed between CIs.
Enable alert timer reset	If this option is set to **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. The default is **false**.
Enable logging to DB	If this option is set to **true**, alerts and notifications are not logged in the Profile database. The default is **false**.
Enable notifications and actions	If this option is set to **true**, the alert engine is able to perform actions and send notifications. This customization is available only for EUM alerts. The default is **true**.
Legacy SNMP Port, Legacy SNMP Target Address	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 the BSM Application Administration Guide or Create SNMP Trap/Edit SNMP Trap Dialog Box in the BSM Application Administration Guide. 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	Specifies 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	The URL embedded in the notifications.

Parameter	Does the Following
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**. Select this option to display the email address 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 would look as follows: To:JSmith@example.com;MBrown@example.com Profile Name: forAlert Severity: Major • **Logical Name**. Select this option 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:John Smith, Mary Brown Profile Name: forAlert Severity: Major
SNMP alerts charset	The character set used to send SNMP alert traps. By default, the setting uses the platform's default character set. If your operating system supports multi-byte characters, it is recommended to use the "UTF-8" character set.
Symphony request timeout (seconds)	The number of seconds until an alert action times out.
Wait interval between retries (seconds)	The number of seconds between each attempt to execute a notification.

Modify the way alerts are sent by email

To modify the way email alerts are handled:

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.

2. Select **Foundation > Platform Administration**.

3. In the **Alerts E-Mail Settings** area, modify the following:

Parameter	Does the Following
Password for authorized email sending	The default password for authorized sending of email alerts.
SMTP server (Windows only)	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)	The SMTP server port
User for authorized email sending	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:

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.

2. Select **Foundation > Platform Administration**.

3. In the **Alerts Pager Settings** area, modify the following:

Parameter	Does the Following
Password for authorized pager sending	The default password for authorized sending pager alerts.
SMTP server (Windows only)	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)	The SMTP server port
User for authorized pager sending	The default user for authorized sending pager alerts. If not set, the system sends pager alerts without authorization.

Modify the way alerts are sent by SMS

To modify the way SMS alerts are handled:

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.

2. Select **Foundation > Platform Administration**.

3. In the **Alerts SMS Settings** area, modify the following:

Parameter	Does the Following
Password for authorized SMS sending	The default password for authorized sending SMS alerts.

Parameter	Does the Following
SMTP server (Windows only)	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)	The SMTP server port
User for authorized SMS sending	The default user for authorized sending SMS alerts. If not set, the system send SMS alerts without authorization.

Modify the way notifications are handled

To modify the way notifications are handled:

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**

2. Select **Foundations > Platform Administration**.

3. In the **Platform Administration - Recipient Notification Service** area, modify the following:

Parameter	Does the Following
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, (Windows only) Alternate SMTP server port (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 notifications 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	The name of the sender of alert emails.

Parameter	Does the Following
Enable recipient notifications	If this option is set to **false**, the system will not send email notifications.
Notification date format	The format used to display dates in notifications.
Pager notifications charset	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	The default password for authorized message sending. If this option is not set, the system sends messages without authorization.
SMS notifications charset	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)	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)	The SMTP server port
SMTP server socket connection timeout (seconds) (Windows only)	The default timeout (60 seconds) after which an SMTP server socket is disconnected.
User for authorized message sending	The default user for authorized message sending. If this option is not set, the system sends messages without authorization.

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

Alert Type	Path to Log and to Properties File for Log Level Setup	Description
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	For details about CI Status Alerts, see Configuration Item Status Alert Notifications Report in the BSM User Guide.
	For details about SLA Status Alerts, see SLA Status Alert Notifications in the BSM User Guide.
	For details about EUM alerts, see Alert Details in the BSM User Guide.

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 383.

- 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.

Chapter 31

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 BSM 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 397.

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 397.

> **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 in the BSM Application Administration Guide.

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 392.

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 389.

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 393.

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 397.

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 390.

> **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 the next page. For details on clear alerts, see Advanced Settings Tab in the BSM User Guide.

To create, modify, or manage clear alerts notification templates, see "Notification Templates Page" on page 397.

EUM Alerts Notification Templates User Interface

This section describes:

- "Notification Template Properties Dialog Box" below

- "Notification Templates Page" on page 397

Notification Template Properties Dialog Box

This dialog box enables you to define a new alerts notification template.

To access	**Admin > Platform > Recipients > End User Management Alerts Notification Templates** • To create a new template, in the End User Management Alerts Notification Templates page, click the **New** button. • To edit an existing template: in the End User Management Alerts Notification Templates page, select an existing template, and click ✏.
Important information	**Clear alert notifications:** To set up a clear alert notification, select the notification template to use as the basis for your clear alert template and clone it. Make you determination based on the notification templates that was selected for users likely to receive a clear alert notification. Change the name of the template by deleting `Copy of` and adding `_FOLLOWUP` (all caps, one word). Edit the template details as required. It is recommended that you include in the Subject of a clear alert email, the Header, the Alert Specific Information, or both. **Example:** If you are creating a clear alert template based on the LONG default template, you would call the clear alert template LONG_FOLLOWUP. If the clear alert template is based on a user-defined template called MyTemplate, name the clear alert template MyTemplate_FOLLOWUP. **Default:** The _FOLLOWUP string is the default string recognized by BSM as the template name for a clear alert message. **Customization:** You can customize the _FOLLOWUP string. For details, see "How to Configure a Template for Clear Alert Notifications" on the previous page.
Relevant tasks	"How to Configure a Template for Clear Alert Notifications" on the previous page

General Information Area

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

UI Element (A-Z)	Description
<Insert>	Select a parameter to add to the section. Repeat to add as many text parameters as you want from the list.
	Add free text before or after the text parameters. The text parameters available for this section are:
	• **Alert Name.** The name of the alert, as defined in the alert scheme.
	• **Severity.** The severity label assigned to the alert in the alert scheme.
	• **HP BSM URL.** The URL of the 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	Enter a name for the template.
	If possible, use a descriptive name that includes information on the type of alert (email, pager, SMS) for which you plan to use the template, or the recipients who receive alerts using this template.
Subject	Specify the information that you want BSM to include in the subject of the email, pager message, or SMS message.
	Use the **<insert list for Subject / Header / Footer>** to add parameters and free text to create a customized subject. Use as many parameters as you want from the list.

Header Area

Use this area to specify the information that you want to appear at the top of the alert notice. Select parameters from the **<Insert>** list and free text to create a customized header. Use as many parameters as you want from the list.

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

UI Element (A-Z)	Description
<Insert>	Select a parameter to add to the section. Repeat to add as many text parameters as you want from the list. Add free text before or after the text parameters. The text parameters available for this section are: • **Alert Name.** The name of the alert, as defined in the alert scheme. • **Severity.** The severity label assigned to the alert in the alert scheme. • **HP BSM URL.** The URL of the 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. • **Entity ID.** The ID of the CI attached to the alert.

Alert Specific Information Area

Use this area to add alert information to the notification.

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

UI Element (A-Z)	Description
<insert list for Alert Specific Information>	Select a text parameter to add to the section. Repeat to add as many text parameters as you want from the list. • **Trigger Cause.** A description of the alert trigger conditions, as specified in the alert scheme. • **Actual Details.** A description of the actual conditions at the time of the alert.

Transaction Area

Use this area to specify the BMP transaction details relevant only for the BPM alert type.

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

UI Element (A-Z)	Description
<Insert>	Select a parameter to add to the section. Repeat to add as many text parameters as you want from the list. Add free text before or after the text parameters. The text parameters available for this section are: • **Data Collector Name.** The name of the data collector running the transaction related to the alert. • **Script Name.** The name of the script containing the transaction related to the alert. • **Transaction Time.** The date and time of the alert. • **Transaction Description.** A description of the transaction, if it has been defined in System Availability Management. • **Transaction Name.** The name of the transaction related to the alert. • **Transaction Error.** The error message generated by the data collector for the transaction, if a transaction error occurred at the time of the alert. • **Location Name.** The location of the data collector running the transaction related to the alert.

Footer Area

Use this area to specify the information that you want to appear at the bottom of the alert notice. Select parameters from the **<Insert>** list and free text to create a customized footer. Use as many parameters as you want from the list.

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

UI Element (A-Z)	Description
<Insert>	Select a parameter to add to the section. Repeat to add as many text parameters as you want from the list.
	Add free text before or after the text parameters. The text parameters available for this section are:
	• **Alert Name.** The name of the alert, as defined in the alert scheme.
	• **Severity.** The severity label assigned to the alert in the alert scheme.
	• **HP BSM URL.** The URL of the 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.
	• **Entity ID.** The ID of the CI attached to the alert.

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 > End User Management Alerts Notification Templates**

Important information	When configuring alert schemes, you can instruct BSM to automatically follow up the alert by sending a clear alert notification. For details on selecting this option while creating your alert scheme, see "How to Configure a Template for Clear Alert Notifications" on page 392.
	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.
	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.
	• 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 391

User interface elements are described below:

UI Element (A-Z)	Description
⧉	**Click to duplicate notification template.** Clones the selected notification template. The Notification Template Properties dialog box opens where you can edit the cloded notification. For details, see "Notification Template Properties Dialog Box" on page 393.
✏	**Click to modify notification template properties.** Click to edit the selected template. For details, see "Notification Template Properties Dialog Box" on page 393.
✖	**Click to delete notification template.** Delete the selected templates simultaneously.
	To delete multiple templates simultaneously, select their check boxes, and click the ✖ button located at the bottom of the templates list.
New Template	Click the **New Template** button to open the Notification Template Properties dialog box. For details, see "Notification Template Properties Dialog Box" on page 393.

UI Element (A-Z)	Description
Notification Template Name	Lists the default templates and the custom templates. The default templates are: • **DEFAULT_LOG_FORMAT.** Includes all the elements needed to create a default long format notification for reports. • **DEFAULT_POSITIVE_FORMAT.** Includes all the elements needed to create a default long format notification for positive or clear alerts. For details on clear alerts, see "How to Configure a Template for Clear Alert Notifications" on page 392. • **LONG.** Includes all the elements needed to create a default long format notification. • **SHORT.** Includes all the elements needed to create a default short format notification. **Note:** For details on the parameters displayed in each template, see "Notification Template Properties Dialog Box" on page 393.

Part 6

Troubleshooting

Chapter 32

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).

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 Run-time 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 "JMX Console" on page 102.)

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" on page 60.

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

---

HP Business Service Management (9.22)

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.

- 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:

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**.

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.

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 BSM Hardening Guide.

> **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 **showConfigurationSummaryInvoke** 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 Database Schema Verification in the BSM Database Guide.

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.mspx.

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 have changed

You can no longer access BSM using 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.