HP Service Health Reporter

Windows® and Linux operating systems

Software Version: 9.40

Integration Guide

Document Release Date: May 2015

Software Release Date: January 2015

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 2010 - 2015 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

Oracle®, Oracle WebLogic®, and Java® are registered trademarks of the Oracle Corporation and/or its affiliates.

IBM and WebSphere are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide.

Documentation Updates

The title page of this document contains the following identifying information:

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

To check for recent updates or to verify that you are using the most recent edition of a document, go to: **http://h20230.www2.hp.com/selfsolve/manuals**

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: **http://h20229.www2.hp.com/passport-registration.html**

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

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

Support

Visit the HP Software Support 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

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is **http://h20230.www2.hp.com/sc/solutions/index.jsp**

Contents

Contents 3
Integrating with Monitoring Solutions 5
Integrating SHR with MyBSM 6
Steps for Integrating SHR with MyBSM 6
Step 1: Creating a User in SHR and Configuring Preferences 6
Step 2: Configuring BSM/SHR LW-SSO Authentication 14
Step 3: Configuring SAP BusinessObjects Trusted Authentication 19
Step 4: Generating the Report Component XML and Loading it to MyBSM 20
Step 5: Creating MyBSM Page and Adding the Report Component 25
Steps for Integrating SHR with OMi 10 26
Enable Global ID OMI10 System 26
Step 1: Creating a User in SHR and Configuring Preferences 27
Step 2: Configuring OMi 10/SHR LW-SSO Authentication 33
Step 3: Configuring SAP BusinessObjects Trusted Authentication 37
Step 4: Generating the Report Component XML and Loading it to MyBSM 38
Step 5: Creating MyBSM Page and Adding the Report Component 44
Best Practices 45
Finding the Document ID of a Report 46
We appreciate your feedback! 48

Integrating with Monitoring Solutions

This section provides information about integrating SHR with other monitoring solutions of HP Software to simplify and enhance the experience of launching and viewing SHR reports.

Integrating SHR with MyBSM

This chapter provides the steps to view HP Service Health Reporter (SHR) reports on the HP Business Service Management MyBSM user interface. You can launch SHR reports in the context of a Configuration Item (CI) or Business View from the MyBSM user interface.

Integrating SHR with MyBSM enriches the component gallery and provides a convenient way to view all the BSM and SHR reports in one place, without launching SHR.

Steps for Integrating SHR with MyBSM

Step 1: Creating a User in SHR and Configuring Preferences

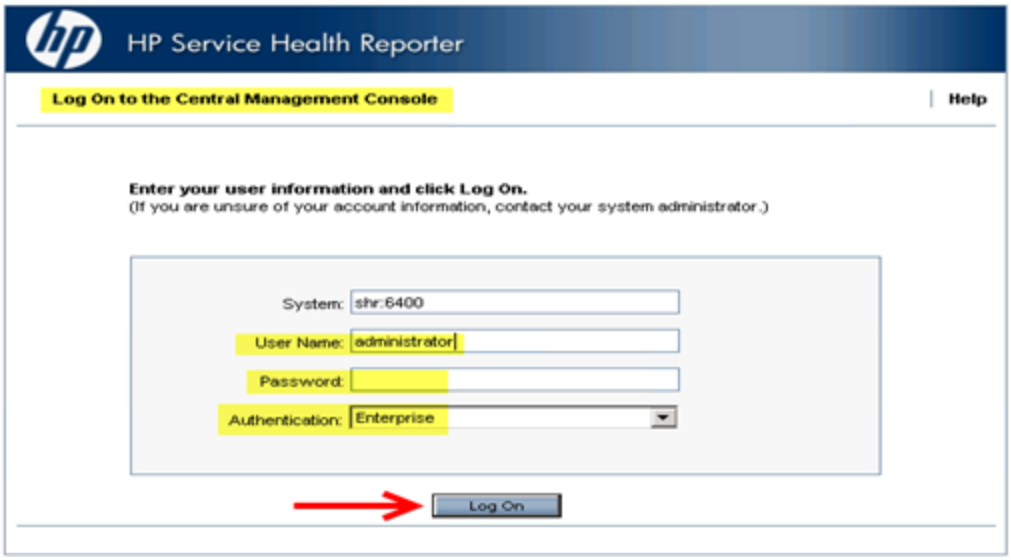
As a prerequisite, you should have already created a user account in BSM with permissions to create and view pages in MyBSM. This BSM user should also be a user in SHR with authorization to view SHR reports.

SHR uses SAP BusinessObjects for user management. To create a user in SHR, perform the following steps:

1. Log on to **SAP BusinessObjects Central Management Console (CMC)** by typing the address **http://<hostname>:8080/CmcApp** into the browser window.

   Note: The hostname must be the name of the server on which SAP BusinessObjects is installed.

Figure 1.1 Log on screen of SAP BusinessObjects Central Management Console



SHR supports redirection of HTTP URL to HTTPS URL. Perform the following steps:

a. Stop the following Services:

   - HP_PMDB_Platform_Administrator
   - Business Objects Webserver

b. Locate the `web.xml` file instances in the following paths:

   - Admin UI: `%PMDB_HOME%/ adminServer/webapps/BSMRApp/WEB-INF/web.xml`.
   - InfoViewApp: `%PMDB_HOME%/BOWebServer/webapps/InfoViewApp/WEB-INF/web.xml`.
   - CmcApp:`%PMDB_HOME%/BOWebServer/webapps/CmcApp/WEB-INF/web.xml`

c. Enable the following in the `web.xml` instances:

```
<security-constraint>

<web-resource-collection>

<web-resource-name>Entire Application</web-resource-name>

<url-pattern>/*</url-pattern>

</web-resource-collection>

<user-data-constraint>
```

```
<transport-guarantee>CONFIDENTIAL</transport-guarantee>

</user-data-constraint>

</security-constraint>
```

d. Start the following Services:

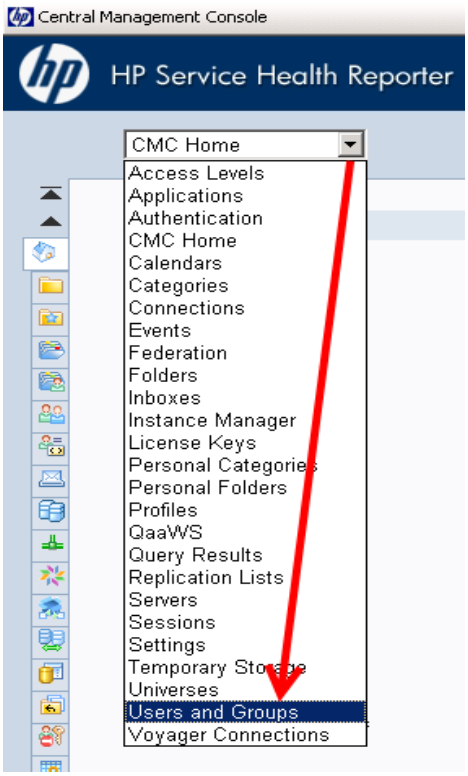
- HP_PMDB_Platform_Administrator
- Business Objects Webserver

e. Accessing the HTTP URL should redirect it to HTTPS.

> **Note:** Make sure the following ports are open, in the environment:
>
> - 21411 - HP PMDB Platform Administrator
> - 21412 - SSL Connector redirect
> - 8443 - SSL Connector defaut
> - 8080 - Apache Tomcat

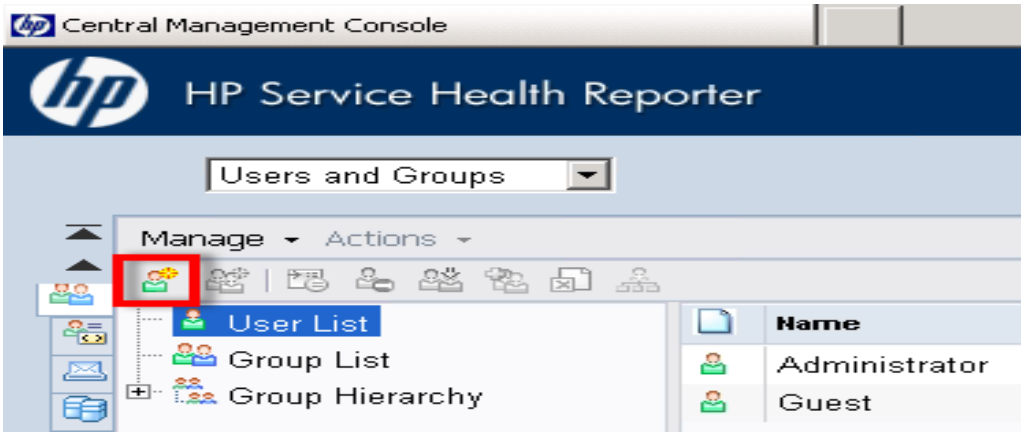
2. Select **Users and Groups** from the drop-down box.

Figure 1.2 CMC Users and Groups screen



3. Select **User List** and click **Create New User** icon as shown in figure 1.3.

Figure 1.3 Creating a new user



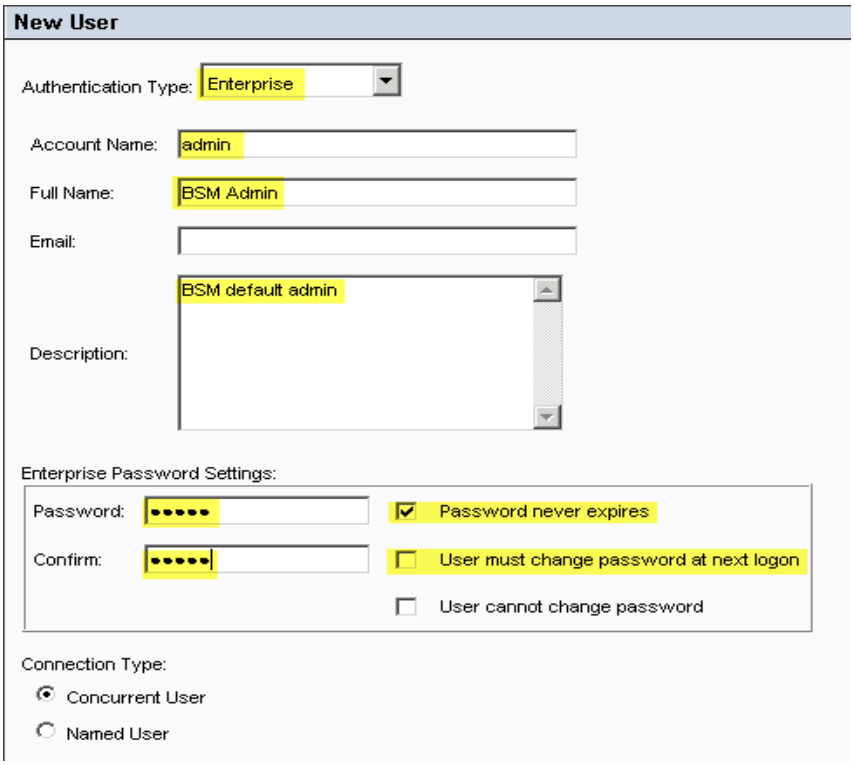
4. Enter the user details in the **New User** window as shown in figure 1.4 (a).

Note: Your SAP BusinessObjects username must be the same as your Account Name in HP BSM.

a. Check **Password never expires** under Enterprise Password Settings.

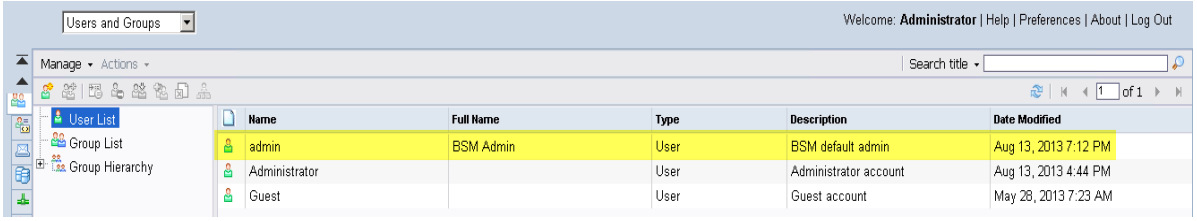
b. Click **Create & Close**.

Figure 1.4 (a) Create New User Screen



The newly created user appears in the **User List** as shown in the following figure.

Figure 1.4 (b) Admin



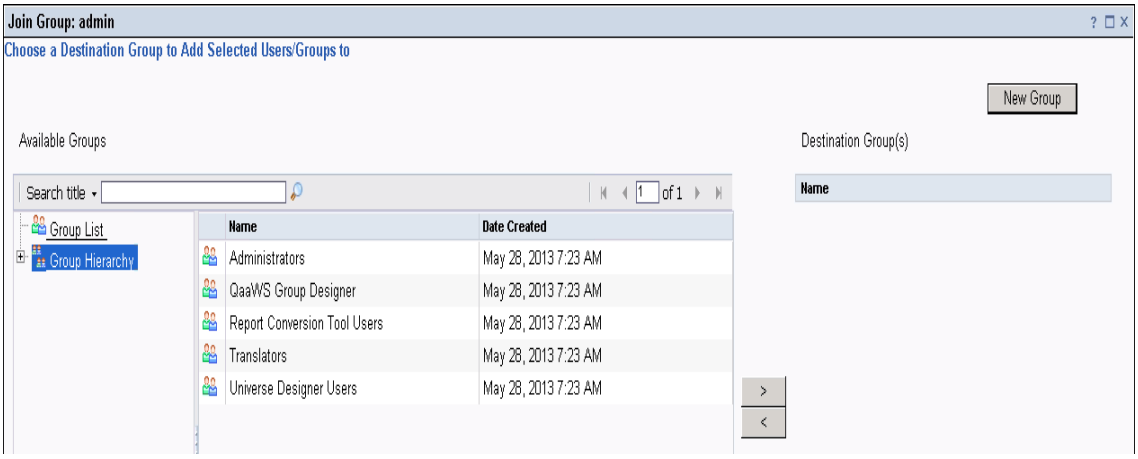
5. To add the SHR user to Administrator group, perform the following steps:

   a. Select the user you created and click the **Add member to user group** icon as shown below.

   Figure 1.5(a).

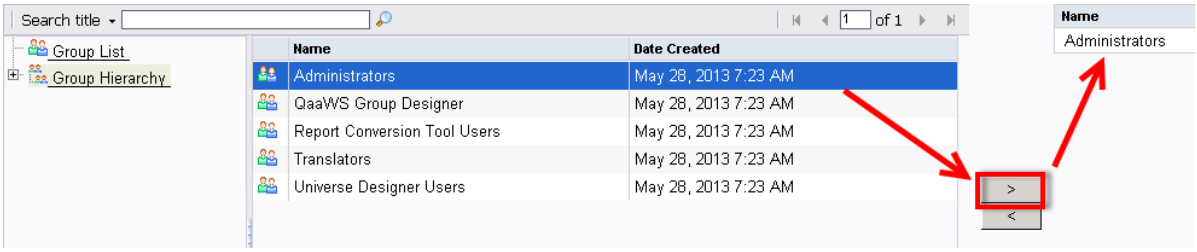
   b. A pop-up window Join Group: <<username>> appears as shown in figure 1.5 (b).

   Figure 1.5 (b)



   c. To move Administrators from **Available Groups** to **Destination Group(s)**, select **Administrators**, click **>** button, then click **OK** as shown in figure 1.5 (c).

Figure 1.5 (c)

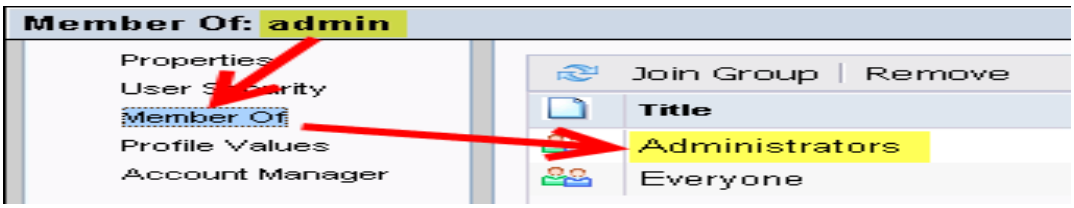


6. To verify User and Group configuration, perform the following steps:

   a. Double-click **Admin**, the user you created from the list of users.

   b. Select **Member Of** and check if Administrators is listed on the right side as shown in figure 1.6.

   Figure 1.6



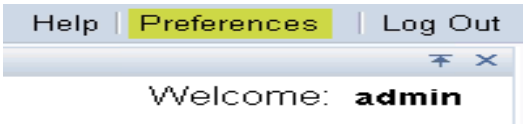
7. To ensure proper functioning of the Drill Up/Drill Down functionality in reports while accessing them from the MyBSM console, you must set the user preferences as follows:

   a. Connect to **http://<hostname>:<port>/InfoViewApp** where hostname is the name of the server on which SAP BusinessObjects is installed.

   b. Log on as SHR user.

   c. Click **Preferences** in the upper right corner as shown in figure 1.7 (a).

   Figure 1.7 (a)



   d. Under **General**,enable the options as shown in the following figures:

Figure 1.7 (b) Set User Preference-1

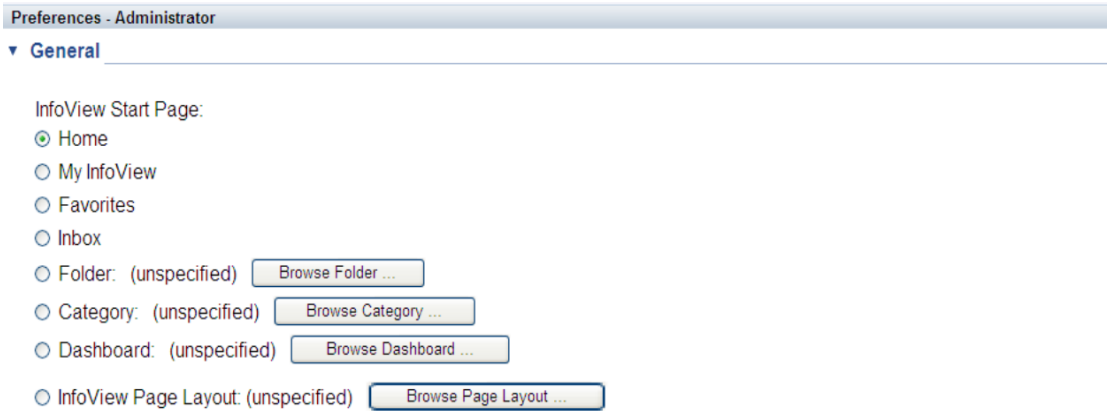
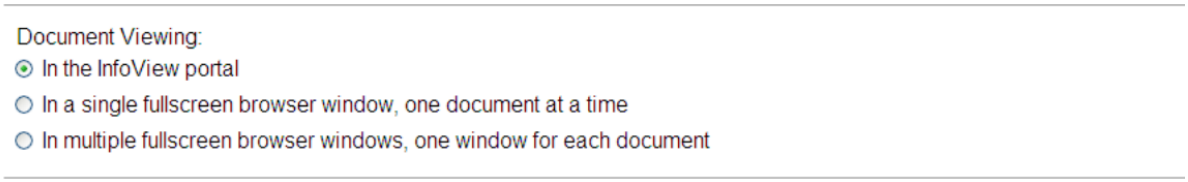


Figure 1.7 (c) Set User Preference-2



e. Click **Web Intelligence** and select the option **Synchronize drill on report blocks**. This is the only change necessary to make Preferences accept all other defaults and click **OK**.

Figure 1.7 (d) Set User Preference-3

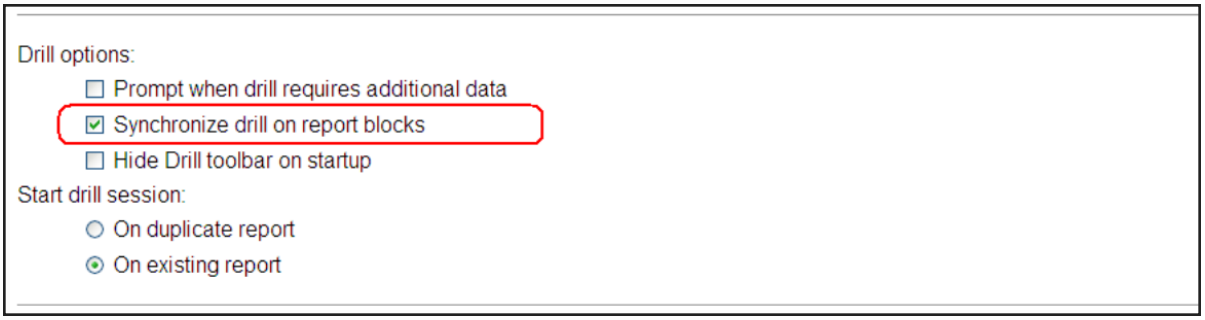
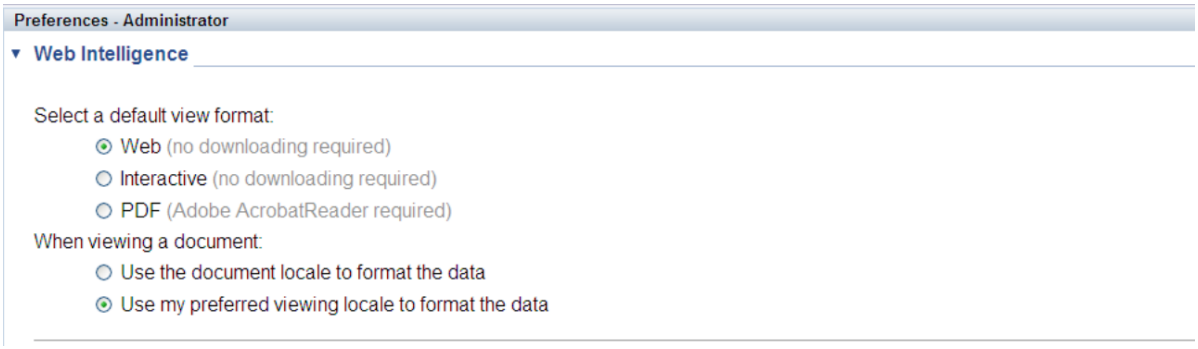


Figure 1.7 (e) Set User Preference-4



Step 2: Configuring BSM/SHR LW-SSO Authentication

Using Lightweight Single Sign-on (LW-SSO), you can enable a MyBSM user to access SHR reports with the same user credentials.

Note: As SAP BusinessObjects is a third-party application, Single Sign-on (SSO) cannot be directly achieved with BSM using LW-SSO. For MyBSM, SSO is first setup between the SHR Admin Web App and BSM using LW-SSO as explained in Step 2. Then, SSO is setup between the SHR Admin Web App and SAP BusinessObjects using SAP BusinessObjects Trusted Authentication as explained in Step 3.

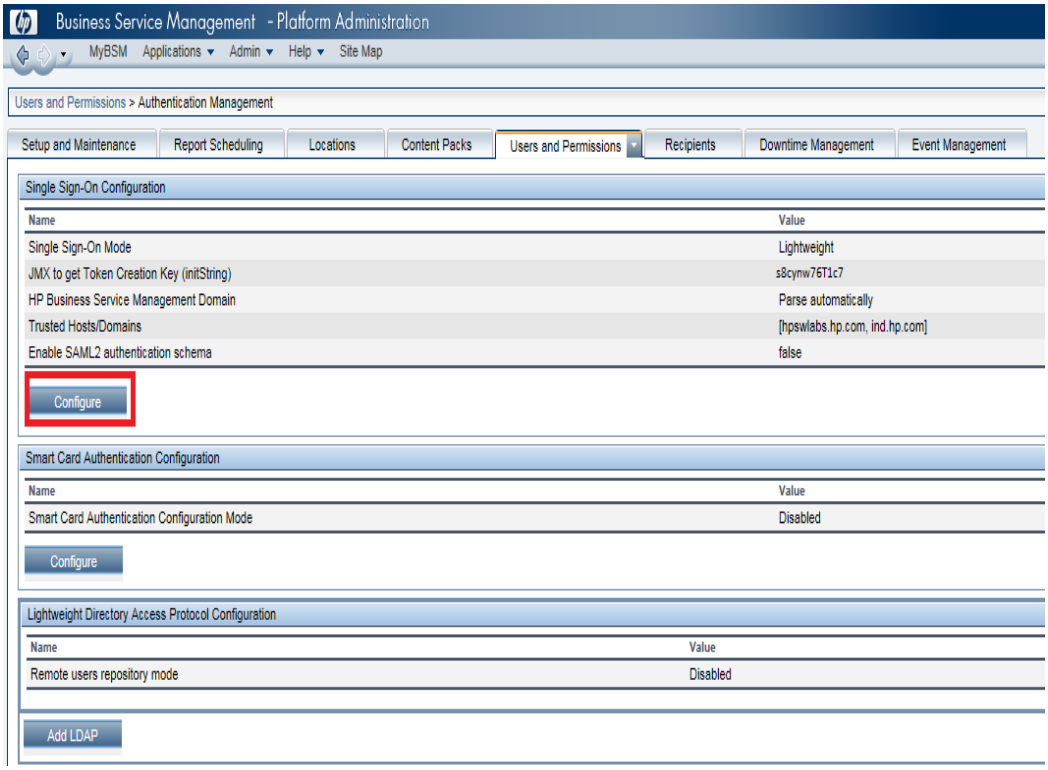
To configure LW-SSO, perform the following steps:

1. Copy the LW-SSO token from BSM:

   a. Log on to the BSM system as Administrator.

   b. Navigate to **Admin > Platform > Users and Permissions** tab Click **Authentication Management**.

Figure 2.1



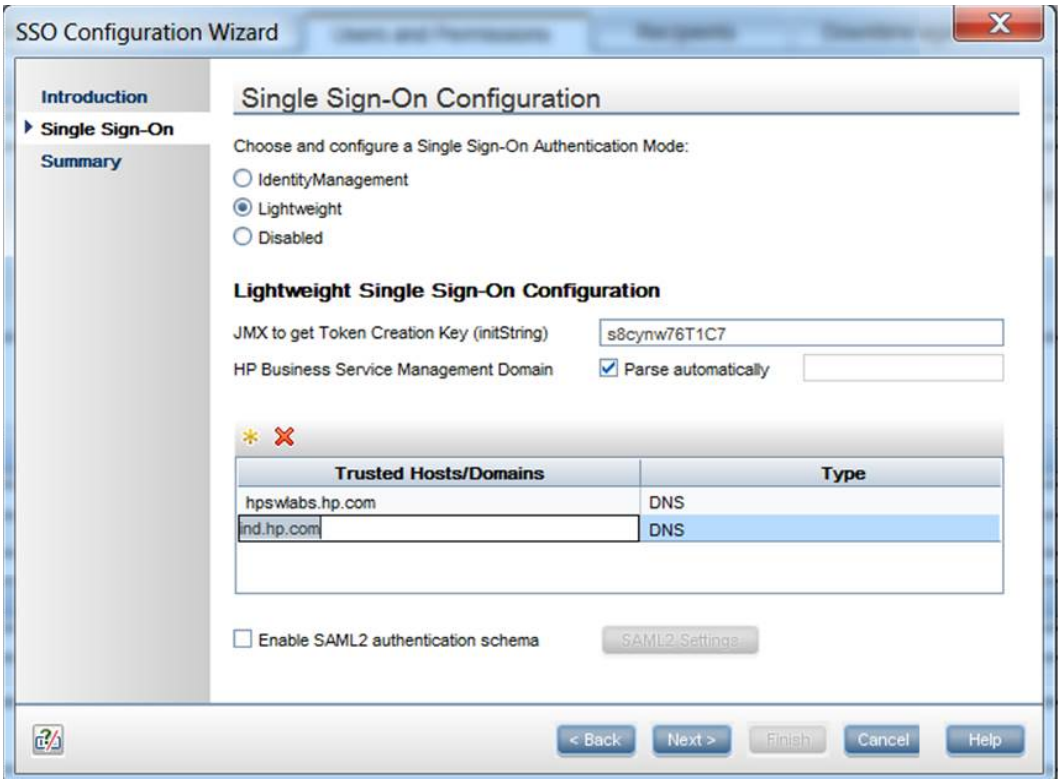
c. Copy the **Token Creation Key (InitString)** and note it down in a text file.

d. Click **Configure**.

   The SSO Configuration Wizard appears.

e. Click **Single Sign-On**.

   Figure 2.2



f. Under **Trusted Hoists/Domains**, add the SHR and BSM domain names.

> **Note:** If SHR and BSM are hosted on the same domain, it is enough it add the domain name once to the Trusted Hosts/Domains list.

g. **Uncheck** the Enable SAML2 authentication schema check-box.

h. Click **Next**, and then click **Finish**.

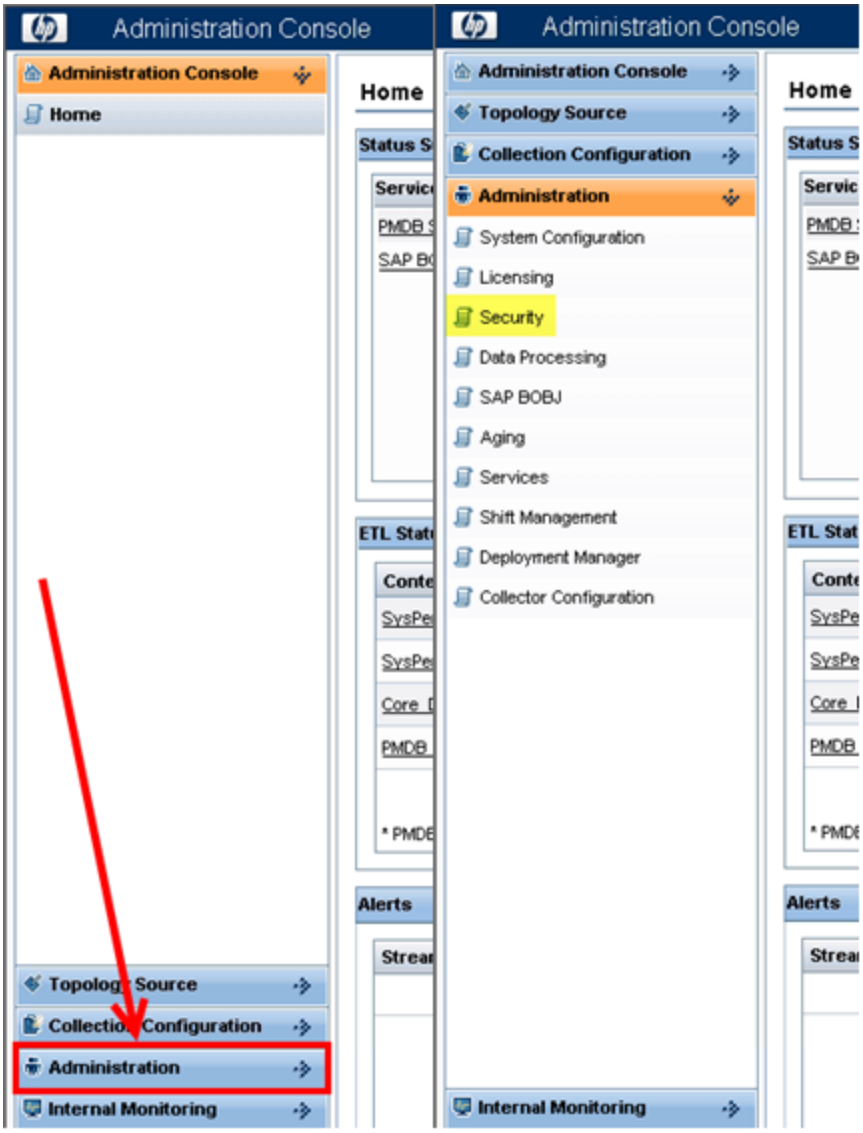
i. Restart the BSM services for the authentication changes to take effect.

2. To configure LW-SSO in SHR, perform the following steps:

a. Log on to SHR Administration Console by typing the address **http://<hostname>:21411/BSMRAppApp** in the browser window, where hostname is the name of the server on which SHR is installed.

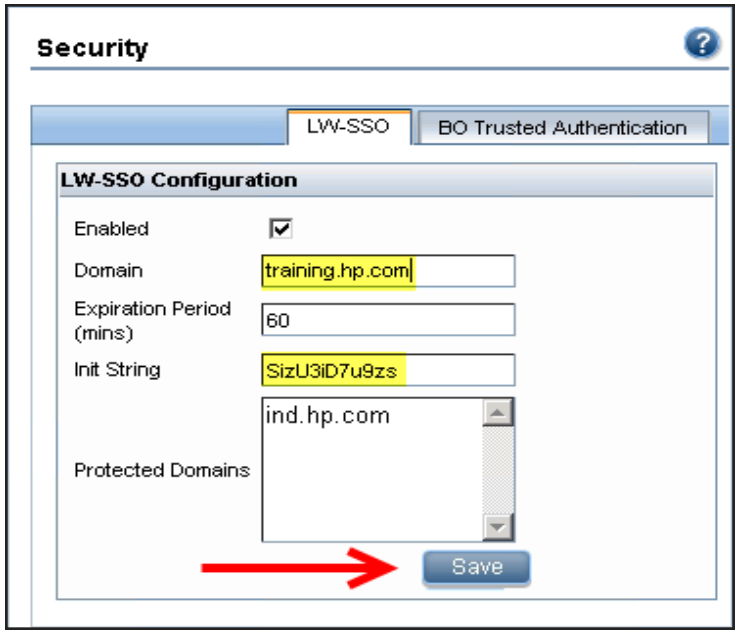
b. Go to **Administration > Security** in the left pane.

Figure 2.3



c. Click **Security** and the **LW-SSO** tab opens as shown in figure below.

Figure 2.4



d. Copy the values from the Token Creation Key (InitString) field in BSM (This is the InitString you have copied from BSM to a text file.) and paste them into the **Init String** field.

e. Check the **Enabled** option.

f. In the **Domain** field, enter the SHR domain.

g. In the **Expiration Period** field, enter the recommended value of **60** minutes for LW-SSO configuration.

h. In the **Protected Domains** field, add the BSM domain name.

Note:

i. Even if SHR and BSM are hosted in the same domain, add the domain name to the **Protected Domain** field.Even if SHR and BSM are hosted in the same domain, add the domain name to the **Protected Domain** field.

ii. Ensure `<INSTALL_DIR>\PMDB\data\config.prp, bo.cms` is set to fully qualified name of the SHR system.

i. Click **Save** to save the configuration as shown in figure 2.3.

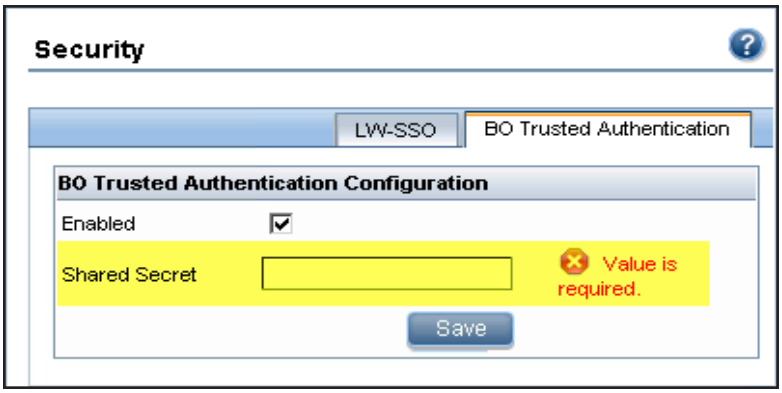
A confirmation message stating `LW-SSO Configuration saved successfully. Please restart the HP_PMDB_Platform_Administrator' service for these changes to take effect` appears. Restart this service as explained in Step 3.

Step 3: Configuring SAP BusinessObjects Trusted Authentication

To setup SSO between the SHR Admin Web App and SAP BusinessObjects, perform the following steps:

1. On the SHR system, go to **Administration >Security > BO Trusted Authentication**.
2. Check the **Enabled** option.
3. Enter a string of your choice in the **Shared Secret** field.

   Figure 3.1



> **Note:** SAP BusinessObjects Trusted Authentication works based on a shared secret mechanism between the SHR Admin Web App and SAP BusinessObjects. The string you enter in figure 3.1 is the shared secret. This string is the same shared secret across SHR Admin Web App and SAP BusinessObjects.
>
> To verify if the same shared secret is also configured in SAP BusinessObjects, log on to SAP BusinessObjects CMC.

4. Click **Save** to save the configuration.
5. Restart the **HP_PMDB_Platform_Administrator** service from the Windows services list, to apply the changes made in "Step 2: Configuring BSM/SHR LW-SSO Authentication" on page 14 and "Step 3: Configuring SAP BusinessObjects Trusted Authentication" above.

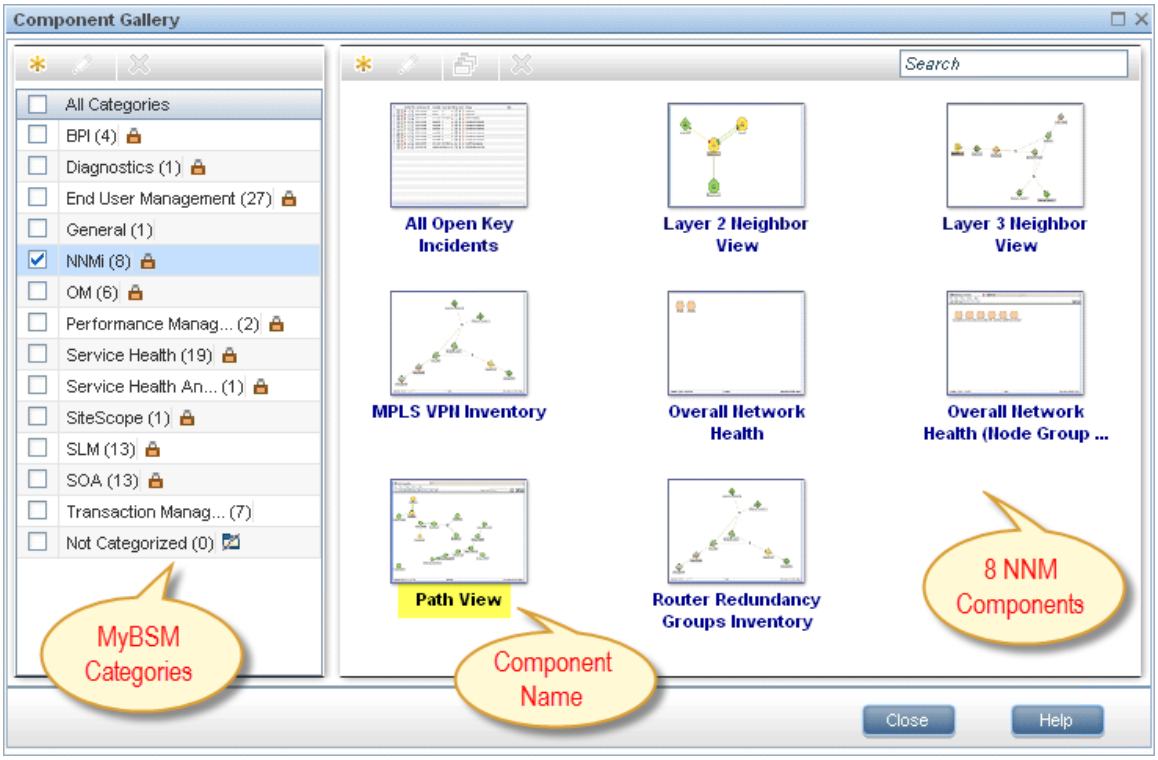
> **Note:** On a Linux host, log on as a root user and run the following command:
>
> `Service HP_PMDB_Platform_Administrator stop/start`

Step 4: Generating the Report Component XML and Loading it to MyBSM

Every MyBSM component, such as any of the eight NNM components shown in Figure 4.1, is represented in XML files located on the BSM host. To make an SHR report appear in the Component Gallery of MyBSM, create an XML and deploy it in the BSM host.

Generate the component XML file using the ComponentGenerator command on the SHR host and load it to the BSM host through a combination of manual copying and using the JMX Console.

Figure 4.1



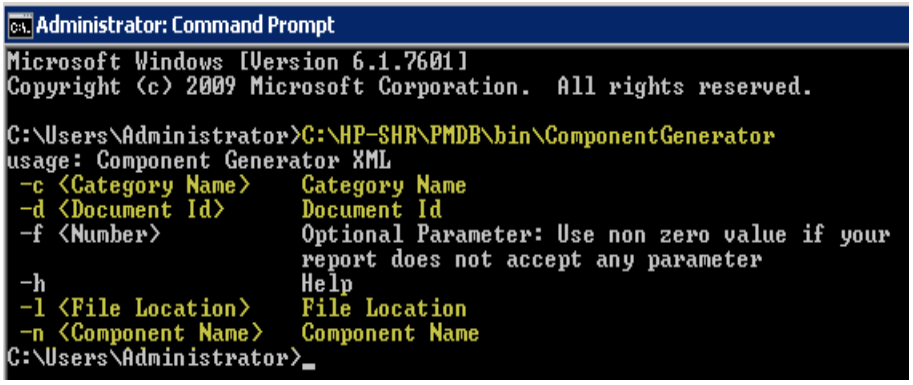
To generate the report component XML file, perform the following steps:

1. Log on to the SHR system.
2. Open a command line window (for Windows) or a shell prompt (for Linux) .
3. Run the following commands to see the ComponentGenerator syntax:

   For Windows: `%PMDB_HOME%\bin\ComponentGenerator`

   For Linux: `$PMDB_HOME/bin/ComponentGenerator`

Figure 4.2 (Windows)



4. Run the following command to generate the XML file:

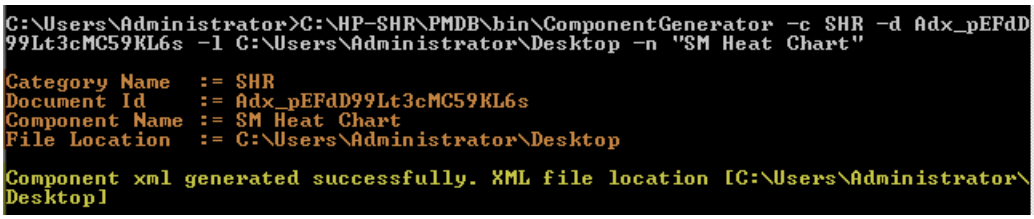
   For Windows: `%PMDB_HOME%\bin\ ComponentGenerator -c <categoryName> -d <documentId > -n <componentName> -l <outputDir> -f <optional Parameter>`

   For Linux: `$PMDB_HOME/bin/ ComponentGenerator -c <categoryName> -d <documentId > -n <componentName> -l <outputDir> -f <optional Parameter>`

   - Category Name = This is the Category to be created in Component Gallery in MyBSM
   - Document Id = This is the report's unique document ID – see the "Finding the Document ID of a Report " on page 46 section for more information.
   - File Location = This is the directory where the component XML file will be created
   - Component Name = The Component name to be created for the report in MyBSM (note the use of quotes here)
   - Optional Parameter = Use non zero value if the report does not accept view or CIID as parameter.

   > **Note:** The above command generates `<Component Category><componentName>.uim.xml` file in outputDir.

   Figure 4.3 (Linux)



To load the component to MyBSM, perform the following steps:

1. On the BSM system, copy the component XML file to `%TOPAZ_HOME%\conf\uimashup\import\toload\Components`.

   Note: If BSM is deployed in a distributed environment, the XML file resides in the Gateway Server.

2. Load the XML (`*.uim.xml`) file using the JMX Console.

   a. Log on to the BSM JMX Console by entering the address **http://<bsm hostname>:8080/jmx-console/** into the browser window.

   b. Enter BSM credentials if prompted for a username and password.

   c. Click **service=UIMDataLoader** link as shown in figure 4.4 (a) and navigate to **JMX MBean View** screen as per figure 4.4 (b)

   Figure 4.4 (a)

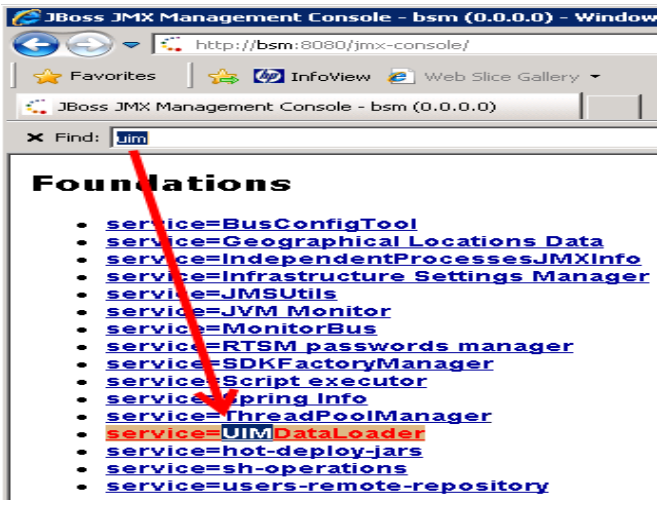
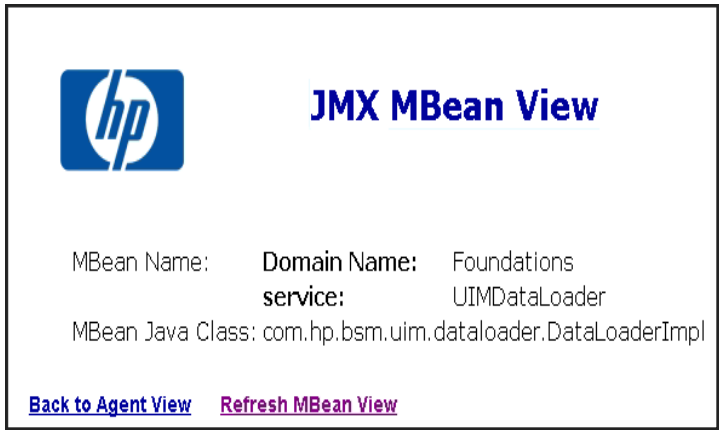
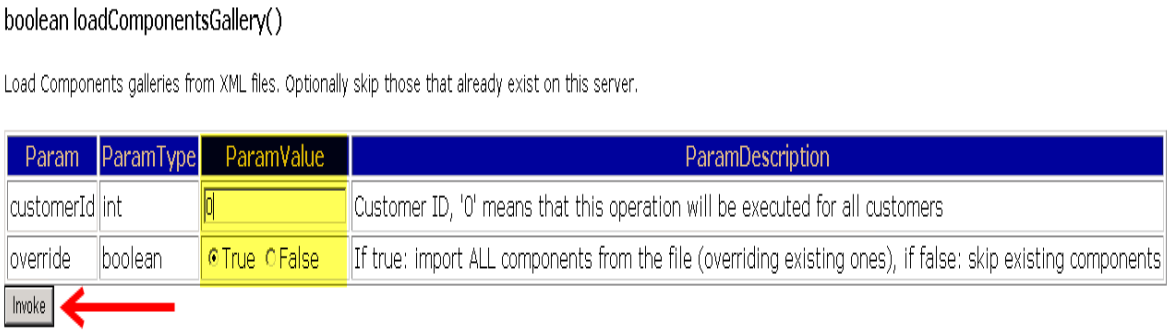


Figure 4.4 (b)



d. Go to the method named **boolean loadComponentsGallery ()**

Figure 4.5



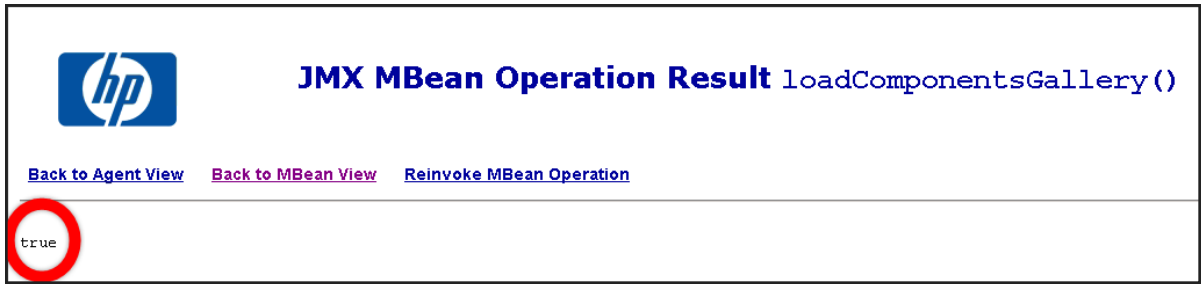
e. Enter **0** as input value in the text field.

f. Click **Invoke** to load the `*.uim.xml` file.

If the load process is successful, the component XML is moved to the `%TOPAZ_HOME%\conf\uimashup\import\loaded\Components` folder.

If the load process fails, the component XML is moved to the `%TOPAZ_HOME%\conf\uimashup\import\errors` folder.

Figure 4.6



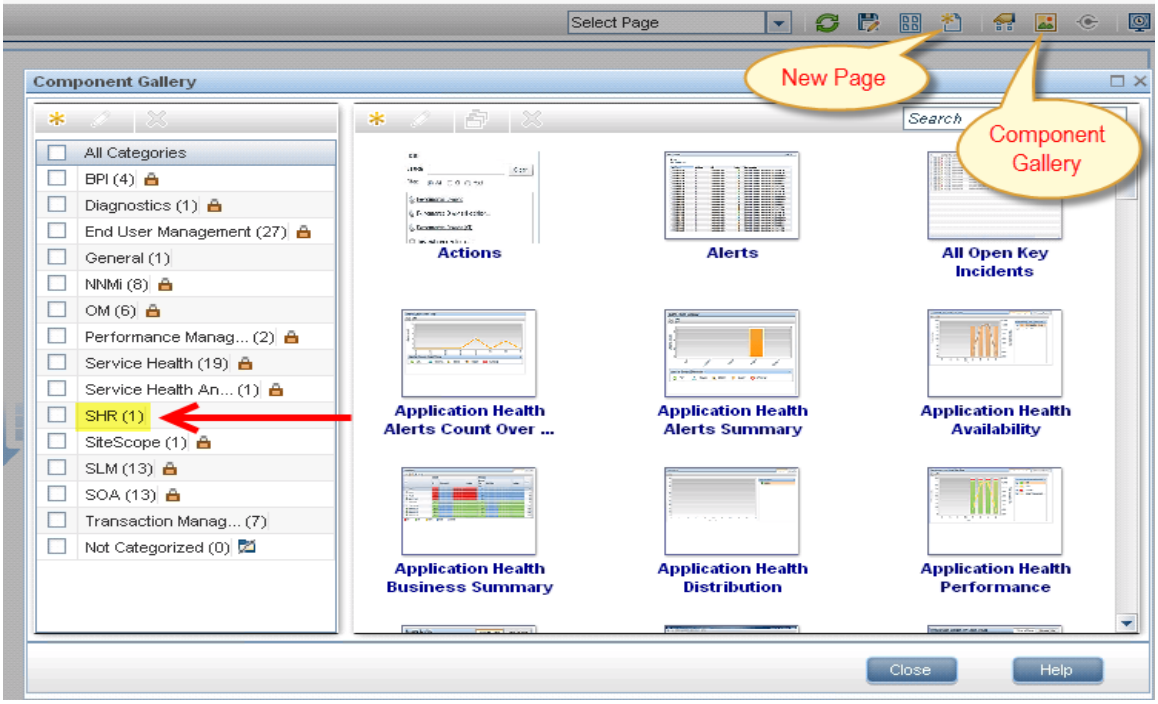
3. To verify the availability of the component in MyBSM console:

   a. Log on to the BSM user interface.

   b. Click **MyBSM**

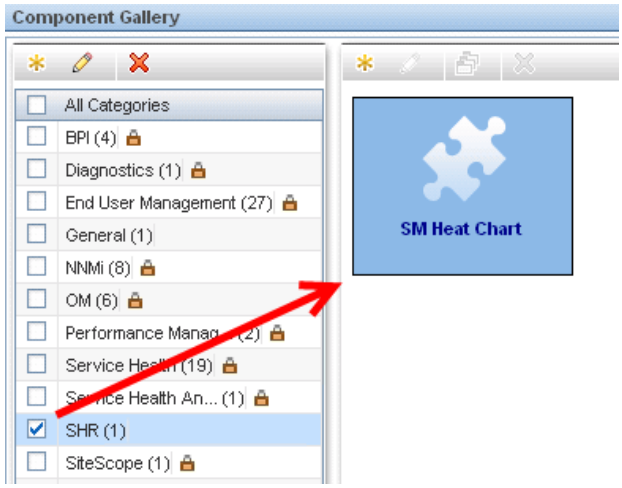
   c. Click **New Page > Component Gallery**.

   Figure 4.7



   d. The component must be available within the category.

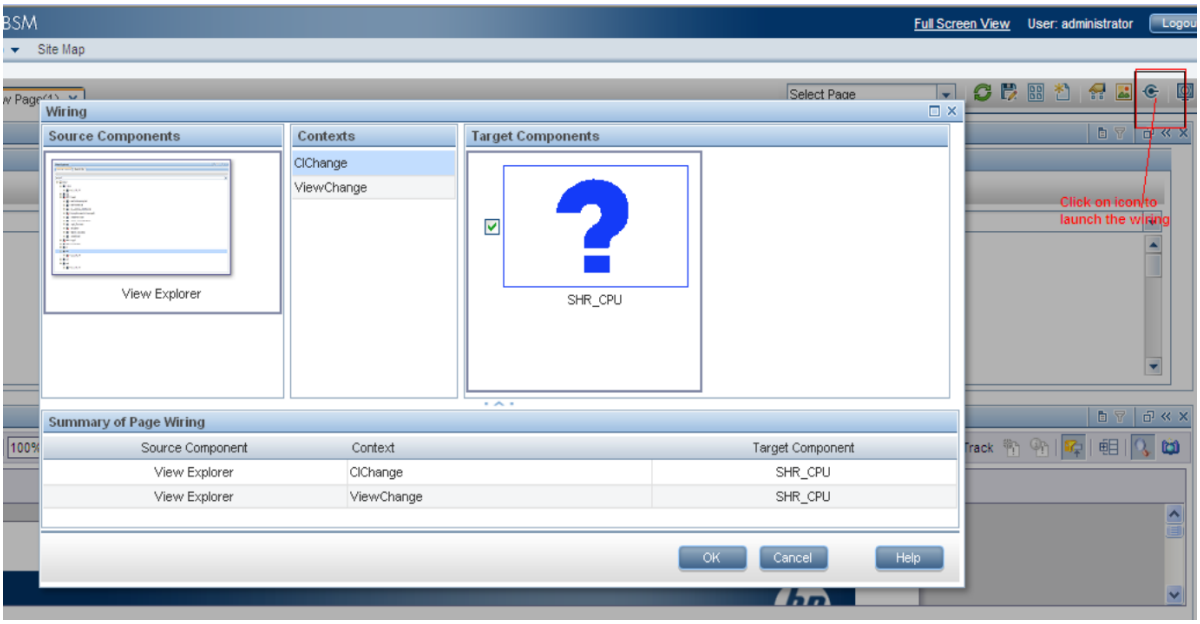
Figure 4.8



4. To verify the wiring, Click **Wiring** as shown in Figure 4.9.

> **Note:** By default, all reports are wired on ClChange and ViewChange event. If the report does not support any events, clear the check-box to disable the wiring.

Figure 4.9



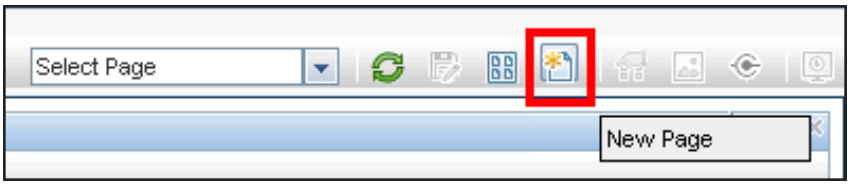
Step 5: Creating MyBSM Page and Adding the Report Component

You must create a MyBSM page and add the SHR report to it as a component.

To create a MyBSM page, perform the following steps:

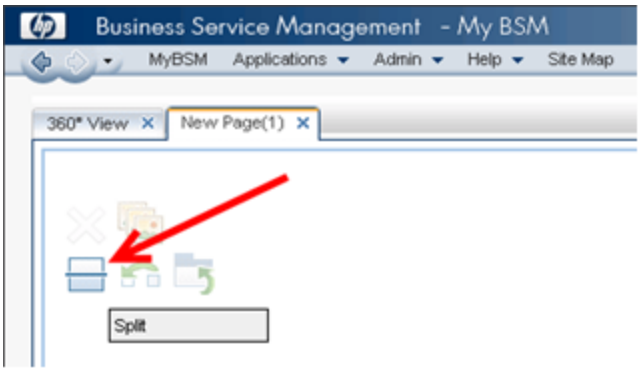
1. On the BSM user interface click **Create New**.

   Figure 5.1

2. Split the page as per the requirement.

   Figure 5.2

3. Click **Components** and drag-drop the components, such as View Explorer, to trigger the events.

4. Drag and drop the required SHR components. The SHR report can be viewed in the MyBSM page.

5. Save the page to view it from the MyBSM user interface.

Steps for Integrating SHR with OMi 10

Enable Global ID OMI10 System

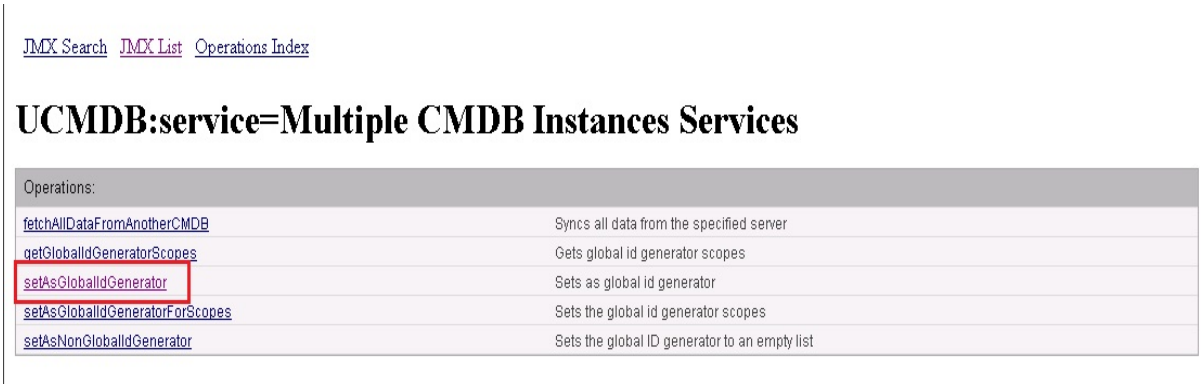
Global ID must be enabled for multiple BSM scenarios. One BSM system acts as a central BSM and all the other BSM systems reconcile with the Global ID generated at the central BSM system.

1. From the OMi 10 system, change the Global ID Generator settings from the Jmx Console using the following link:

   http://localhost:21212/jmx-console/

2. Click **UCMDB:service=Multiple CMDB Instances Services**. The UCMDB:service=Multiple CMDB Instances Services page appears.

3. Click **setAsGlobalIdGenerator**.

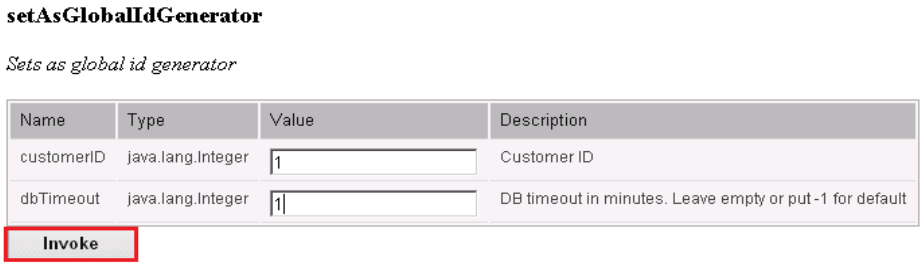


4. Type the following values:

   customerID - 1

   dbTimeout - 1

5. Click **Invoke**.



Omi 10 is set as Global ID Generator.

Step 1: Creating a User in SHR and Configuring Preferences

As a prerequisite, you should have already created a user account in OMi 10 with permissions to create and view pages in MyBSM. This OMi 10 user should also be a user in SHR with authorization to view SHR reports.

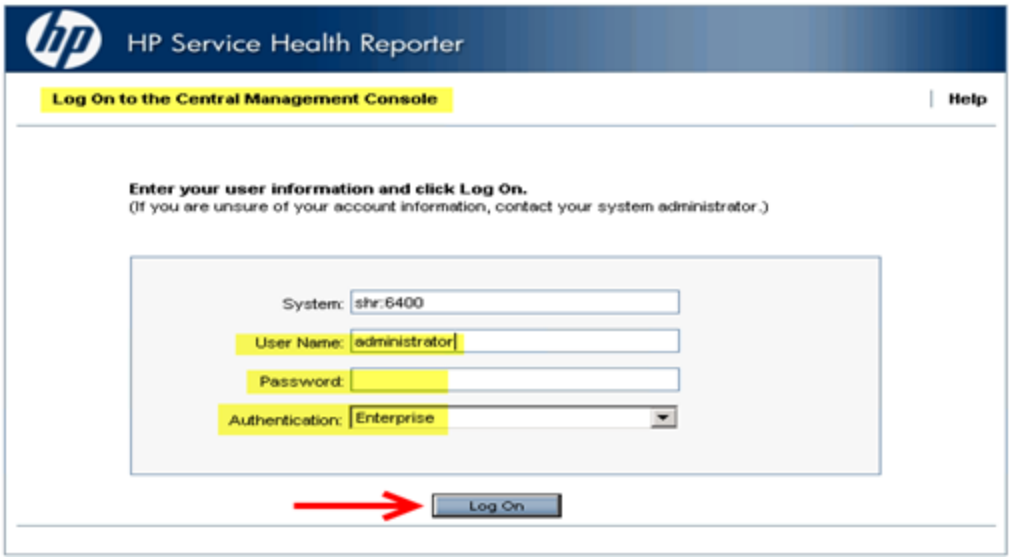
SHR uses SAP BusinessObjects for user management. To create a user in SHR, perform the following steps:

1. Log on to **SAP BusinessObjects Central Management Console (CMC)** using the following link:

   http://<hostname>:8080/CmcApp

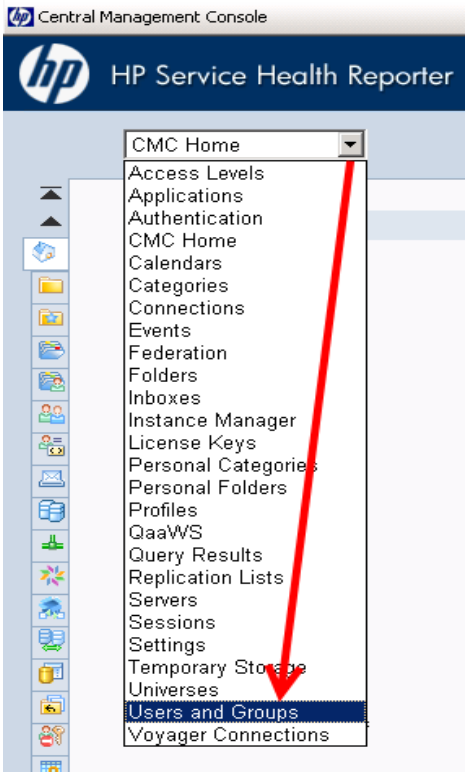
   Note: The hostname must be the name of the server on which SAP BusinessObjects is installed.

   Figure 1.1 Log on screen of SAP BusinessObjects Central Management Console



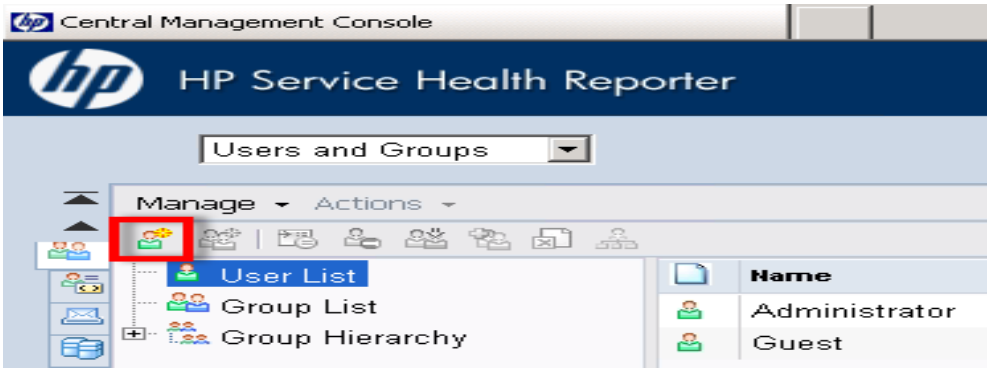
2. Select **Users and Groups** from the drop-down box.

Figure 1.2 CMC Users and Groups screen



3. Select **User List** and click **Create New User** icon as shown in figure 1.3.

Figure 1.3 Creating a new user



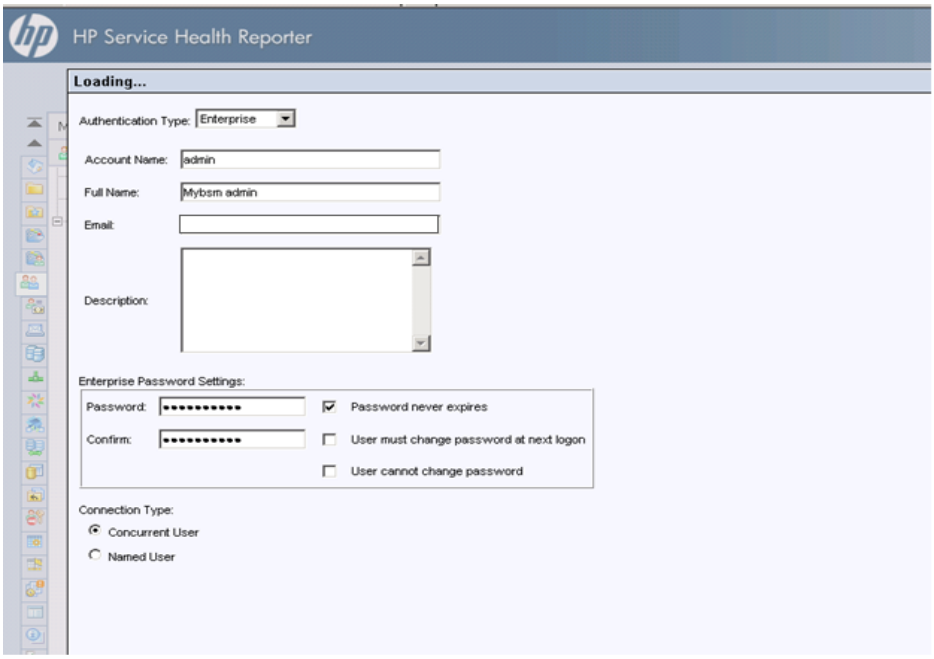
4. Enter the user details in the **New User** window as shown in figure 1.4 (a).

> **Note:** The SAP BusinessObjects username must be the same as the Account Name in HP OMi 10.

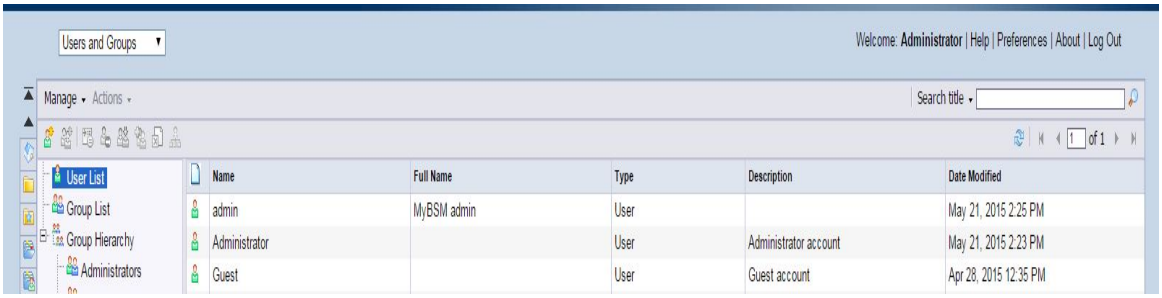
a. Check **Password never expires** under Enterprise Password Settings.

b. Click **Create & Close**.

Figure 1.4 (a) Create New User Screen



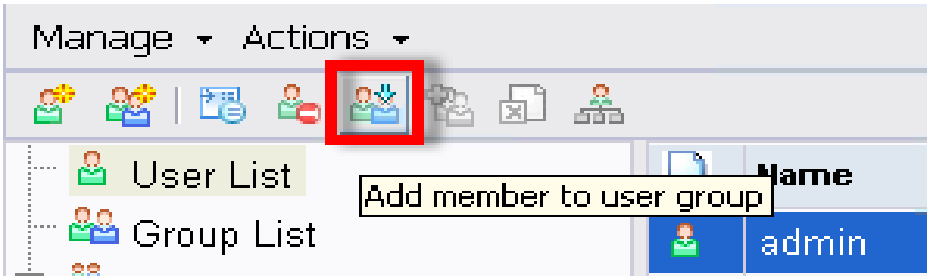
The newly created user appears in the **User List** as shown in the following figure:



5. To add the SHR user to Administrator group, perform the following steps:

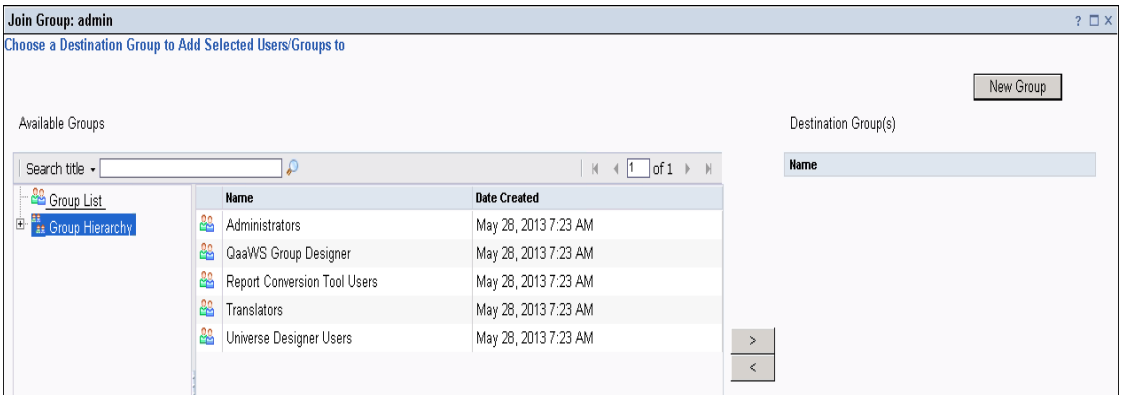
   a. Select the user you created and click the **Add member to user group** icon as shown below.

Figure 1.5(a).



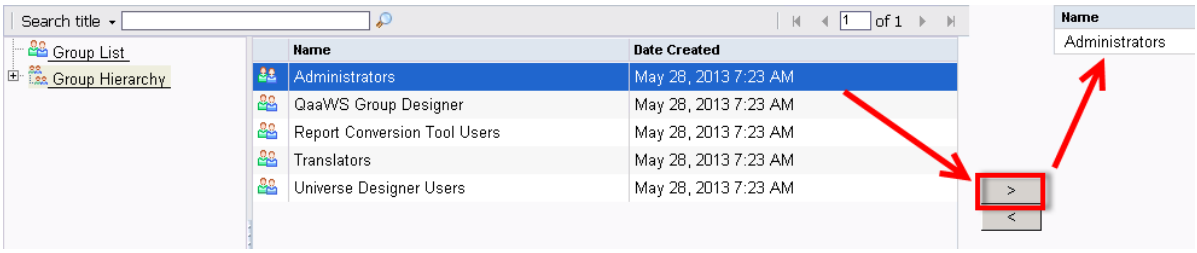
b. A pop-up window Join Group: <username> appears as shown in figure 1.5 (b).

Figure 1.5 (b)



c. To move Administrators from **Available Groups** to **Destination Group(s)**, select **Administrators**, click **>**, then click **OK** as shown in figure 1.5 (c).

Figure 1.5 (c)

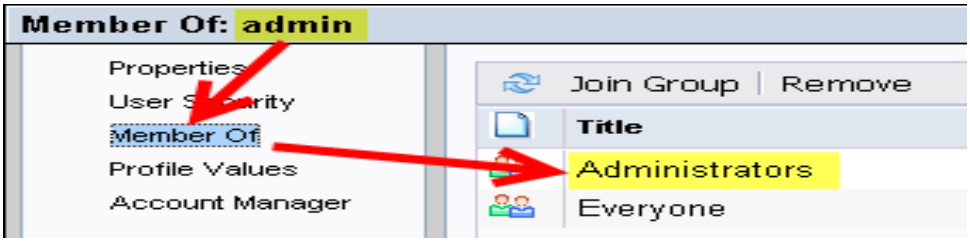


6. To verify User and Group configuration, perform the following steps:

   a. Double-click **Admin**, the user you created from the list of users.

   b. Select **Member Of** and check if Administrators is listed on the right side as shown in figure 1.6.

Figure 1.6



7. To ensure proper functioning of the Drill Up/Drill Down functionality in reports while accessing them from the MyBSM console, you must set the user preferences as follows:

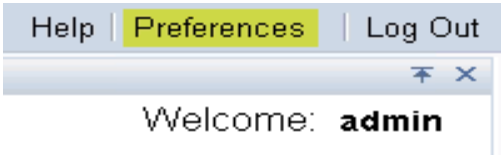
   a. Log on to SHR InfoView as SHR user from the following link:

      http://<hostname>:<port>/InfoViewApp

      where, hostname is the name of the server on which SAP BusinessObjects is installed.

   b. Click **Preferences** in the upper right corner as shown in figure 1.7 (a).

      Figure 1.7 (a)



   c. Under **General**,enable the options as shown in the following figures:

      Figure 1.7 (b) Set User Preference-1

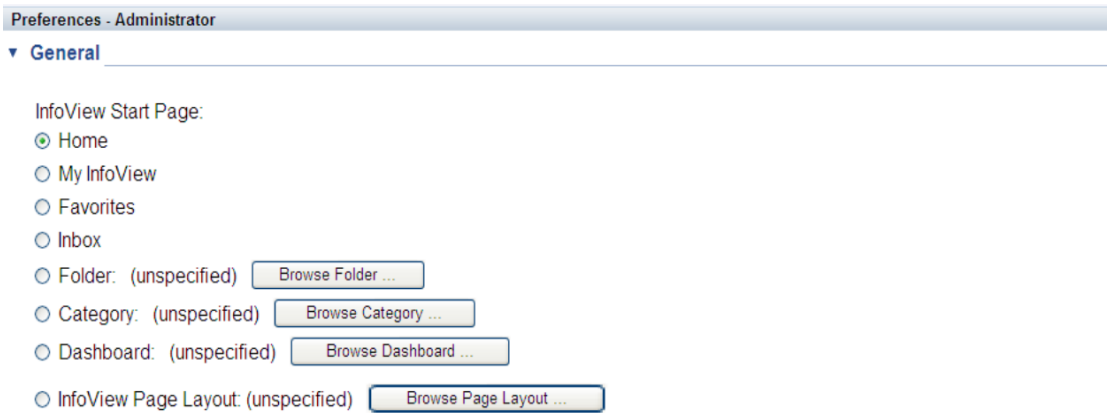
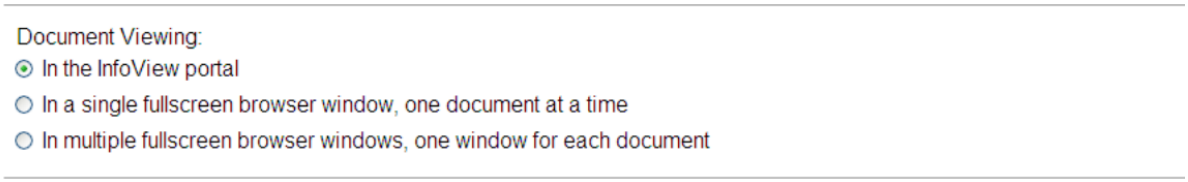


Figure 1.7 (c) Set User Preference-2



d. Click **Web Intelligence** and select the option **Synchronize drill on report blocks**. This is the only change necessary to make Preferences accept all other defaults and click **OK**.

Figure 1.7 (d) Set User Preference-3

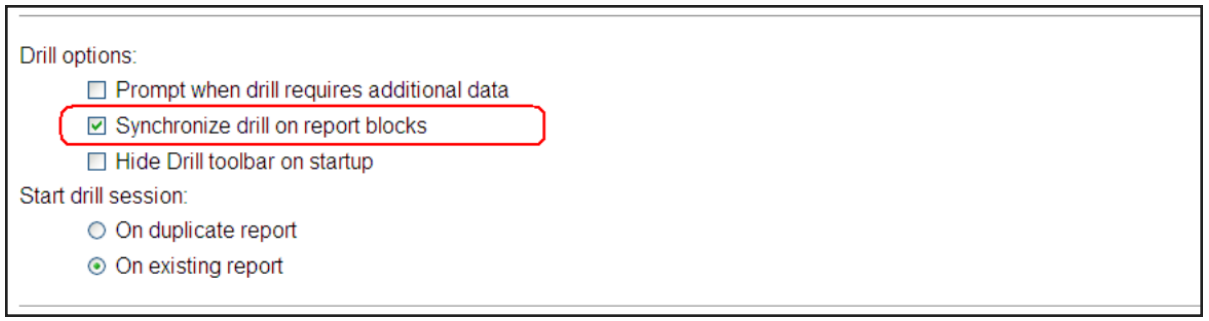
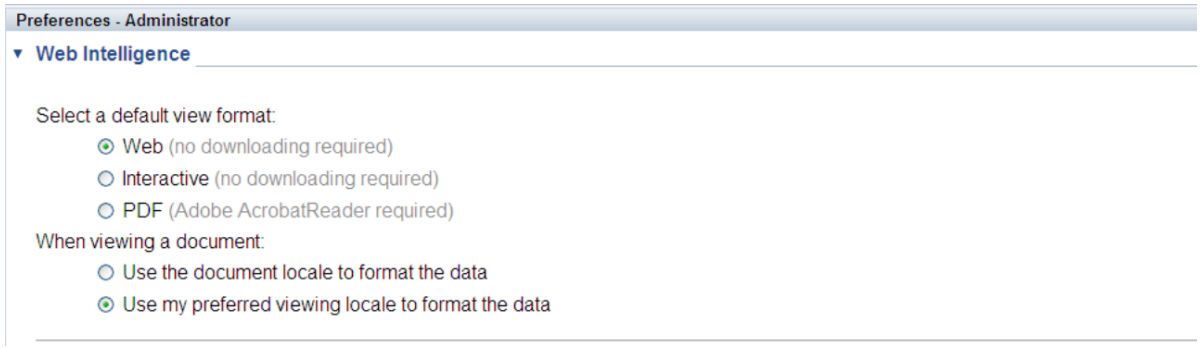


Figure 1.7 (e) Set User Preference-4



Step 2: Configuring OMi 10/SHR LW-SSO Authentication

Using Lightweight Single Sign-on (LW-SSO), you can enable a MyBSM user to access SHR reports with the same user credentials.

Note: As SAP BusinessObjects is a third-party application, Single Sign-on (SSO) cannot be directly achieved with OMi 10 using LW-SSO. For MyBSM , SSO is first setup between the SHR Admin Web App and OMi 10 using LW-SSO as explained in Step 2. Then, SSO is setup between the SHR Admin Web App and SAP BusinessObjects using SAP BusinessObjects Trusted Authentication as explained in Step 3.

To configure LW-SSO, perform the following steps:

1. Copy the LW-SSO token from OMi 10:

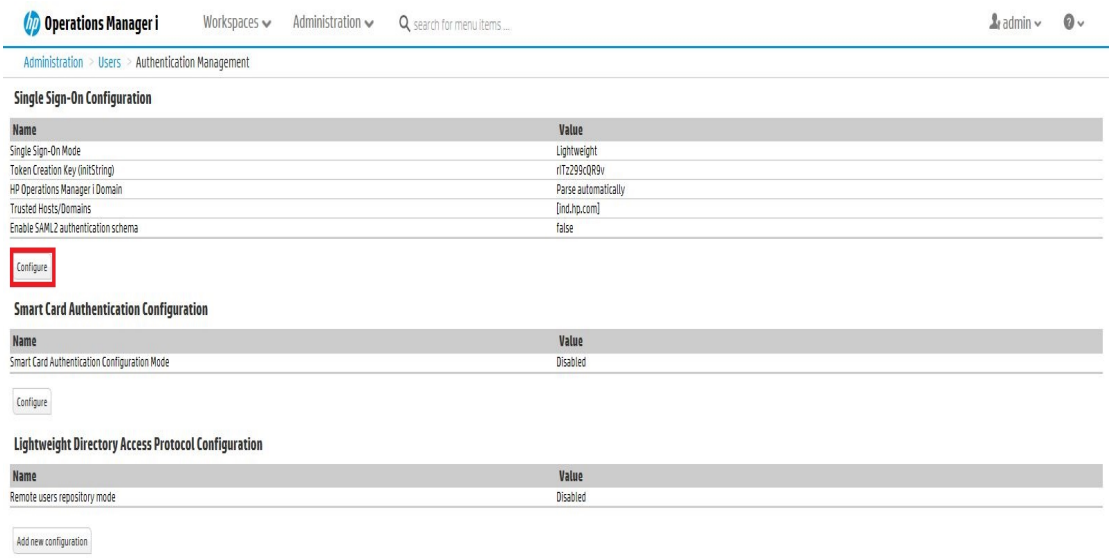
   a. Log on to the OMi 10 system as Administrator.

   b. Navigate to **Administration > Users > Authentication Management**.

   c. Copy the **Token Creation Key (InitString)** and note it down in a text file.

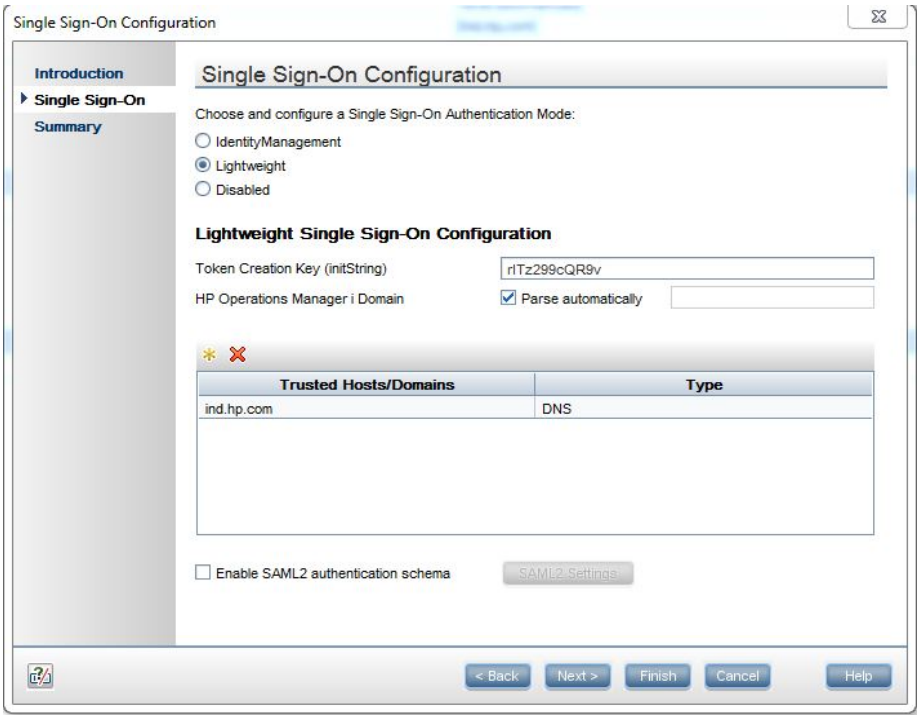
   d. Click **Configure**. The SSO Configuration Wizard appears.

   Figure 2.1



   e. Click **Single Sign-On**.

   Figure 2.2



f. Under **Trusted Hoists/Domains**, add the SHR and OMi 10 domain names.

> **Note:** If SHR and OMi 10 are hosted on the same domain, it is enough it add the domain name once to the Trusted Hosts/Domains list.

g. **Uncheck** the Enable SAML2 authentication schema check-box.

h. Click **Next**, and then click **Finish**.

i. Restart the OMi 10 services for the authentication changes to take effect.

2. To configure LW-SSO in SHR, perform the following steps:

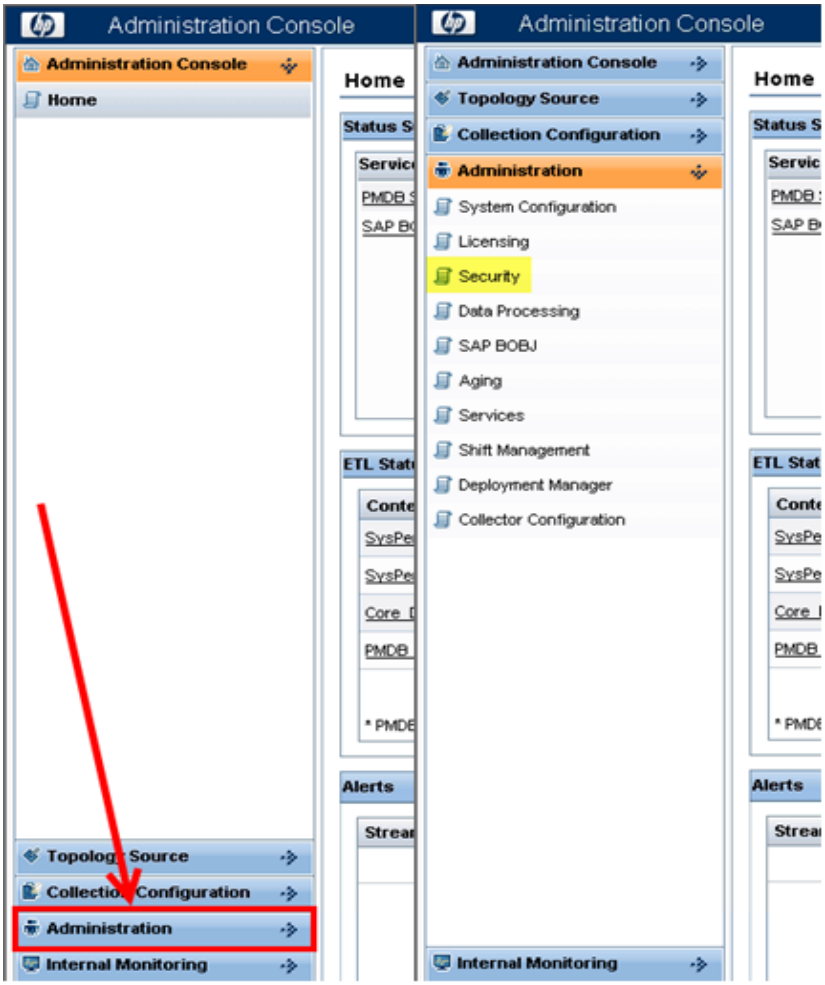
a. Log on to SHR Administration Console from the following link:

http://<hostname>:21411/BSMRAppApp

where, **hostname** is the name of the server on which SHR is installed.

b. Go to **Administration > Security** in the left pane.

Figure 2.3



c. Click **Security** and the **LW-SSO** tab opens as shown in figure below.

Figure 2.4

d. Copy the values from the Token Creation Key (InitString) field in OMi 10(This is the InitString you have copied from OMi 10 to a text file.) and paste them into the **Init String** field.

e. Check the **Enabled** option.

f. In the **Domain** field, enter the SHR domain.

g. In the **Expiration Period** field, enter the recommended value of **60** minutes for LW-SSO configuration.

h. In the **Protected Domains** field, add the OMi 10 domain name.

> **Note:**
>
> i. Even if SHR and OMi 10 are hosted in the same domain, add the domain name to the **Protected Domain** field.Even if SHR and OMi 10 are hosted in the same domain, add the domain name to the **Protected Domain** field.
>
> ii. Ensure `<INSTALL_DIR>\PMDB\data\config.prp, bo.cms` is set to fully qualified name of the SHR system.

i. Click **Save** to save the configuration as shown in figure 2.4.

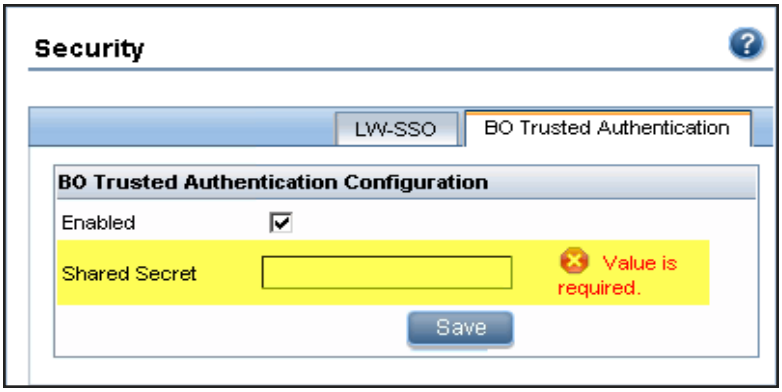
A confirmation message stating `LW-SSO Configuration saved successfully. Please restart the HP_PMDB_Platform_Administrator' service for these changes to take effect` appears. Restart this service as explained in Step 3.

Step 3: Configuring SAP BusinessObjects Trusted Authentication

To setup SSO between the SHR Admin Web App and SAP BusinessObjects, perform the following steps:

1. On the SHR system, go to **Administration >Security > BO Trusted Authentication**.
2. Check the **Enabled** option.
3. Enter a string of your choice in the **Shared Secret** field.

Figure 3.1



Note: SAP BusinessObjects Trusted Authentication works based on a shared secret mechanism between the SHR Admin Web App and SAP BusinessObjects. The string you enter in figure 3.1 is the shared secret. This string is the same shared secret across SHR Admin Web App and SAP BusinessObjects.

To verify if the same shared secret is also configured in SAP BusinessObjects, log on to SAP BusinessObjects CMC.

4. Click **Save** to save the configuration.
5. Restart the **HP_PMDB_Platform_Administrator** service from the Windows services list, to apply the changes made in "Step 2: Configuring OMi 10/SHR LW-SSO Authentication" on page 33 and "Step 3: Configuring SAP BusinessObjects Trusted Authentication" on the previous page.

Note: On a Linux host, log on as a root user and run the following command:

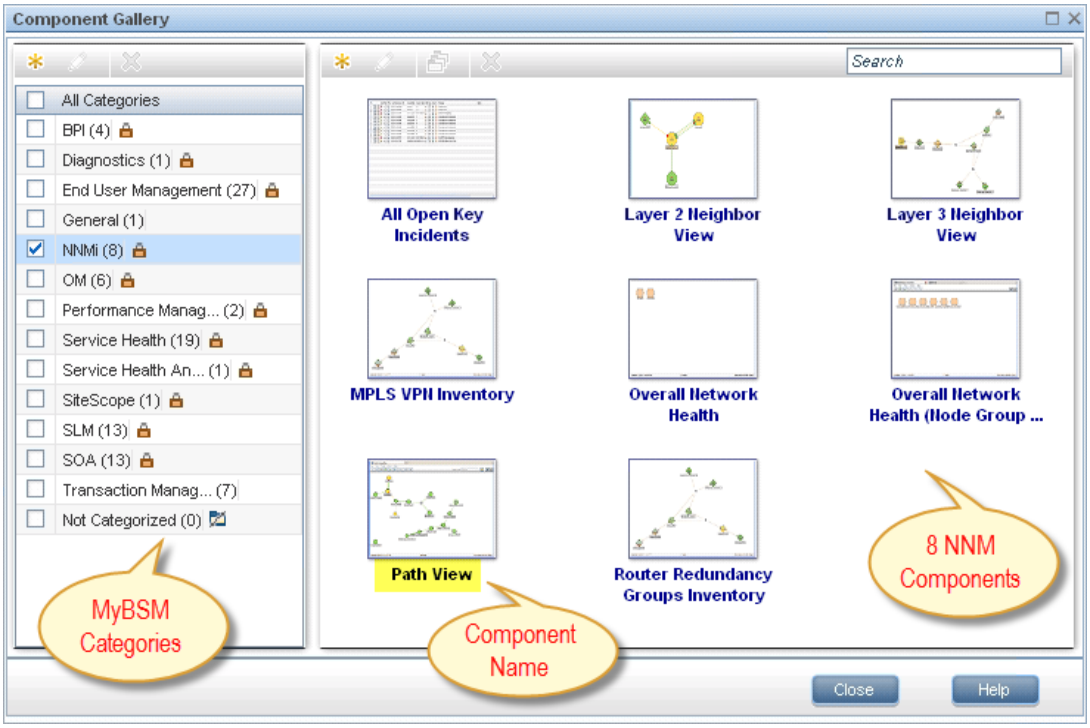
```
Service HP_PMDB_Platform_Administrator stop/start
```

Step 4: Generating the Report Component XML and Loading it to MyBSM

Every MyBSM component, such as any of the eight NNM components shown in Figure 4.1, is represented in XML files located on the OMi 10 host. To make an SHR report appear in the Component Gallery of MyBSM, create an XML and deploy it in the OMi 10 host.

Generate the component XML file using the ComponentGenerator command on the SHR host and load it to the OMi 10 host through a combination of manual copying and using the JMX Console.

Figure 4.1



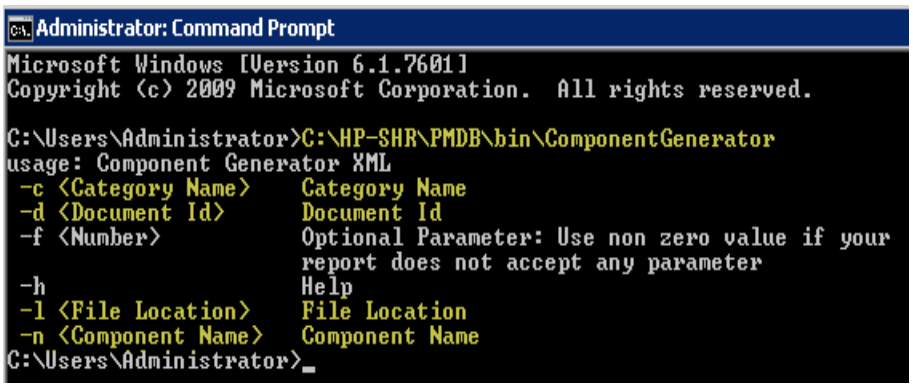
To generate the report component XML file, perform the following steps:

1. Log on to the SHR system.
2. Open a command line window (for Windows) or a shell prompt (for Linux) .
3. Run the following commands to see the ComponentGenerator syntax:

   For Windows: `%PMDB_HOME%\bin\ComponentGenerator`

   For Linux: `$PMDB_HOME/bin/ComponentGenerator`

   Figure 4.2 (Windows)



4. Run the following command to generate the XML file:

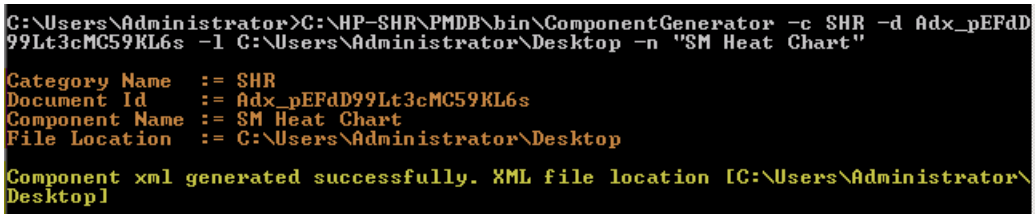
   For Windows: `%PMDB_HOME%\bin\ ComponentGenerator –c <categoryName> -d <documentId > -n <componentName> -l <outputDir> -f <optional Parameter>`

   For Linux:`$PMDB_HOME/bin/ ComponentGenerator –c <categoryName> -d <documentId > -n <componentName> -l <outputDir> -f <optional Parameter>`

   - Category Name = This is the Category to be created in Component Gallery in MyBSM
   - Document Id = This is the report's unique document ID – see the "Finding the Document ID of a Report " on page 46 section for more information.
   - File Location = This is the directory where the component XML file will be created
   - Component Name = The Component name to be created for the report in MyBSM (note the use of quotes here)
   - Optional Parameter = Use non zero value if the report does not accept view or CIID as parameter.

   > **Note:** The above command generates `<Component Category><componentName>.uim.xml` file in outputDir.

   Figure 4.3 (Linux)



To load the component to MyBSM, perform the following steps:

1. On the OMi 10 system, copy the component XML file to `%TOPAZ_HOME%\conf\uimashup\import\toload\Components`.

   > **Note:** If BSM is deployed in a distributed environment, the XML file resides in the Gateway Server.

2. Load the XML (`*.uim.xml`) file using the JMX Console.

a. On the OMi 10 system, log on to the OMi 10 JMX Console using the following link:

http://localhost:29000/mbean?objectname=Foundations%3Aservice%3DUIMDataLoader

b. Enter the credentials if prompted for a username and password.

c. Click **service=UIMDataLoader** link as shown in figure 4.4 (a) and navigate to **JMX MBean View** screen as per figure 4.4 (b)

Figure 4.4 (a)

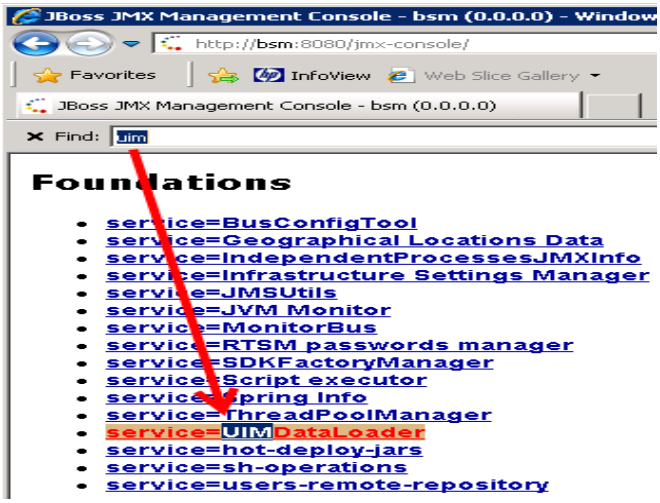
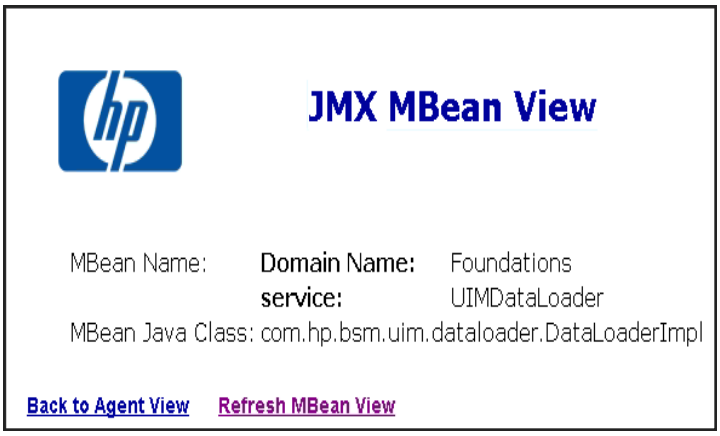
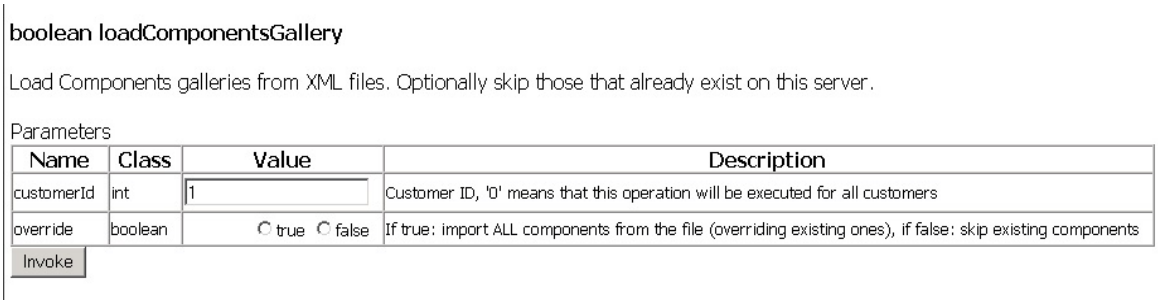


Figure 4.4 (b)



d. Go to the method named **boolean loadComponentsGallery ()**

Figure 4.5



e. Enter **1** as input value in the text field.

f. Click **Invoke** to load the `*.uim.xml` file.

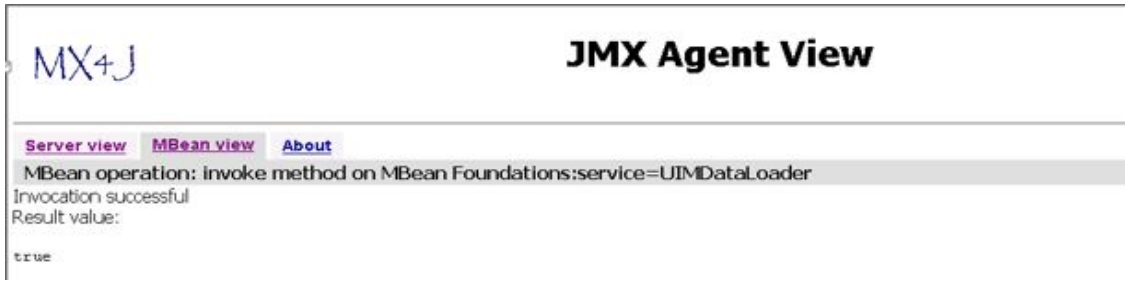
Before upload the component is visible on OMi 10 system in the following location:

`C:\HPBSM\conf\uimashup\import\toload\Components`

After successful upload, the component is visible in the following location:

`C:\HPBSM\conf\uimashup\import\loaded\Components`

Figure 4.6

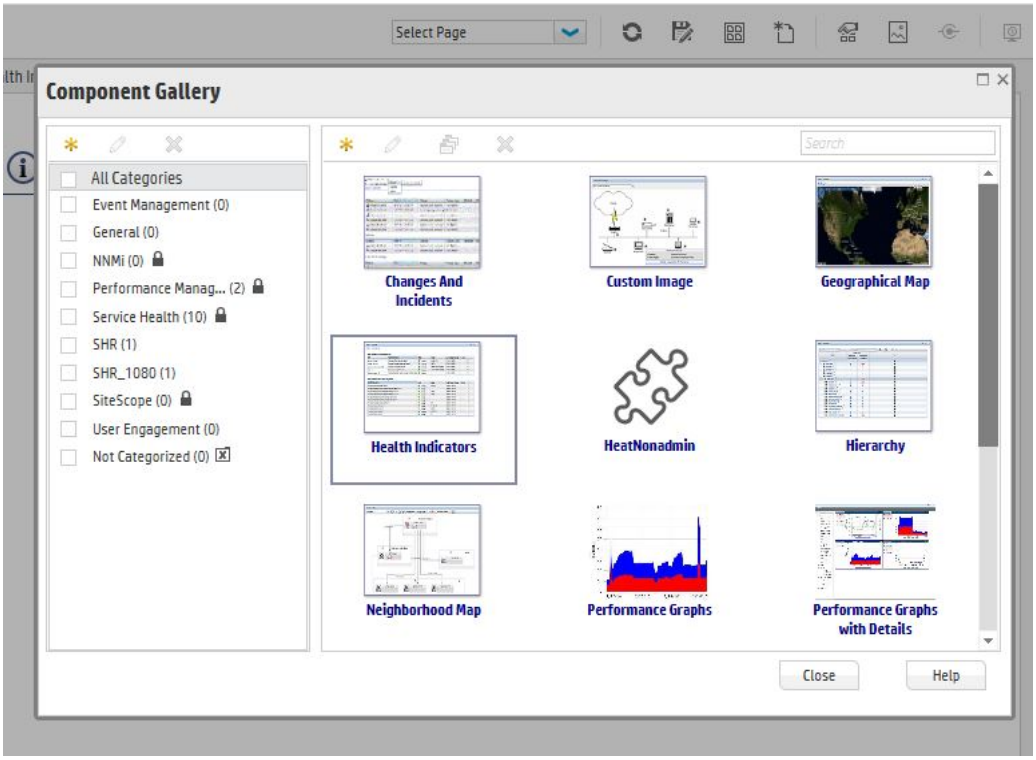


3. To verify the availability of the component in MyBSM console:

a. Log on to the OMi 10 user interface.

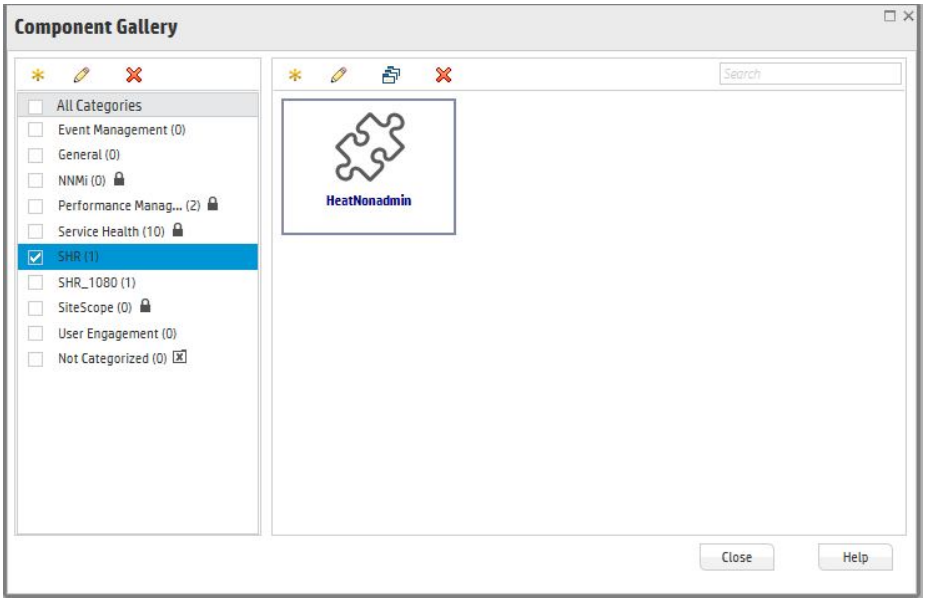
b. Click **Workspaces > My Workspace > Component Gallery**.

Figure 4.7



c. The component must be available within the category.

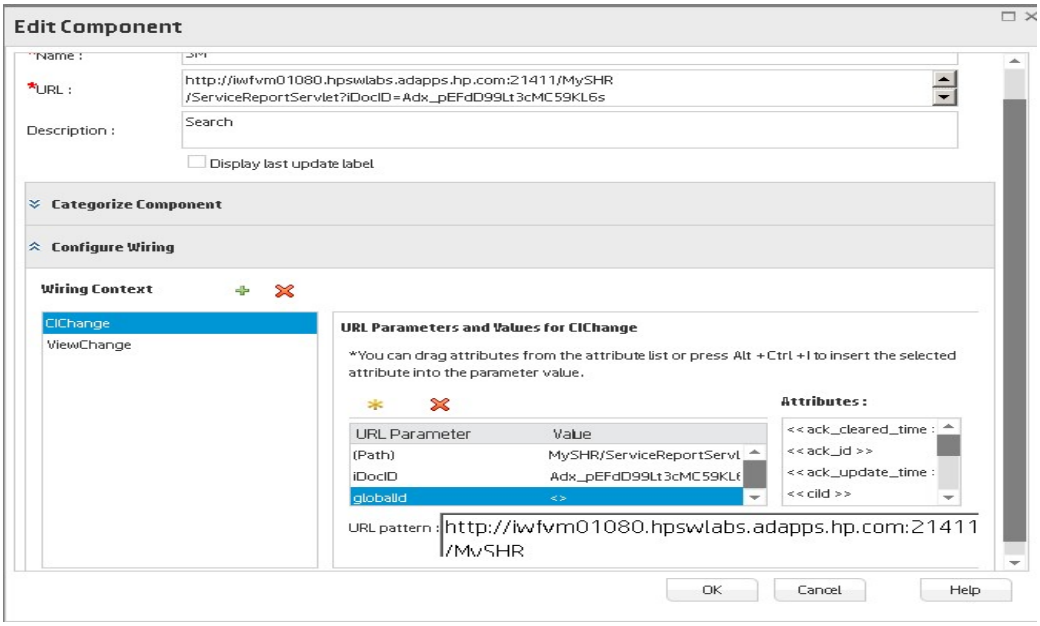
Figure 4.8



4. To verify the wiring, Click **Wiring** as shown in Figure 4.9.

Note: By default, all reports are wired on CIChange and ViewChange event. If the report does not support any events, clear the check-box to disable the wiring.

Figure 4.9



Step 5: Creating MyBSM Page and Adding the Report Component

You must create a MyBSM page and add the SHR report to it as a component.

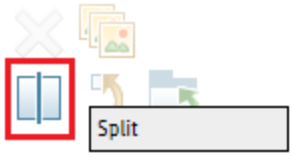
To create a MyBSM page, perform the following steps:

1. On the OMi 10 user interface click **New page**.

   Figure 5.1

2. Split the page as per the requirement.

Figure 5.2



3. Click **Components** and drag-drop the components, such as View Explorer, to trigger the events.
4. Drag and drop the required SHR components. The SHR report can be viewed in the MyBSM page.
5. Save the page to view it from the MyBSM user interface.

Best Practices

- Use existing SHR Report template for creating new reports and integrate it with MyBSM to utilize the formatting features and structure aligned with out-of-the-box (OOTB) reports.
- Use the existing user name that is configured in HP Business Service Management BSM user credentials for creating new Mashup reports in SAP BusinessObjects. If the user does not exist, create a new user with the same name.
- All SHR OOTB reports might not be qualified for integrating with MyBSM. For such reports, a prompt parameter is mandatory and BSM cannot generate that parameter.
- To integrate an OOTB SHR report with MyBSM, copy the report under Mashup Reports folder in SAP BusinessObjects InfoView, rename it (to differ with OOTB Report CUID), and perform any customizations.
- On CI change event for a Business service CI type, the Business Service CI(s) are passed as parameters to the SM CPU Heat Chart and SM Memory Heat Chart reports. This is only supported for Business Service CIs in this report.

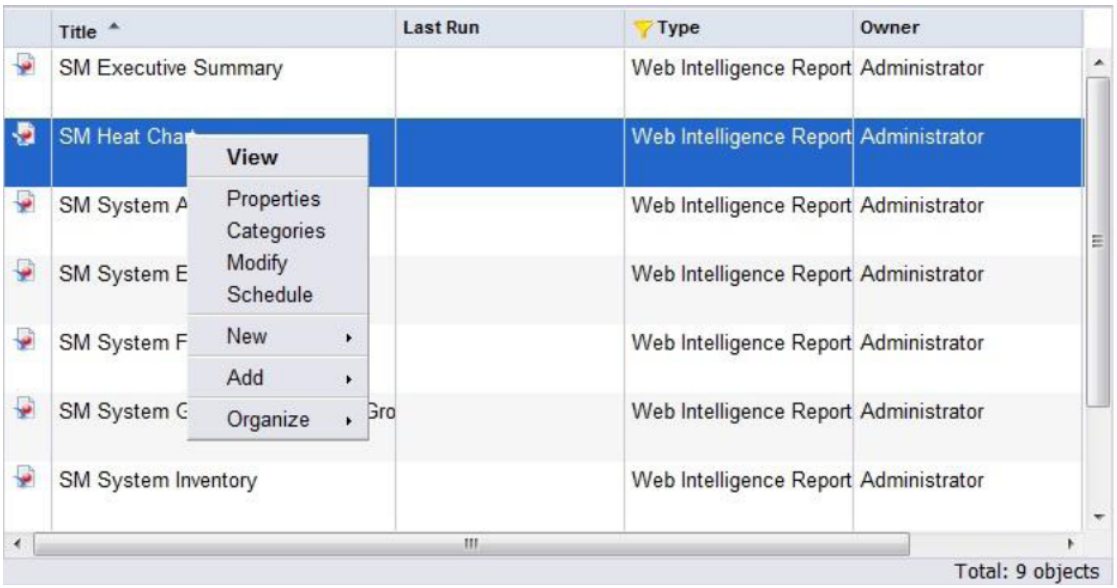
  If non-Biz Svc CIs need to be handled in custom mashup reports, a prompt named ciID should be created using the CIID attribute from the corresponding dimension (for example, ciID of Systems, Applications, and so on)
- Create Summary reports at daily/hourly level, which can be easily integrated with My BSM, because report refresh time is considerably reduced.
- Make sure the reports have **Date Range** prompt with default values to improve performance. For Inventory reports, add a Business Service/View prompt to experience better report performance.

- Add Prompts as required, but provide default values, except when the report parameters are provided by BSM, such as Business Service/Node CIID.
- To create new Objects/Filters in Universe, add them in Supplemental section of the respective Universe.
- When creating new reports, create a new data provider for each set of measures/class to avoid context related issues.
- Aim to minimize the report variables in Mashup reports.
- See the *SAP BusinessObjects Web Intelligence Guide* for new features and formatting related concerns in Mashup reports.

Finding the Document ID of a Report

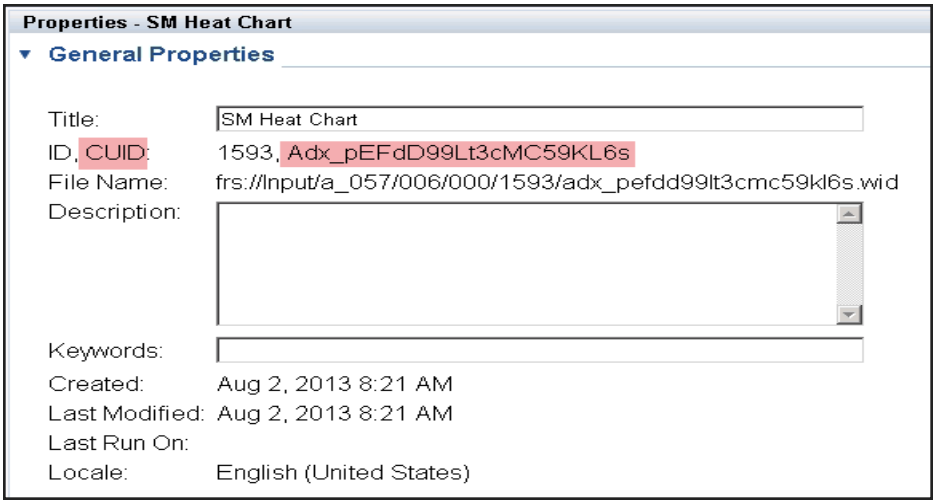
1. Log on to the SAP BusinessObjects InfoView by entering the address to **http://<hostname>:8080/InfoViewApp** in the browser window.
2. Click **Document List** and navigate to the folder that contains the report.

   Figure A.1



3. Right-click the **Report** and select **Properties**. The CUID value is the Document ID of the report.

Figure A.2


Properties - SM Heat Chart
General Properties
Title:
SM Heat Chart
ID, CUID:
1593, Adx_pEFdD99Lt3cMC59KL6s
File Name:
frs://Input/a_057/006/000/1593/adx_pefdd99lt3cmc59kl6s.wid
Description:
Keywords:
Created:
Aug 2, 2013 8:21 AM
Last Modified:
Aug 2, 2013 8:21 AM
Last Run On:
Locale:
English (United States)

We appreciate your feedback!

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Integration Guide (Service Health Reporter 9.40)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to docfeedback@hp.com.